

ELEMENTARY NUMBER THEORY

BY

J. V. USPENSKY

Professor of Mathematics, Stanford University

AND

M. A. HEASLET

*Assistant Professor of Mathematics
San Jose State College*

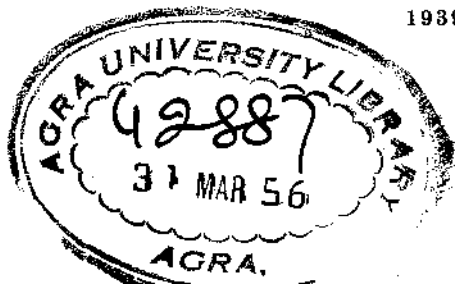
www.dbraulibrary.org.in

FIRST EDITION
SEVENTH IMPRESSION

McGRAW-HILL BOOK COMPANY, Inc.

NEW YORK AND LONDON

1939



COPYRIGHT, 1939, BY THE
MCGRAW-HILL BOOK COMPANY, INC.

PRINTED IN THE UNITED STATES OF AMERICA

*All rights reserved. This book, or
parts thereof, may not be reproduced
in any form without permission of
the publisher.*

www.dbraunlibrary.org.in

Downloaded from www.dbraunlibrary.org.in

PREFACE

Although many excellent books on number theory are available, there seems to be no one text that develops, in a systematic manner, the more elementary portions of the subject in a way adapted particularly for the classroom and the beginning student. The absence of such a book is keenly felt, inasmuch as the instruction in elementary number theory is given in an ever-increasing number of American universities and colleges. With this fact in mind the authors have endeavored to prepare a text carefully restricted to the elementary portions of the subject and yet containing things of sufficient interest to show to undergraduate students the reason for the enthusiasm with which the devotees of number theory approach their subject.

Owing to self-imposed limitations on the size of the book, many topics of interest had to be omitted. A chapter on continued fractions would have been particularly desirable, but only through manifold applications can their real value be understood, and this would have extended the book beyond reasonable limits. Geometrical and analytical methods were excluded for the same reason. Of the theory of quadratic forms only so much is given as to arouse in students the desire to study deeper this fascinating topic.

In several respects the material included in this book differs from that of standard texts in English. Here and there general principles are illustrated by applications to questions that are likely to interest beginners. Such are the appendixes on Magic Squares, Calendar Problems, and Card Shuffling. Chapter IX deals with arithmetical properties of Bernoullian

numbers, including a little known and yet very useful theorem of Voronoi from which a great many properties of Bernoullian numbers are easily derived. Chapters XII and XIII also contain some material not to be found readily in other texts.

Although the problem sets are not overly extended, they are definitely a part of the book and were designed to supplement the sections and chapters in which they appear. The student should enjoy testing his grasp of the theory by solving them.

J. V. USPENSKY.

M. A. HEASLET.

STANFORD UNIVERSITY,
SAN JOSE STATE COLLEGE,
August, 1939.

www.dbraulibrary.org.in

Downloaded from www.dbraulibrary.org.in

CONTENTS

PAGE

v

PREFACE v

CHAPTER I

✓ ELEMENTARY PROPERTIES OF INTEGERS 1

1. Origin of the Theory of Numbers—2. Operations of Addition and Multiplication—3. Summation of Certain Series—4. Polygonal Numbers—5. Subtraction and Division—6. Scales of Notation—7. The Binary System—8. The Lure of Number Theory.

CHAPTER II

✓ DIVISIBILITY AND RELATED TOPICS 24

1. Theorems Concerning Divisibility—2. Common Divisors—3. Euclid's Algorithm—4. Greatest Common Divisor of More Than Two Numbers—5. The Binary Operation Concerning Common Divisors—6. The Fundamental Theorem of Arithmetic—7. Common Multiples—8. Solution of $x^2 + y^2 = z^2$ in Integers.

CHAPTER III

✓ EUCLID'S ALGORITHM. DIOPHANTINE EQUATIONS OF THE FIRST DEGREE. 43

1. Lamé's Theorem—2. The Least-remainder Algorithm—3. Lemma—4. Kronecker's Theorem—5. Indeterminate Equations of the First Degree—6. Continuation—7. Nonnegative Solutions of Linear Indeterminate Equations—8. Equations in Several Unknowns and Systems of Equations.

CHAPTER IV

✓ ON PRIME NUMBERS. 68

1. Prime and Composite Numbers—2. A Test of Primality—3. The Sieve of Eratosthenes—4. Unique Factorization Theorem—5. Criterion of Divisibility—6. Divisors of Numbers—7. The Number and Sum of Divisors—8. Numerical Functions Depend-

ing on Divisors—9. Euler's Recurrence Formula—10. Perfect Numbers—11. Number of Primes Infinite—12. Bouse's Inequality—13. A Property of Thirty—14. Remarks on the Distribution of Primes—15. Primes in Arithmetic Progressions—16. Some Unsolved Problems Concerning Primes—17. Integral Part of a Real Number—18. The Highest Power of a Prime Contained in a Factorial—19. Some Applications.

CHAPTER V

A GENERAL COMBINATORIAL THEOREM AND ITS APPLICATIONS. 105

1. Combinatorial Theorem—2. Euler's Function $\varphi(n)$ —3. Moebius's Function $\mu(n)$ —4. Fundamental Property of $\mu(n)$ —5. A Property of $\varphi(n)$ —6. An Inversion Formula—7. Another Application of the Combinatorial Formula—8. Meissel's Formula.

CHAPTER VI

ON THE CONGRUENCE OF NUMBERS 126

1. Definition and Simple Properties of Congruences—2. Elementary Properties of Congruences (Continued)—3. Distribution of Numbers in Classes Modulo m —4. Various Useful Complete Systems of Residues—5. Generation of a Complete System Modulo ab When $(a, b) = 1$ —6. Generation of a Complete System of Residues mod a^n —7. An Application—8. Reduced System of Residues—9. Theorems of Fermat and Euler—10. Another Proof—11. Residues of $S_n(p)$ mod p —12. Wilson's Theorem—Appendix on Magic Squares: 1. Definition of Magic Squares—2. Auxiliary Squares—3. Magic Squares for Odd n —4. Magic Squares for n Divisible by 4—5. Magic Squares for n Divisible by 2 Only.

CHAPTER VII

CONGRUENCES WITH ONE UNKNOWN. LAGRANGE'S THEOREM AND ITS APPLICATIONS 173

1. Congruences in General—2. Congruences of the First Degree—3. Methods for Solving Congruences of the First Degree—4. Continuation—5. An Important System of Congruences—6. The Case of Moduli Relatively Prime in Pairs—7. Congruences of Higher Degree: Composite Moduli—8. Congruences of Higher Degree: Moduli Powers of Primes—9. Congruences with a Prime Modulus; Lagrange's Theorem—10. Some Appli-

ications of Lagrange's Theorem—11. Condition for a Congruence to Have Number of Roots Equal to Its Degree—12. An Application—Appendix on Calendar Problems: 1. Relation between Dates and Days of the Week—2. Remarks on the Church Calendar—3. The Date of Easter.

CHAPTER VIII

RESIDUES OF POWERS 222

1. Exponent of $a \pmod m$ —2. Practical Rule for the Formation of Periods—3. Properties of Exponents $\pmod m$ —4. Primitive Roots for Prime Moduli—5. Method for Finding Primitive Roots—6. Indices—7. Application of Indices to the Solution of Congruences—8. Tables of Indices and Primitive Roots—Appendix on Card Shuffling.

CHAPTER IX

ARITHMETICAL PROPERTIES OF BERNOULLIAN NUMBERS 249

1. Origin of Bernoullian Numbers—2. Definition of Bernoullian Numbers by a Symbolic Formula—3. The General Expression for the Sum $S_n(N)$ —4. Proof That Bernoullian Numbers Are Positive—5. Staudt's Theorem—6. An Auxiliary Congruence—7. Another Auxiliary Congruence—8. Von Stürm's Theorem and Its Applications—9. Fractions $\pmod m$. Kummer's Congruences.

CHAPTER X

QUADRATIC RESIDUES 270

1. Definition of Quadratic Residues—2. Prime Moduli—3. Quadratic Residuability of a Product—4. Euler's Criterion—5. Legendre's Symbol—6. Fundamental Problems—7. Quadratic Character of -1 and 2 —8. Quadratic Reciprocity Law—9. The Lemma of Gauss—10. Proof of the Reciprocity Law—11. Applications—12. Jacobi's Symbol—13. The Evaluation of Jacobi's Symbol—14. Solution of the Equation $(P/Q) = \pm 1$ for Q —15. Quadratic Residues of Composite Moduli—16. Moduli 2^m —17. General Conclusion—18. Solution of Quadratic Congruences for Prime Moduli—19. The Exclusion Method.

CHAPTER XI

SOME PROBLEMS CONNECTED WITH QUADRATIC FORMS 325

1. Object of This Chapter—2. Fundamental Lemma—3. The Equation $x^2 - ay^2 = m$ —4. Applications of the Fundamental

	PAGE
Lemma—5. Fermat's Equation—6. The Equation $x^2 - ay^2 = m$ with Positive a —7. A Test of Primality—8. The Exclusion Method—9. Another Application of the Fundamental Lemma—10. Kummer's Proof of the Reciprocity Law—11. The Four Squares Theorem.	

CHAPTER XII

SOME DIOPHANTINE PROBLEMS	388
-------------------------------------	-----

1. Object of This Chapter—2. Equations $x^2 + ay^2 = z^n$ —3. Particular Cases—4. Some Equations of the Type $x^2 + a = y^n$ —5. Some Insoluble Diophantine Problems—6. Another Fermat Problem—7. Fermat's Last Theorem—8. One More Fermat Problem—9. An Ancient Problem.

CHAPTER XIII

LIUVILLE'S METHODS	429
------------------------------	-----

1. Object of This Chapter—2. Arbitrary Functions. Conditions of Parity—3. The First Fundamental Identity—4. The Second Fundamental Identity—5. Euler's Recurrence Formula—6. Specialization of the Fundamental Identities—7. An Application—8. Jacobi's Theorem—9. Additional Identities—10. Representations by the Sums of Three Squares.

INDEX	481
-----------------	-----

ELEMENTARY NUMBER THEORY

CHAPTER I

ELEMENTARY PROPERTIES OF INTEGERS

1. Origin of the Theory of Numbers. The theory of numbers, also called higher arithmetic, is concerned, at least in its elementary parts, with the properties of whole numbers or integers. As an established mathematical discipline it is one of the youngest, yet its roots go deep into history.

The notion of the whole number as an aggregate of units is so primitive that it is hardly possible to imagine human beings who do not possess it in the form of counting, at least within a limited range. As far back as any records can be found, mankind possessed adequate methods for keeping a tally of things, while our knowledge of ancient civilizations reveals an already highly developed art of denoting and operating on numbers as far back as 3500 B.C. and earlier.

The needs of everyday life were primarily responsible for the rise of practical arithmetic. On the higher level of civilization when urgent needs were satisfied and opportunity and leisure were available to ponder about things, numbers in themselves began to attract attention. Peculiarities of individual numbers or classes of numbers began to be observed. But such speculations on numbers, far from being a real study of their

properties, developed at first into a peculiar number mysticism prevalent among ancient civilized peoples. Such numbers as 3 and 7 were accepted as omens of good luck. Later, such terms as perfect numbers, feminine numbers, and amicable numbers were used with no appreciation as to whether the concepts were of a strictly mathematical nature or merely of mystical properties. Ancient Hebrews and Greeks were versed in a kind of numerology made more adaptable to superstition and quasi-religious beliefs by their particular number systems. These peoples used the letters of the alphabet to write numbers so that words had a double significance. It is contended that certain Biblical passages involve such a double significance, which must be recognized if the passages are to be completely understood.

The first rudiments of a scientific approach to the study of numbers, still intermixed with a good deal of number mysticism, can be traced back to Pythagoras (sixth century B.C.) and his disciples. It is believed that the distinction between prime and composite numbers was made in the Pythagorean school and, if true, this distinction is almost as much to the credit of the Pythagoreans as their other great discovery of incommensurable magnitudes. That the Pythagoreans attained some degree of proficiency in the theoretical investigation of numbers is attested again by the rule attributed to the head of the school himself for forming right-angle triangles with integral sides like the age-old triangle with sides 3, 4, 5.

By the time of Euclid (about 300 B.C.) the Greeks possessed quite a number of strictly scientific facts about numbers, mostly pertaining to their divisibility. A great impulse to the further development of number theory was not received until the seventeenth century, with the memorable discoveries of many deep and abstruse properties of numbers by Fermat.

This is not the place to go into more details concerning the historic development of our science. It suffices to say that,

sharing its origin with mystical speculations on numbers, the theory of numbers in time grew into a vast and beautiful branch of mathematics with ramifications linking it with almost every other branch of this science.

Another great science, astronomy, also owes its origin to a pseudo-science, astrology. And strangely enough, just as astrology still survives side by side with astronomy, so the ancient number mysticism thrives even now under the guise of numerology—a fact that would make one despair of mankind had not, on the other hand, the human spirit produced sublime creations, of which the theory of numbers is one.

2. Operations of Addition and Multiplication. Almost inseparable from the concept of an integer itself is that of the addition of two or more integers. When the units of which two integers a and b consist are put together, a new integer $a + b$ —the sum of a and b is generated. It is intuitively clear that the operation of addition conforms to the following laws:

www.dbraulibrary.org.in

Commutative law for addition:

$$a + b = b + a.$$

Associative law for addition:

$$(a + b) + c = a + (b + c),$$

and everything else pertaining to addition follows from these laws.

The multiplication of integers is merely repeated addition; that is, to multiply a by b is to find the sum of b numbers, each of which is a . Like addition, multiplication is a commutative and associative operation; moreover, it is distributive with respect to addition. We mean by this that multiplication conforms to the following laws:

Commutative law for multiplication:

$$ab = ba.$$

Associative law for multiplication:

$$(ab)c = a(bc).$$

Distributive law:

$$(a + b)c = ac + bc.$$

The distributive law is a simple corollary to the commutative and associative laws for addition. As to the two other laws, long practice in arithmetic since childhood makes them seem obvious, although a few explanations are necessary to convince oneself of their universal validity. Take b rows, each consisting of a units,

$$\begin{array}{c} \overbrace{1, 1, 1, \dots, 1}^{a \text{ times}} \\ 1, 1, 1, \dots, 1 \\ \dots \dots \dots \\ 1, 1, 1, \dots, 1 \end{array} \left. \vphantom{\begin{array}{c} \overbrace{1, 1, 1, \dots, 1}^{a \text{ times}} \\ 1, 1, 1, \dots, 1 \\ \dots \dots \dots \\ 1, 1, 1, \dots, 1 \end{array}} \right\} b \text{ times}$$

and add these units first by rows. The sum in each row is a and there are b such rows; hence the total sum is ab . On the other hand, add the units by columns. The sum in each column is b and there are a such columns; hence the total sum is ba . Thus $ab = ba$. The principle involved in this reasoning—counting the same collection in two different ways—is very often used to derive much more abstruse results.

Consider now c rows, each consisting of a number b repeated a times:

$$\begin{array}{c} b, b, b, \dots, b \\ b, b, b, \dots, b \\ \dots \dots \dots \\ b, b, b, \dots, b \end{array}$$

and add these numbers first by rows and then by columns. The result of the summations can be expressed in two ways: first, as $(ba)c$; and second, as $(bc)a$, so that

$$(ba)c = (bc)a.$$

But by the commutative law

$$ba = ab, \quad (bc)a = a(bc),$$

so

$$(ab)c = a(bc).$$

Everything else pertaining to multiplication and addition follows from the enumerated fundamental laws, but we need not go into details to show how it can be proved.

The operations of addition and multiplication open the way to various classifications of integers according to their origin. As an example, we see that some integers can be generated by repeated addition of 2, while the others cannot. Hence the distinction between even and odd integers—possibly the oldest of such classifications. Again, some integers can be generated as products of factors none of which is unity; for instance, $6 = 2 \cdot 3$, while the others, like 5, cannot be generated in this fashion. Hence there arises an important division of integers into composite and primes. Squares, cubes, biquadrates, etc., are generated as products of two, three, four, etc., equal numbers.

3. Summation of Certain Series. Nothing is more natural than to seek the sum

$$1 + 2 + 3 + 4 + \cdots + n$$

of all integers from 1 to any given integer n . Of course this can be done by direct addition when n is given, though for a large n this is inconvenient. The question arises whether the same number can be generated in some other way which would be simple and more convenient. The answer has been known since time immemorial. To find the sum

$$1 + 2 + 3 + 4 + \cdots + n$$

it suffices to multiply one-half of n by $n + 1$ if n is even and one-half of $n + 1$ by n if n is odd. It is in this reduction of

the original problem to a much simpler one that the summation of the series

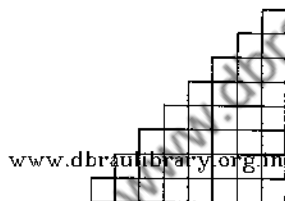
$$1 + 2 + 3 + 4 + \cdots + n$$

consists. This and some other "summations" can be treated by a very simple and intuitive geometrical method which we shall now explain.

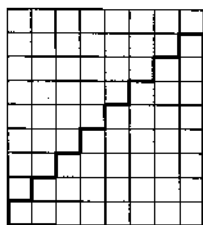
Let us consider first the series

$$1 + 2 + 3 + 4 + \cdots + n.$$

Denote the number 1 by a square of unit area, 2 by two such areas, and so on. The problem of summing the numbers is now changed to the problem of finding the area of the figure



where the dimensions are n along the base and side. Taking an identical figure, we may join them so as to produce the rectangle

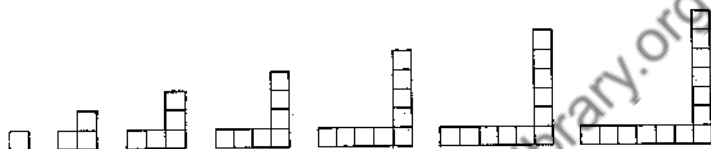


The dimensions of the rectangle are n by $n + 1$, and its area is $n(n + 1)$. It follows that the original area is $n(n + 1)/2$, and the sum of n consecutive integers is equal to one-half the number of integers times this number increased by 1.

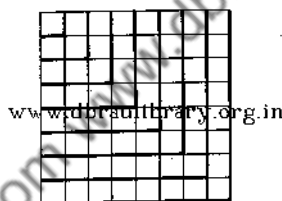
Again consider the sum of the first n odd integers

$$1 + 3 + 5 + 7 + \cdots + (2n - 1).$$

Using the same geometrical figures, we see the sum is the total area of the following figures



where the last one has n squares along each side. These areas can be combined into a square as shown here,



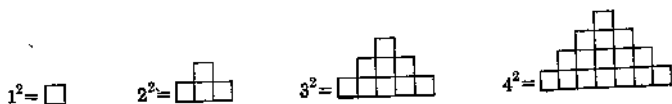
from which we conclude

$$1 + 3 + 5 + 7 + \cdots + (2n - 1) = n^2.$$

Slightly more ingenious methods are needed to sum the series

$$1^2 + 2^2 + 3^2 + \cdots + n^2.$$

We shall develop the result for $n = 4$, using, however, reasoning which can be immediately generalized. From the figures



we can conclude that the sum of the given cubes is the same as the sum of the numbers in the following figure:

1	2	3	4
2	4	6	8
3	6	9	12
4	8	12	16

That the above relations are true in general we may see, since

$$i + 2i + \dots + (i-1)i + ii + (i-1)i + \dots + 2i + i = 2i(1 + 2 + 3 + \dots + (i-1)) + ii = i(i-1)i + ii = i^3.$$

Since each column in the figure is a multiple of the first column, the sum of the numbers can be written

$$(1 + 2 + 3 + 4)(1 + 2 + 3 + 4) = (1 + 2 + 3 + 4)^2$$

and, as a general result,

$$1^3 + 2^3 + \dots + n^3 = (1 + 2 + \dots + n)^2.$$

The results we have obtained are more or less trivial algebraic facts, but it is easy to see that they must have been considered quite astonishing to ancient discoverers who were entirely lacking in our algebraic methods and were handicapped by their unwieldy number systems.













4. Polygonal Numbers. The bent of the Greeks toward geometry no doubt explains their interest in numbers connected with geometrical figures. These so-called "polygonal" or "figurate" numbers can be defined in a purely geometrical fashion, but we shall discuss them algebraically as well.

Consider the arithmetic progressions

$$\begin{aligned} &1, 2, 3, 4, 5, 6, \dots, n; \\ &1, 3, 5, 7, 9, 11, \dots, 2n - 1; \\ &1, 4, 7, 10, 13, 16, \dots, 3n - 2; \\ &1, 5, 9, 13, 17, 21, \dots, 4n - 3; \\ &\dots \end{aligned}$$

The sums of these progressions give respectively the triangular, square, pentagonal, hexagonal, . . . numbers of rank n . In general the n th r -gonal number P_n^r is equal to the sum of the n first terms of the arithmetic progression beginning with 1 and with the common difference $r - 2$.

The reason for the geometrical nomenclature is apparent when the numbers are replaced by dots and the dots are arranged in the following figures:

NAME	RANK 1	RANK 2	RANK 3	RANK 4
Triangular				
Square				
Pentagonal				

Thus, considering regular polygons homothetic with respect to one of the vertices and containing 2, 3, 4, . . . , n points at equal distances along the sides, the collection of points gives a geometric representation of the polygonal numbers.

The n th term of an arithmetic progression, beginning with 1 and with the difference $r - 2$, is

$$1 + (n - 1)(r - 2),$$

and since the sum of the terms of an arithmetic progression is the product of the number of terms by the half-sum of the extreme terms, it follows that

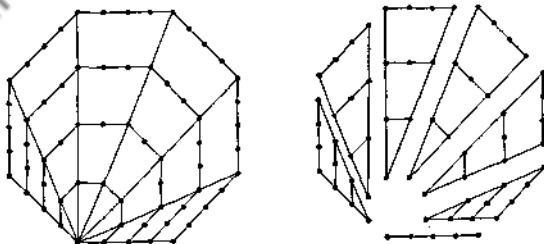
$$P_n^r = \frac{n}{2}[2 + (n - 1)(r - 2)] = n + (r - 2)\frac{n(n - 1)}{2}.$$

A table of the first few polygonal numbers is given below:

Number	1st	2d	3d	4th	5th	6th	7th	8th	9th	10th
Triangular.....	1	3	6	10	15	21	28	36	45	55
Square.....	1	4	9	16	25	36	49	64	81	100
Pentagonal.....	1	5	12	22	35	51	70	92	117	145
Hexagonal.....	1	6	15	28	45	66	91	120	153	190
Heptagonal.....	1	7	18	34	55	81	112	148	189	235
Octagonal.....	1	8	21	40	65	96	133	176	225	280

Once one has the explicit expressions for polygonal numbers, many simple properties connected with them reduce to mere algebraic identities, but a certain amount of ingenuity can be expended in establishing their properties geometrically. Let us consider a simple example: Every octagonal number is equal to its rank plus the triangular number of preceding rank multiplied by 6.

This is a literal statement of the algebraic expression for P_n^8 and is obviously a special case of a more general fact. Geometrically it is clear that an octagonal number of any rank can be broken up as shown below:



5. Subtraction and Division. Addition and multiplication can be applied to integers without restriction. The reverse operation to addition—subtraction—however, is not always possible. To avoid this inconvenience, the series of integers 1, 2, 3, . . . is completed by adjoining 0 and negative integers, -1, -2, -3, We now think of integers in a general sense as consisting of the sequence of numbers

$$\dots, -3, -2, -1, 0, 1, 2, 3, \dots,$$

which can be indefinitely extended in both directions and is closed under the operations of addition, subtraction and multiplication.

If b denotes an arbitrarily selected positive integer, the integers

$$\dots, -2b, -b, 0, b, 2b, \dots$$

are called "multiples" of b . An integer a either coincides with one of the multiples of b or is situated between two consecutive multiples. In the former case there is an integer c such that $a = bc$; in the latter case there is again a determined integer c such that $bc < a < b(c + 1)$. Since, in this case, $a - bc > 0$ and, on the other hand, $a - bc < b$, we can set

$$a = bc + r \tag{1}$$

where $r > 0$ and $r < b$. When a is a multiple of b , the same equality will hold, but with $r = 0$. Thus, given two integers a, b , the latter being positive, there exist unique integers c and r such that

$$a = bc + r$$

where $0 \leq r < b$. Numbers c and r are called, respectively, the "quotient" and "remainder" in the division of a by b , and in practice they are found by a process of division explained in elementary arithmetic.

It was assumed that b was a positive integer; but clearly (1) will hold with proper c and r if b is a negative integer, only then will the limitations for r be $0 \leq r < |b|$. The case of $b = 0$, however, must be excluded. The fact that for any integer a with respect to an integer $b \neq 0$ there exists a representation in the form (1) with $0 \leq r < |b|$ appears very trivial; nevertheless it is a fact of truly fundamental importance in the theory of numbers.

6. Scales of Notation. For purely theoretical purposes it is quite immaterial what system of representing integers is adopted. Greeks, with the most cumbersome notation for numbers, were able to discover some fundamental arithmetical truths. However, for practical purposes it is desirable to denote numbers in such a way as to facilitate the actual performance of operations on them. In this respect the Hindu-Arabic or decimal system satisfies all the requirements exceedingly well. It is based on the possibility of representing any integer N in the form

$$N = c_0 + c_1 10 + c_2 10^2 + \dots + c_n 10^n$$

where the "digits" c_0, c_1, c_2, \dots are either 0 or numbers from 1 to 9 denoted by special signs.

Instead of the number 10 as a base or radix, any other number ρ greater than 1 can be taken and any integer can be represented in the form

$$N = c_0 + c_1 \rho + c_2 \rho^2 + \dots + c_m \rho^m$$

with digits c_0, c_1, c_2, \dots as numbers not greater than $\rho - 1$ and not less than 0. To show that such a representation is possible, we divide N by ρ ; let N_1 be the quotient and c_0 the remainder in this division. Then

$$N = N_1 \rho + c_0; \quad 0 \leq c_0 < \rho$$

and $N_1 < N$. As long as $N_1 \geq \rho$ we divide again N_1 by ρ , obtaining N_2 for a quotient and c_1 for a remainder, so that

$$N_1 = N_2\rho + c_1, \quad 0 \leq c_1 < \rho.$$

If $N_2 \geq \rho$ we continue in the same manner. Thus a series of decreasing positive integers arises:

$$N > N_1 > N_2 > \cdots > N_{m-1} > N_m$$

and this series can be continued after each term N_i which is $\geq \rho$. Now this is an evident principle often used in the number theory: a series of positive decreasing integers cannot be continued indefinitely. Hence there will be some term N_m in the above series which is positive and less than ρ . Then, setting

$$N_m = c_m$$

and eliminating N_m, N_{m-1}, \dots, N_1 from the system

$$N = N_1\rho + c_0$$

$$N_1 = N_2\rho + c_1$$

$$\text{www.dbraulibrary.org.in}$$

$$N_{m-2} = N_{m-1}\rho + c_{m-2}$$

$$N_{m-1} = N_m\rho + c_{m-1}$$

$$N_m = c_m,$$

we get the desired representation

$$N = c_0 + c_1\rho + c_2\rho^2 + \cdots + c_m\rho^m$$

with $c_i < \rho$ for $i = 0, 1, \dots, m$ and $c_i \geq 0$ for $i = 0, 1, \dots, m-1$ while $c_m > 0$. That this representation is unique follows simply from the observation that in any such representation

$$N = d_0 + d_1\rho + d_2\rho^2 + \cdots$$

d_0 is the remainder in the division of N by ρ , d_1 is the remainder in the division of

$$N_1 = \frac{N - d_0}{\rho}$$

by ρ , d_2 is the remainder in the division of $N_2 = \frac{N_1 - d_1}{\rho}$ by ρ , and so on, so that d_0, d_1, d_2, \dots of necessity coincide with c_0, c_1, c_2, \dots

For a given base or radix ρ the number N may be indicated by merely writing the coefficients of the expression for N in reverse order. Since the coefficients are integers from 0 to $\rho - 1$, only ρ symbols are needed to express N no matter how large N is. For $\rho = 10$ we use the Hindu-Arabic symbols 0, 1, 2, 3, 4, 5, 6, 7, 8, 9. For $\rho = 7$ we might use 0, 1, 2, 3, 4, 5, 6 and for $\rho = 2$ merely 0 and 1. As an example, consider the number fourscore and six. Using these scales of notation, we should have

$$\begin{aligned}(86)_{10} &= 8 \cdot 10 + 6 = 1 \cdot 7^2 + 5 \cdot 7 + 2 = (152)_7 \\ &= 1 \cdot 2^6 + 1 \cdot 2^4 + 1 \cdot 2^2 + 1 \cdot 2 = (1010110)_2.\end{aligned}$$

For increasing bases we get, respectively, the binary, ternary, quaternary systems, and so on. When the base is 12, two new symbols are needed for 10 and 11. If we take as our list of digits 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, α , β we have, for example,

$$(30,816)_{10} = (15,\alpha 00)_{12}.$$

Division by 12 naturally consists in pointing off a "duodecimal" place; division by 6, as in the case of 5 in the decimal system, merely consists of multiplying by 2 and moving the duodecimal place to the left; divisions by 4, 3, and 2 similarly may be replaced by operations in multiplication.

7. The Binary System. In the binary system each integer is represented in the form

$$N = 2^m + e_1 2^{m-1} + e_2 2^{m-2} + \dots + e_m$$

where the digits e_1, e_2, e_3, \dots are either 1 or 0. Dropping terms with coefficients equal to 0, we see that every integer

can be represented as a sum of powers of 2 and in only one way. Thus, for example,

$$343 = 2^8 + 2^6 + 2^4 + 2^2 + 2 + 1$$

considering 1 as the zero power of 2.

That every integer can be partitioned into parts which are powers of 2 is an interesting, useful, and not quite trivial proposition. Besides its theoretical value it has curious applications in "recreational mathematics." Though this does not belong properly to the theory of numbers, it should be interesting to present an application of the binary system, by no means trivial, to the theory of the game of Nim, an ancient pastime originating probably in China.

In the original form Nim is played with three piles of counters and is for two contestants. The contestants play alternately and may pick up as many counters as they wish, at one time, from *one* pile, but they must take at least one counter. The winner is the one picking up the last counter. The game and its generalization, which we intend to consider, may be analyzed completely through the use of the binary system; that is, definite rules may be established such that if one knows these rules and has a favorable opening move, he can always win the game. In the general form of the game, we assume there are m piles with A, B, C, \dots, L objects. It is allowed to take up any numbers of objects from not more than k piles, where $k \leq m - 1$, and the player picking up the last counter wins.

The method of solution lies in the determination of certain positions such that if one player P leaves this position, the other player Q cannot possibly win. We proceed as follows: Write A, B, C, \dots, L in the binary system of notation and write the sum of the digits in every column. If in all the columns the sum is divisible by $k + 1$, we have an "extraordinary position"; otherwise we have an "ordinary position."

From an extraordinary position, no matter how one plays, an ordinary position results. This is almost evident, for the digits in some column must change, and in the first column from the left in which the change occurs, only units may change into zeros, not zeros into units, since the numbers diminish. Again, at least one unit and not more than k are changed into zeros and, in consequence of this change, the sum of the digits, which originally was divisible by $k + 1$, no longer will retain this property.

It is possible, from an ordinary position, to deduce an extraordinary position. To prove this we first disregard the columns with sums divisible by $k + 1$. In the remaining columns l, l_1, l_2, \dots , counting from left to right, suppose the sums leave the remainders r, r_1, r_2, \dots when divided by $k + 1$, each being less than or equal to k . Write r numbers having r units in column l in the first r lines and replace all these units by 0. Smaller numbers will result, not more than k piles will be affected, and the sum of the digits in column l will be divisible by $k + 1$. Consider now column l_1 and let the number of zeros in the first r lines of it be s_1 . Suppose at first $r_1 + s_1 > k$; that is, $s_1 \geq k + 1 - r_1$. Changing $k + 1 - r_1$ zeros to 1, the sum of the digits in column l_1 will be divisible by $k + 1$. Suppose next that $r_1 + s_1 \leq k$. To the r numbers already chosen we add as many of the remaining as are needed to give r_1 units in column l_1 and replace these units by zeros. In both possibilities the numbers considered may only diminish, and we have made the sum of the digits in column l_1 divisible by $k + 1$ while not changing more than k piles. Passing to column l_2 we proceed in the same way, and so on. This proves the statement.

Examples will illustrate these operations better. Suppose we have given $m = 6, k = 4$ with piles containing 6, 8, 11, 25, 29, and 31 objects. Summing the columns, we find $l = 1, l_1 = 3, l_2 = 4, l_3 = 5$, and $r = 3, r_1 = 3, r_2 = 3, r_3 = 4$.

Since $r = 3$, we must change three units to zeros. Since $s_1 = 1$, $r_1 = 3$, and $s_1 + r_1 = 4 = k$, we must adjoin a number so as to have $3 = r_1$ units in the third column. Again, $s_2 = 2$, $r_2 = 3$, and $s_2 + r_2 = 5 > k$, so that we change $k + 1 - r_2 = 2$ zeros to 1. Finally, $s_3 = 1$, $r_3 = 4$, and $s_3 + r_3 = 5 > k$, so that we change $k + 1 - r_3 = 1$ zero to 1. The work may be arranged as follows:

*		*		*	*
1 → 0	1	0		0 → 1	1
1 → 0	1	1 → 0		0 → 1	1
1 → 0	1	1 → 0		1	1
		1 → 0		1	0 → 1
	1	0		0	0
	1	0		1	1

and we have as a result the extraordinary position

$$\begin{array}{r}
 \text{www.dbraulibrary.org.in} \\
 1011 < 11,001 \\
 1011 < 11,101 \\
 1011 < 11,111 \\
 11 < 110 \\
 1000 \\
 1011 \\
 \hline
 5055
 \end{array}$$

For a second example, suppose $m = 6$, $k = 3$ with piles containing 2, 3, 4, 9, 13, and 14 objects. We find $l = 1$, $l_1 = 2$, $l_2 = 3$, $l_3 = 4$, and $r = 3$, $r_1 = 3$, $r_2 = 3$, $r_3 = 3$. Since $r = 3$ we must change three units to zeros in column l . Since $s_1 = 1$, $r_1 = 3$, and $r_1 + s_1 = 4 > k$, we change $k + 1 - r_1 = 1$ zero to 1. Again, $s_2 = 2$, $r_2 = 3$, and $r_2 + s_2 = 5 > k$; hence we change $k + 1 - r_2 = 1$ zero to 1. Finally, $s_3 = 1$, $r_3 = 3$, and $r_3 + s_3 = 4 > k$, so that we change again $k + 1 - r_3 = 1$ zero to 1.

The work may be arranged as follows:

*	*	*	*
$1 \rightarrow 0$	1	1	$0 \rightarrow 1$
$1 \rightarrow 0$	1	$0 \rightarrow 1$	1
$1 \rightarrow 0$	$0 \rightarrow 1$	0	1
		1	1
	1	0	0
		1	0

and we have as a result the extraordinary position

$$\begin{array}{r}
 0111 < 1110 \\
 0111 < 1101 \\
 0101 < 1001 \\
 \quad 11 \\
 \quad 100 \\
 \quad \underline{10} \\
 \quad 444
 \end{array}$$

www.dbraulibrary.org.in

In the game we shall suppose P has a favorable opening move; namely, that he is confronted with an ordinary position. He will then leave Q an extraordinary position and, as we have shown, Q must leave P an ordinary position from which P can obtain an extraordinary position. This sequence of alternate events will continue until eventually some of the piles are 0. As long as the game is in progress, after P has played there are at least $k + 1$ piles of objects, since this is necessary for an extraordinary position. Hence Q is always faced with at least $k + 1$ piles and cannot win the game by removing all the objects. But the number of piles must eventually become less than $k + 1$, and since such a situation would result in an ordinary position, the next move must be that of P , and by removing all the objects he will win.

8. The Lure of Number Theory. The theory of numbers, unlike some other branches of mathematics, is a purely

theoretical science without practical applications. Some of the men who actually took part in promoting its limits even boast about this lack of application. One of the greatest representatives of number theory in the nineteenth century, Kummer, is said to have remarked on one occasion that of all his discoveries he appreciated ideal numbers most because they had not soiled themselves as yet with any practical applications.

What, then, compels men to spend a lot of time and effort on arithmetical investigations? Surely not the trivial properties of numbers such as those with which we have dealt in this chapter. They may amuse beginners and amateurs but not great mathematicians. Yet only very few among the great mathematicians did not work at one time or another in the theory of numbers. The answer is that the whole beauty of this science becomes apparent only to those who penetrate deep into it. That is exactly what Gauss wrote in one of his letters to a ^{www.dbraulibrary.org in} talented and learned lady, Sophie Germain: "Les charmes enchanteurs de cette science sublime ne se décèlent dans toute leur beauté qu'à ceux qui ont le courage de l'approfondir."

To penetrate deep means to discover and prove or at least to be able to understand recondite relations between numbers. Pierre de Fermat (1601-1665), who may be called the father of modern number theory, was the first man to discover really deep properties of numbers.

Fermat was an extraordinary man. A jurist by profession, he was also a great mathematician and an accomplished classical scholar. With Pascal he laid the foundations of the theory of probability, developed analytical geometry independently of Descartes, and was one of the founders of infinitesimal calculus. Yet his discoveries in number theory overshadow everything else he did. These discoveries he communicated mostly in letters to his contemporaries; some of them he jotted down in marginal notes on the copy of the Diophantus "Arithmetic" in his possession. But he never revealed his proofs and gave only very general

indications about his methods. Yet all of his theorems later were found true, with one exception, and one—the famous Fermat's Last Theorem—still remains unproved except in particular cases.

Just a few of Fermat's theorems will show what deep relations exist between numbers. At first sight there is no apparent relation between polygonal numbers and integers in general. Yet according to Fermat every integer is either triangular or the sum of 2 or 3 triangular numbers; every number is either a square or the sum of 2, 3, or 4 squares; either pentagonal or the sum of 2, 3, 4, or 5 pentagonal numbers; and so on. This is a truly deep property of numbers.

Nothing apparently links numbers which are sums of two squares and primes which exceed by one a multiple of four. Yet Fermat discovered that every such prime is the sum of two squares. For example:

$$5 = 1^2 + 2^2, \quad 13 = 3^2 + 2^2, \quad 41 = 5^2 + 4^2, \text{ etc.}$$

In relation to cubes and other powers, one might cite the so-called Waring's theorem, according to which every integer is the sum of not more than 9 positive cubes or 19 biquadrates, and so on.

On the subject of number theory, in the preface to the collected works of Eisenstein, Gauss said,

“A great part of its theories derives an additional charm from the peculiarity that important propositions, with the impress of simplicity upon them, are often easily discoverable by induction, and yet are of so profound a character that we cannot find their demonstration till after many vain attempts; and even then, when we do succeed, it is often by some tedious and artificial process, while the simpler methods may long remain concealed.”

It is natural that much preliminary study of things which are not so very interesting in themselves is required before one can appreciate some of the arithmetical treasures contained in later chapters of this book. But this is inescapable:

before learning to walk one first learns to crawl. With this admonition to the reader we pass, in the next and following chapters, to the systematic study of the elements of number theory.

Exercises and Problems

- Express $(3,847)_{10}$ in the binary system; in the ternary system.
- Express $(42,381)_{10}$ in the duodecimal system.
- Multiply $(641)_7$ by $(533)_7$. Divide $(2,806)_9$ by $(35)_9$.
- Extract the square root of $(341)_8$.
- The fraction $1\frac{16}{64}$ has the peculiar property that an incorrect cancellation, $\frac{16}{64}$, gives the correct answer. Find a similar pair of two digit numbers with this property, using the base 8. Could a similar pair be found using the base 7?
- Write all the extraordinary positions in the ordinary game of Nim when each pile has 5 or less counters.
- Show geometrically that every hexagonal number equals its rank plus four times the triangular number of preceding rank.
- Show geometrically that nine times a triangular number of rank n plus one is a triangular number with rank $3n + 1$.
- Show that a pentagonal number cannot end in 3, 4, 8, or 9.
- Prove that a hexagonal number cannot end in 2, 4, 7, or 9.
- Find at least two numbers, neither being unity, which are simultaneously square and triangular.
- A vendor had a quantity of eggs for sale. To his first customer he sold half of his eggs plus half an egg, to the second customer half of the eggs left plus half an egg, and continued to sell them in this manner. After serving six customers he had sold all of his eggs. How many did he have in the beginning?
- Determine a set of weights to be used on balancing scales with the weighing pan and the weight pan separate. The load varies from 1 to 63 pounds, and not more than 6 weights are to be used.
- Prove that every integer can be represented, and in one way only, in the form

$$3^a + \epsilon_1 3^{a-1} + \epsilon_2 3^{a-2} + \dots + \epsilon_a$$

where $\epsilon_1, \epsilon_2, \dots, \epsilon_a$ can have only three values: 0, +1, -1.

- Determine a set of four weights which make possible weighing loads from 1 to 40 pounds if weights can be placed on either of the pans. How can you generalize this problem?

16. Two numbers, for instance, 23 and 35, can be multiplied as follows: Divide 23 repeatedly by 2 as far as possible, always rejecting fractions; and correspondingly double the other number 35. As a result we have two columns of numbers:

A	B
23	<u>35</u>
11	<u>70</u>
5	<u>140</u>
2	<u>280</u>
1	<u>560</u>

Take the sum of numbers in column B to which correspond odd numbers in column A. Then the sum

$$35 + 70 + 140 + 560 = 805$$

gives the requested product of 23 by 35. By resorting to representation of numbers in the binary scale, prove that this rule is general.

www.dbraulibrary.org.in

Downloaded from www.dbraulibrary.org.in

CHAPTER II

DIVISIBILITY AND RELATED TOPICS

1. Theorems Concerning Divisibility. If a is a multiple of b ; that is, if there is an integer c such that $a = bc$, we say also that a is "divisible" by b , and that b is a "divisor" or a "factor" of a . Thus 12 is divisible by 3, since $12 = 3 \cdot 4$. Also we may say that 3 is a divisor of 12. If b is a divisor of a , then $-b$ will also divide a , so that positive and negative divisors occur always in pairs. For this reason usually only positive divisors are considered. From the concept of divisibility the following simple propositions follow immediately:

1. If a is divisible by c , then ab is divisible by c . For $a = cd$ where d is an integer by hypothesis; consequently $ab = (cd)b = (bd)c$, and so ab is divisible by c .

2. If a is divisible by b and b is divisible by c , then a is divisible by c . In other words, if b is a divisor of a , then every divisor of b is a divisor of a . For, by hypothesis, $a = bd$, $b = ce$, where d and e are integers. Consequently $a = (ce)d = (ed)c$, and a is divisible by c .

3. If both a and b are divisible by c , then $a \pm b$ is divisible by c . For $a = cd$, $b = ce$ with d, e integers. Hence

$$a \pm b = cd \pm ce = (d \pm e)c$$

is divisible by c .

Combining 1 and 3, we derive the following proposition:

4. If a, b, c, \dots, m are integers divisible by n and $\alpha, \beta, \gamma, \dots, \mu$ are arbitrary integers, then

$$a\alpha + b\beta + c\gamma + \dots + m\mu$$

is an integer divisible by n .

2. Common Divisors. Given an integer a , which can be assumed to be positive, we next consider the problem of finding all its divisors. As obvious divisors one always has 1 and a . To find others, if any, it suffices to test by actual division the remaining numbers 2, 3, . . . , $a - 1$ and see whether we find among them divisors of a . The problem thus can be solved in a finite number of steps, but this theoretical solution requires too many trials when applied to numbers which are somewhat large, and it is desirable to abridge it by eliminating trials which are a priori useless. In a later chapter we shall consider methods for reducing the number of trials considerably. It must suffice now to say that the problem of finding all the divisors of a given integer in practice may be very difficult when this integer is large and it is required to exhibit actually all of its divisors. Consider, for example, the number 100,895,598,169, which was sent to Fermat by Mersenne with a request for its divisors. It is a tribute to Fermat's ability that he was able to answer immediately that the number was the product of 898,423 and 112,303 both of which contain no smaller divisors other than 1.

In general, in number theory a problem is considered as solved when what is sought can actually be exhibited in a finite number of steps, but among various methods of solving the same problem those which require a smaller number of trials are considered more nearly perfect.

A number which divides several integers is called their "common divisor." For instance, 2 and 3 are common divisors of 12, 30, 72, and 120. The problem of finding all common divisors of several integers can be reduced to the previously considered problem of finding all the divisors of a single integer. In fact we shall prove presently that among the common divisors of several integers there is one, say D , such that every other common divisor is a divisor of D and, vice versa, every divisor of D is a common divisor of the given

integers. The particular common divisor D for obvious reasons is called the "greatest common divisor" (abbreviated g.c.d.). If the given integers are denoted by a, b, c, \dots, m we shall consistently denote their g.c.d. by the symbol (a, b, c, \dots, m) . Thus

$$(12, 30, 72, 120) = 6.$$

In fact, by actual trial we find that all the divisors of 12 are 1, 2, 3, 4, 6, 12. Of them only 1, 2, 3, 6 divide the remaining numbers 30, 72, 120. Again the common divisors 1, 2, 3 divide 6; hence 6 is the g.c.d. of 12, 30, 72, and 120.

3. Euclid's Algorithm. In order to prove the existence of the greatest common divisor, we shall consider first the case of two integers a and b , and we shall use the process of successive divisions known as "Euclid's Algorithm," for it occurs in Euclid's "Elements," Book VII, Prop. 2.

The word algorithm, like several other mathematical expressions, comes from the Arabic name *al-Khwarizmi* of Al Khowarizmi, the name of an Arabian mathematician of the ninth century, whose writings were prominent in bringing the present method of numeration to the Occident. During the middle ages the word algorithm referred simply to the use of Hindu-Arabic numerals, but at present it applies to any formalized procedure whereby requested mathematical objects are found by a definite chain of operations, each operation requiring the results of preceding ones.

Let $a > b$ and $b > 0$. Dividing a by b , suppose we get the quotient q_1 and the remainder b_1 , so that

$$a = bq_1 + b_1; \quad 0 \leq b_1 < b.$$

Now, if $b_1 = 0$ the operations are ended. If, however, $b_1 > 0$, we can go one step further, dividing b by b_1 and obtaining

$$b = b_1q_2 + b_2; \quad 0 \leq b_2 < b_1$$

where q_2 is the quotient and b_2 the remainder of the division. If it happens that $b_2 = 0$, the operations are ended; otherwise we go one step further by dividing b_1 by b_2 and obtaining

$$b_1 = b_2q_3 + b_3; \quad 0 \leq b_3 < b_2.$$

Unless $b_3 = 0$, in which case the process ends, we can go one step further, dividing b_2 by b_3 , and can continue this as long as remainders in successive divisions are positive.

Now

$$b > b_1 > b_2 > b_3 > \dots$$

is a sequence of decreasing positive integers which cannot be continued indefinitely; consequently Euclid's process must end, and this happens only when we come to a certain remainder b_n which divides the immediately preceding remainder b_{n-1} , so that

$$b_{n-1} = b_nq_{n+1}$$

where q_{n+1} is an integer. As a result we have the following system of equations:

$$\begin{aligned} a &= bq_1 + b_1 \\ b &= b_1q_2 + b_2 \\ b_1 &= b_2q_3 + b_3 \\ &\text{www.dbraulibrary.org.in} \\ b_{n-2} &= b_{n-1}q_n + b_n \\ b_{n-1} &= b_nq_{n+1}. \end{aligned} \tag{1}$$

Now b_n divides b_{n-1} ; dividing $b_{n-1}q_n$ and b_n , it will divide b_{n-2} (by (4), Sec. 1). Again, as b_n divides b_{n-1} and b_{n-2} , it will divide b_{n-3} . Continuing the same reasoning and advancing upward in the set of equations (1), we finally come to the conclusion that b_n divides a and b . Thus b_n is a common divisor of a and b . Now let c be any common divisor of a and b . Dividing a and b , it will divide $b_1 = a - bq_1$ (by (4), Sec. 1). Again, as c divides b and b_1 it will divide b_2 ; continuing the same reasoning and descending downward in the set of equations (1), we conclude finally that c divides b_n . Thus b_n , being a common divisor of a and b , is divisible by any common divisor of these numbers. Consequently b_n is the greatest common divisor of a and b .

Example. Find the g.c.d. of 78,696 and 19,332. By applying Euclid's algorithm, as described above, we have

$$\begin{aligned} 78,696 &= 19,332 \cdot 4 + 1,368 \\ 19,332 &= 1,368 \cdot 14 + 180 \\ 1,368 &= 180 \cdot 7 + 108 \\ 180 &= 108 \cdot 1 + 72 \\ 108 &= 72 \cdot 1 + 36 \\ 72 &= 36 \cdot 2. \end{aligned}$$

Consequently the g.c.d. of 78,696 and 19,332 is 36. All other common divisors are divisors of 36; by trials we find that these divisors are

$$1, 2, 3, 4, 6, 9, 12, 18, 36.$$

Euclid's algorithm, as to expediency and convenience, leaves nothing to be desired. All unnecessary trials are eliminated in it except unavoidable trials which occur in the process of division. It affords an example of an ideal solution of a number-theoretic problem.

4. Greatest Common Divisor of More Than Two Numbers.

Let us consider now three numbers a, b, c . Take two of them, for example, a and b , and let D be their g.c.d. Now any common divisor of a, b, c , because it divides a and b , must be a divisor of D . Being a divisor of D and c , it will divide their g.c.d.

$$D_1 = (D, c).$$

But D_1 , dividing D and c , will itself be a common divisor of a, b, c . Thus not only does D_1 divide a, b, c , but any common divisor of the three divides D_1 ; consequently D_1 is the g.c.d. of a, b, c . It can be found by Euclid's algorithm in two steps: first we determine $D = (a, b)$ and next $D_1 = (D, c)$.

Suppose we have four numbers a, b, c, d and let $D_1 = (a, b, c)$. Every common divisor of a, b, c, d is a common divisor of a, b, c and consequently divides D_1 ; but dividing d and D_1 , it divides their g.c.d.

$$D_2 = (D_1, d).$$

But D_2 , dividing D_1 and d , is a common divisor of a, b, c, d ; hence D_2 is the g.c.d. of a, b, c, d . It can be found by Euclid's algorithm in three steps: First we determine $D = (a, b)$, next $D_1 = (D, c)$, and finally $D_2 = (D_1, d)$. It is clear that in the same manner we can deal with 5, 6, and more numbers. In general, if we have n numbers a, b, c, \dots, k, l , we can determine their g.c.d. in $n - 1$ steps; that is, we determine successively

$$D = (a, b); \quad D_1 = (D, c); \quad D_2 = (D_1, d); \quad \dots ; \\ D_{n-3} = (D_{n-4}, k); \quad D_{n-2} = (D_{n-3}, l)$$

and D_{n-2} will be the g.c.d. of a, b, c, \dots, k, l .

Example. Find the g.c.d. of 1,932, 476, 952, 504, 9,261. By applying Euclid's algorithm four times, we find

$$(476, 1,932) = 28; \quad (28, 952) = 28; \quad (28, 504) = 28; \\ (28, 9,261) = 7;$$

consequently $(476, 504, 952, 1,932, 9,261) = 7$.

NOTE. To avoid possible misunderstanding it must be remembered that in establishing the existence of the g.c.d. of several numbers we assume that none of them is 0. The number 0 is divisible by any integer; consequently if we adjoin 0 to the numbers a, b, \dots, k , none of which is 0, then

$$(a, b, c, \dots, k, 0) = (a, b, c, \dots, k).$$

In particular $(a, 0) = a$ and $(1, 0) = 1$.

5. Theorems Concerning Common Divisors. Euclid's algorithm not only enables us to find the g.c.d. of several numbers but also proves useful as a basis of the proof of some important theorems which we shall now proceed to consider.

THEOREM 1. If two numbers a and b with g.c.d. D are multiplied by a positive integer m , then the g.c.d. of ma and mb will be mD . In other words

$$(ma, mb) = m(a, b).$$

PROOF. The proof is based on a very simple remark: If on dividing a by b we get the quotient q and remainder r , so that

$$a = bq + r,$$

then on dividing ma by mb we have the same quotient but the remainder will be mr . In fact we have

$$ma = mbq + mr$$

and $0 \leq mr < mb$, so that mr is the remainder in the division of ma by mb . Now suppose that after applying Euclid's algorithm to a and b we get the following set of equations:

$$\begin{aligned} a &= bq_1 + b_1 \\ b &= b_1q_2 + b_2 \\ &\dots\dots\dots \\ b_{n-1} &= b_nq_{n+1}. \end{aligned}$$

On multiplying them by m , we have

$$\begin{aligned} ma &= mbq_1 + mb_1 \\ mb &= mb_1q_2 + mb_2 \\ &\dots\dots\dots \\ mb_{n-1} &= mb_nq_{n+1}. \end{aligned} \tag{2}$$

But according to the previous remark, mb_1 is the remainder in the division of ma by mb ; mb_2 is the remainder in the division of mb by mb_1 ; etc. Consequently (2) is the set of equations in Euclid's algorithm applied to ma and mb and $mb_n = (ma, mb)$. But $b_n = (a, b)$; hence the theorem is proved.

THEOREM 2. Let m be a common divisor of a and b ; then

$$\left(\frac{a}{m}, \frac{b}{m}\right) = \frac{(a, b)}{m}.$$

PROOF. Let

$$\left(\frac{a}{m}, \frac{b}{m}\right) = x;$$

then, since $a = m\frac{a}{m}$, $b = m\frac{b}{m}$ by Theorem 1,

$$(a, b) = mx$$

and

$$x = \frac{(a, b)}{m},$$

which proves the theorem.

COROLLARY. Let d be the g.c.d. of a and b . By Theorem 2 the g.c.d. of a/d and b/d will be 1. Now two numbers with g.c.d. = 1 are called "relatively prime" numbers. Hence when two numbers are divided by their g.c.d., the resulting quotients will be relatively prime.

The value of the fraction a/b is not changed when its numerator and denominator are divided by one of their common divisors. Dividing a and b by their g.c.d., we get the relatively prime quotients α and β . Hence any fraction a/b may be replaced by an irreducible fraction α/β in which the numerator and denominator are relatively prime.

THEOREM 3. If several numbers a, b, c, \dots, k are multiplied by the same integer m , then

$$(ma, mb, mc, \dots, mk) = m(a, b, c, \dots, k).$$

PROOF. It suffices to consider three numbers a, b, c . To find $D_1 = (a, b, c)$ we seek in succession $D = (a, b)$ and $D_1 = (D, c)$. Now, by Theorem 1, $(ma, mb) = mD$, and by the same theorem $(mD, mc) = mD_1$; consequently

$$(ma, mb, mc) = mD_1,$$

which was to be shown.

THEOREM 4. Let m be a common divisor of several integers a, b, c, \dots, k ; then

$$\left(\frac{a}{m}, \frac{b}{m}, \frac{c}{m}, \dots, \frac{k}{m}\right) = \frac{(a, b, c, \dots, k)}{m}.$$

PROOF. This theorem follows from Theorem 3 in the same manner that Theorem 2 follows from Theorem 1.

COROLLARY. Several numbers are said to be *without common divisor* (meaning without common divisor > 1) if their g.c.d. = 1. From Theorem 4 it follows that, on dividing several numbers by their g.c.d., the resulting quotients will be numbers without common divisors.

6. The Fundamental Theorem of Arithmetic. From theorems established in Sec. 5, it is easy to deduce a theorem which is rightly called the fundamental theorem of arithmetic:

THEOREM 5. If the product ab of two integers is divisible by an integer c , and c and b are relatively prime, then a is divisible by c .

PROOF. Since

$$(b, c) = 1,$$

by Theorem 1 we have

$$(ab, ac) = a.$$

Now c divides ab (by hypothesis), and ac , that is, c , is a common divisor of ab and ac . Consequently it divides their greatest common divisor, which is a .

THEOREM 6. Each of the numbers a, b, c, \dots, e, f being relatively prime to m , their product will be relatively prime to m , also.

PROOF. Consider first two numbers a, b which are both relatively prime to m ; that is,

$$(a, m) = 1, \quad (b, m) = 1.$$

By Theorem 1

$$(ab, mb) = b.$$

The g.c.d. of ab and m will be a common divisor of ab and mb and consequently will divide b . But being a common divisor of b and m it must divide 1; hence $(ab, m) = 1$. If there are three numbers a, b, c each of which is relatively prime to

m , their product abc may be considered as a product of two factors ab and c . Now it has been proved already that ab and m are relatively prime numbers and c is relatively prime to m by hypothesis; consequently $(ab)c = abc$ is relatively prime to m . By proceeding in the same way, the proof can be extended to any number of factors.

THEOREM 7. If each of the numbers a, b, c, \dots, e, f is relatively prime to each of the numbers $\alpha, \beta, \gamma, \dots, \lambda$, then $abc \dots ef$ is relatively prime to $\alpha\beta\gamma \dots \lambda$.

PROOF. By Theorem 6 the product $abc \dots ef$ is relatively prime to each of the numbers $\alpha, \beta, \gamma, \dots, \lambda$. By the same theorem $\alpha\beta\gamma \dots \lambda$ will be relatively prime to $abc \dots ef$.

COROLLARY. If we agree that all the numbers a, b, c, \dots, e, f are equal and their number is m ; and also if all the numbers $\alpha, \beta, \gamma, \dots, \lambda$ are equal and their number is n , then from Theorem 7 it follows immediately that since a and α are relatively prime numbers their powers a^m and α^n will be relatively prime also.

This corollary may be used to prove that a root of any power n of a positive integer A is either an integer or an irrational number. For suppose that this root is represented by the irreducible fraction r/s . Then

$$\left(\frac{r}{s}\right)^n = A \quad \text{or} \quad r^n = As^n,$$

whence it follows that r^n is divisible by s and consequently $(r^n, s) = s$. But by the corollary $(r^n, s) = 1$ and so $s = 1$, $A = r^n$, that is, A is an n th power of an integer. Consequently if A is not an n th power of an integer, $\sqrt[n]{A}$ must be an irrational number.

The following theorem will find frequent applications:

THEOREM 8. If a and b are relatively prime positive integers and their product is an exact power c^n of an integer, then a and b themselves are exact n th powers.

By hypothesis

$$ab = c^n.$$

Let $(a, c) = \alpha$ and $a = \gamma\alpha$, $c = \beta\alpha$, where, by the corollary to Theorem 2, Sec. 5, γ and β are relatively prime integers. After substitution and cancellation of α , we have

$$\gamma b = \beta^n \alpha^{n-1}.$$

But γ and β^n are relatively prime numbers and β^n divides γb . By the fundamental theorem, β^n must divide b , and we can set

$$b = \beta^n d.$$

On substituting this expression for b and cancelling β^n , we get

$$\gamma d = \alpha^{n-1}.$$

Now α and d must be relatively prime numbers, for their g.c.d. divides a and b and consequently must equal 1, since a and b are relatively prime. Since α^{n-1} divides γd and is relatively prime to d , it must divide γ , so that we can set

$$\gamma = \alpha^{n-1} \epsilon.$$

On substituting this expression into

$$\gamma d = \alpha^{n-1}$$

and cancelling α^{n-1} , we have

$$\epsilon d = 1,$$

whence $\epsilon = d = 1$ since ϵ and d are positive integers. Finally

$$a = \gamma\alpha = \alpha^n, \quad b = d\beta^n = \beta^n$$

and

$$c = \alpha\beta.$$

NOTE. If the signs of a and b are not specified but it is expressly assumed that $c \neq 0$, then from the preceding proof it follows only that

$\epsilon = d = \pm 1$. In other words, if $ab = c^n$, $c \neq 0$, and a and b are relatively prime, then two integers α, β can be found such that

$$c = \alpha\beta, \quad a = \pm\alpha^n, \quad b = \pm\beta^n$$

with signs corresponding.

7. Common Multiples. A number which is divisible by each of the given integers a, b, c, \dots, f is called their "common multiple." For instance 60 is a common multiple of 2, 3, 5, 15, 20, 30. Let us first consider common multiples of two integers a and b . If x is one of them, it must be divisible by a , and we can set

$$x = ak$$

where the integer k must be so chosen as to make ak divisible by b . Now let d be the g.c.d. of a and b and

$$a = \alpha d, \quad b = \beta d.$$

Since $ak = d\alpha k$ is divisible by βd , αk must be divisible by β . To fulfill this condition it is necessary (by Theorem 5, Sec. 6) and sufficient that k should be a multiple of β , say

$$k = \beta t,$$

where t is an arbitrary integer. Thus the general expression for all the multiples of a and b is

$$x = a\beta t = \frac{ab}{d}t,$$

where t is an arbitrary integer. The particular common multiple of a and b ,

$$M = \frac{ab}{d},$$

is numerically the smallest excepting the trivial multiple 0. It is called the "least common multiple" (abbreviated l.c.m.) of a and b , and from the general expression for common multi-

ples it is apparent that all the common multiples of a, b are multiples of their least common multiple M , which we shall also denote by the symbol $[a, b]$.

Now we turn to the consideration of the common multiples of three integers a, b, c . Any such multiple, being a multiple of a and b , is a multiple of their l.c.m. $[a, b] = M$. But since it is also a multiple of c , it will be a common multiple of M and c ; that is, a multiple of the l.c.m. $M_1 = [M, c]$ of M and c . Now M_1 is a particular common multiple of a, b, c and of all such multiples numerically the smallest. It is called the l.c.m. of a, b, c and will conveniently be denoted by the symbol $[a, b, c]$.

Other common multiples of a, b, c are multiples of their l.c.m. Let us take the case of four numbers a, b, c, d . Any common multiple of a, b, c, d , being a multiple of a, b, c , is a multiple of $M_1 = [a, b, c]$ and d ; consequently it is a multiple of $M_2 = [M_1, d]$. The number M_2 is a common multiple of a, b, c, d and of all such multiples numerically the smallest. It is the l.c.m. of a, b, c, d and will be denoted by the symbol $[a, b, c, d]$. Evidently the same reasoning may be extended to 5, 6, and any number of integers. In general n given integers a, b, c, \dots, j, k possess the least common multiple $[a, b, c, \dots, j, k]$, which can be determined as the last in the sequence of numbers

$$M = [a, b], \quad M_1 = [M, c], \quad M_2 = [M_1, d], \quad \dots, \\ M_{n-3} = [M_{n-4}, j], \quad M_{n-2} = [M_{n-3}, k].$$

Example. Find the l.c.m. of 6, 14, 18, 30. We find successively

$$\begin{aligned} (6, 14) &= 2 & [6, 14] &= \frac{6 \cdot 14}{2} = 42 \\ (18, 42) &= 6 & [18, 42] &= \frac{18 \cdot 42}{6} = 126 \\ (30, 126) &= 6 & [30, 126] &= \frac{30 \cdot 126}{6} = 630. \end{aligned}$$

The l.c.m. of 6, 14, 18, 30 is therefore 630.

One particular case deserves special consideration. When the integers are *relatively prime in pairs*; that is, when each two of them are relatively prime, the l.c.m. of them is equal to their product. To prove this take the case of four integers a, b, c, d . Since $(a, b) = 1$, we have $M = ab$. Again, a and b being relatively prime to c , we have $(ab, c) = (M, c) = 1$ and $M_1 = [M, c] = abc$. Further $(abc, d) = (M_1, d) = 1$, and consequently $M_2 = abcd$, but $M_2 = [a, b, c, d]$.

Combining this remark with the fact that any common multiple is divisible by the l.c.m., we can draw the following often used conclusion: An integer which is divisible by each of the numbers a, b, c, \dots, k , which are relatively prime in pairs, is divisible by their product.

NOTE. The case of integers relatively prime in pairs should be distinguished from the case of integers without common divisors. For instance, 2, 4, 6, 9 are integers without common divisors, but not relatively prime in pairs.

8. Solution of $x^2 + y^2 = z^2$ in Integers. In very remote times ancient Egyptians and Chinese were familiar with a right-angle triangle whose sides had as lengths the integers 3, 4, 5, and they used this fact for the construction of right angles in their surveying operations by stretching in a proper manner either three ropes of the respective lengths or one rope with knots marking off proper spacings. Later the general problem of finding right-angle triangles whose sides are expressed by integers was a favorite one with Pythagoreans and later Greek geometers. Ancient tradition attributes to Pythagoras himself a solution expressed by the numbers

$$\frac{n^2 - 1}{2}, n, \frac{n^2 + 1}{2}$$

where n is an arbitrary odd integer > 1 . The problem, by virtue of the Pythagorean theorem, amounts to finding all

systems of positive integers x, y, z which satisfy the "Pythagorean equation"

$$x^2 + y^2 = z^2. \quad (A)$$

It suffices to consider only *primitive* solutions; that is, solutions consisting of integers without common divisors. For, from a primitive solution a, b, c , by multiplying these numbers by an arbitrary integer M , we derive another solution

$$x = Ma, \quad y = Mb, \quad z = Mc$$

with M as the g.c.d. of x, y, z . Conversely, each nonprimitive solution can be derived from some primitive solution in this manner. For, if M is the g.c.d. of x, y, z , we can set

$$x = Ma, \quad y = Mb, \quad z = Mc$$

and then

$$a^2 + b^2 = c^2$$

where a, b, c are numbers without common divisors. Thus, seeking solutions of equation (A), we can confine ourselves to numbers without common divisors. Integers x, y, z will then be relatively prime in pairs; for consider the pair x, y and let d be the g.c.d. of x and y . Since d^2 divides the left-hand side of (A), z^2 will be divisible by d^2 and consequently z will be divisible by d . Hence x, y, z are divisible by d ; however, the greatest common divisor of x, y, z is 1 and so $d = 1$. Similarly we can prove that x, z and y, z are two pairs of relatively prime numbers. Since x and y are relatively prime they cannot be both even, but neither can they both be odd.

The proof of the latter statement is based on a property of odd integers which, simple though it is, must be stated here explicitly. If a is an odd integer, we can set $a = 2n + 1$; then

$$a^2 = 1 + 4n(n + 1).$$

But of two consecutive integers n and $n + 1$, one is even: hence the product $n(n + 1)$ is divisible by 2, and $4n(n + 1)$ is an integer divisible by 8, say $8N$. Consequently

$$a^2 = 1 + 8N;$$

that is, the square of an odd integer, when divided by 8, leaves the remainder 1.

Now suppose that, in equation (A), x and y are both odd. Then

$$x^2 = 1 + 8P, \quad y^2 = 1 + 8Q$$

and

$$z^2 = x^2 + y^2 = 2 + 8R.$$

This shows that z must be even, but the square of an even number is divisible by 4, whereas $2 + 8R$ is not divisible by 4. Of the two numbers x, y , therefore, one is odd and the other even. Without loss of generality we may suppose that y is even, x odd, and z necessarily odd. Now equation (A) can be written as follows:

$$\frac{z+x}{2} \cdot \frac{z-x}{2} = \left(\frac{y}{2}\right)^2.$$

Integers $\frac{z+x}{2}, \frac{z-x}{2}$ are relatively prime because their g.c.d. divides the two relatively prime integers

$$\frac{z+x}{2} + \frac{z-x}{2} = z, \quad \frac{z+x}{2} - \frac{z-x}{2} = x.$$

Moreover they are both positive because they have the same sign and the first of them is positive. By Theorem 8, Sec. 6, we conclude that

$$\frac{z+x}{2} = r^2, \quad \frac{z-x}{2} = s^2, \quad \frac{y}{2} = rs,$$

whence

$$x = r^2 - s^2, \quad y = 2rs, \quad z = r^2 + s^2.$$

Here r and s are two positive integers, necessarily relatively prime and of different parity; moreover, $r > s$. Conversely, with r, s subject to these conditions, x, y, z will constitute a primitive solution of equation (A). That this equation is satisfied follows from the identity

$$(r^2 - s^2)^2 + (2rs)^2 = (r^2 + s^2)^2.$$

Furthermore x, y, z will be positive integers, and it remains to show that they are without common divisors. Let d be their g.c.d.; then d will divide the numbers

$$z + x = 2r^2, \quad z - x = 2s^2, \quad y = 2rs.$$

But $(r^2, s^2, rs) = 1$, since r^2 and s^2 are relatively prime; hence $(2r^2, 2s^2, 2rs) = 2$, and it follows that d divides 2; that is, $d = 1$ or $d = 2$. But d cannot be 2, since z and x are odd; the only remaining possibility is $d = 1$.

From the discussion it follows that all the primitive solutions of the Pythagorean equation (or primitive Pythagorean triangles) are given by the aid of the formulas

$$x = r^2 - s^2, \quad y = 2rs, \quad z = r^2 + s^2$$

where r and s are any two relatively prime numbers of different parity and $r > s$. As an example, we see that when $r = 2, s = 1$, the result gives the Egyptian triangle 3, 4, 5.

Exercises and Problems

1. The g.c.d. of $a + b$ and $a - b$ is either 1 or 2 if $(a, b) = 1$.
2. Show that the fraction $\frac{a + a'}{b + b'}$ is expressed in simplest terms if $ab' - a'b = \pm 1$.
3. If $\alpha, \beta, \gamma, \delta$ are four integers and $\alpha\delta - \beta\gamma = \pm 1$, then the g.c.d. of the numbers

$$\begin{aligned} m &= \alpha a + \beta b \\ n &= \gamma a + \delta b \end{aligned}$$

is the same as that of a and b .

4. The g.c.d. of $a + b$ and $a^2 - ab + b^2$ is either 1 or 3 if $(a, b) = 1$.
5. Show that $(a + b, a - b, ab) = 1$ if $(a, b) = 1$.
6. Show that $a^2 - ab + b^2$ and $a^4 - a^3b + a^2b^2 - ab^3 + b^4$ are relatively prime if $(a, b) = 1$.
7. Two distinct numbers of the form $a^{2^n} + 1$, $a^{2^m} + 1$ are relatively prime if a is even, and have the g.c.d. 2 if a is odd.
8. Make a table of all the primitive right triangles in integers for which the hypotenuse does not exceed 100.
9. The sum of two numbers is 5,432 and their l.c.m. is 223,020. Find the numbers. Ans. 1,652 and 3,780.
10. Let s^2 be the greatest square which divides a . Show that if d^2 is any square dividing a , then s is divisible by d .
11. The sum of two fractions

$$\frac{a}{b} + \frac{c}{d}$$

in lowest terms cannot be an integer unless $b = d$.

12. Show that the most general solution of the equation $ab = cd$ in integers, provided $(a, b) = 1$, $(c, d) = 1$, is given by

$$\begin{matrix} a = \alpha\beta & b = \gamma\delta \\ c = \alpha\gamma & d = \beta\delta \end{matrix} \text{ org.in}$$

where $\alpha, \beta, \gamma, \delta$ are arbitrary integers relatively prime in pairs.

13. Show that the sum

$$1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{n}$$

for $n > 1$ is never an integer. *Indication of Proof:* Let $2^\alpha(2k + 1)$ be that number of the sequence 2, 3, . . . n which is divisible by the highest power of 2. There cannot be another number in the same sequence divisible by 2^α .

14. The sum

$$\frac{1}{p} + \frac{1}{p+1} + \dots + \frac{1}{p+n}$$

is a fraction which, when reduced to simplest terms, has an even denominator.

15. Show that in the series of Fibonacci,

$$1, 2, 3, 5, 8, 13, 21, 34, \dots,$$

in which each term is the sum of two preceding terms, two consecutive terms are always relatively prime.

16. Ancient Egyptians used to represent fractions as sums of unit fractions; that is, fractions with the numerator = 1. One method of doing this can be based upon the following remark: Let a/b be a fraction in simplest terms with its denominator > 1 . If $1/x$ is the largest unit fraction contained in a/b , then

$$\frac{a}{b} = \frac{1}{x} + \frac{a'}{b'}$$

where a'/b' is a fraction in simplest terms and $a' < a$. Represent in the Egyptian manner the following fractions $59/70$, $327/512$, $67/140$.

17. Find formulas exhibiting all the primitive solutions of the equation

$$x^2 + 2y^2 = z^2$$

with positive z .

$$\text{Ans. } x = \pm(r^2 - 2s^2), y = 2rs, z = r^2 + 2s^2; (r, 2s) = 1.$$

18. Do the same for the equation

$$x^2 + 3y^2 = z^2.$$

Ans.

$$(a) \ x = \pm(r^2 - 3s^2), y = 2rs, z = r^2 + 3s^2; r, s \text{ integers of different parity and } (r, 3s) = 1.$$

$$(b) \ x = \pm \frac{r^2 - 3s^2}{2}, y = rs, z = \frac{r^2 + 3s^2}{2}; r, s \text{ odd integers and } (r, 3s) = 1.$$

Downloaded from www.dl.ac.uk

CHAPTER III

EUCLID'S ALGORITHM AND DIOPHANTINE EQUATIONS OF THE FIRST DEGREE

1. Lamé's Theorem. A little practice with the Euclidean algorithm is sufficient to convince anyone of its expediency. The number of divisions required to find the g.c.d. of two numbers, even when these numbers are large, is small in comparison with the magnitude of the numbers. This observation naturally leads one to wonder whether it is possible to establish a priori the limit for the number of operations which are necessary to find the greatest common divisor. The answer to this inquiry is given by a theorem due to Lamé.

Gabriel Lamé (1795–1870) was an outstanding French mathematician and engineer chiefly known for his important contributions to mathematical physics. Though not primarily interested in number theory he left a few neat contributions to this branch of mathematics.

LAMÉ'S THEOREM. The number of divisions required to find the g.c.d. of two numbers is never greater than five times the number of digits in the smaller number.

PROOF. Let

$$a = bq_1 + b_1$$

$$b = b_1q_2 + b_2$$

$$\dots \dots \dots$$

$$b_{n-2} = b_{n-1}q_n + b_n$$

$$b_{n-1} = b_nq_{n+1}$$

be the set of divisions in Euclid's algorithm applied to the numbers a and b ($a > b$). The number of required divisions

is $n + 1$. Quotients q_1, q_2, \dots, q_n are all ≥ 1 , but the last quotient q_{n+1} is ≥ 2 , since $b_{n-1} > b_n$. Thus the preceding set of equations implies the set of inequalities

$$b_n \geq 1, \quad b_{n-1} \geq 2b_n, \quad b_{n-2} \geq b_{n-1} + b_n, \\ b_{n-3} \geq b_{n-2} + b_{n-1}, \quad \dots, \quad b \geq b_1 + b_2.$$

Now consider the Fibonacci series

$$u_1 = 1, \quad u_2 = 2, \quad u_3 = 3, \quad u_4 = 5, \quad \dots$$

in which the first two numbers are 1 and 2 and each following term is the sum of the preceding two, so that in general

$$u_n = u_{n-1} + u_{n-2}.$$

We have

$$b_n \geq u_1, \quad b_{n-1} \geq u_2$$

and

$$b_{n-2} \geq b_{n-1} + b_n \geq u_1 + u_2 = u_3.$$

Again,

$$b_{n-3} \geq b_{n-2} + b_{n-1} \geq u_2 + u_3 = u_4,$$

and so in general

$$b_{n-k} \geq u_{k+1};$$

consequently

$$u_{n+1} \leq b,$$

and this inequality will serve to establish an upper limit for the number of divisions $n + 1$.

Let us compare Fibonacci's numbers

$$1, 2, 3, 5, 8, \dots$$

to the powers

$$1, \xi, \xi^2, \xi^3, \xi^4, \dots$$

of the root

$$\xi = \frac{1 + \sqrt{5}}{2}$$

of the equation

$$\xi^2 = \xi + 1.$$

In the first place $\xi < 2$; consequently

$$\xi^2 = \xi + 1 < u_2 + u_1 = u_3.$$

Again,

$$\xi^3 = \xi^2 + \xi < u_3 + u_2 = u_4,$$

and so, in general,

$$\xi^k < u_{k+1}.$$

The inequality

$$u_{n+1} \leq b$$

implies

$$\xi^n < b,$$

whence

$$n < \frac{\log b}{\log \xi}.$$

But if the number of digits of b is p , then

$$b < 10^p, \quad \log b < p,$$

and on the other hand

$$\log \xi > \frac{1}{5};$$

hence

$$n < 5p$$

and $n + 1 \leq 5p$. This completes the proof of Lamé's theorem.

2. The Least-remainder Algorithm. Euclid's algorithm is based on the remark that, given two integers a and $b > 0$, we can set

$$a = bq + r,$$

where $0 \leq r < b$. Admitting negative remainders, we can arrange the division so as to have

$$a = b(q + 1) - (b - r)$$

with a negative remainder $-(b - r)$, which will be less than b numerically provided $r > 0$. And the division can always be arranged so as to give a positive or negative remainder numerically not exceeding $\frac{1}{2}b$, for of two numbers r and $b - r$ one at least is $\leq \frac{1}{2}b$, and they both can attain this limit only if $r = \frac{1}{2}b$. Thus, when a is not divisible by b , choosing $\epsilon = \pm 1$ arbitrarily, we can set

$$a = bq + \epsilon r$$

where $0 < r < b$. With a proper choice of ϵ we can make $r \leq \frac{1}{2}b$, and such a division may be called "division with the least remainder." From these remarks it is evident that Euclid's algorithm can be modified by allowing in each division either positive or negative remainders. Thus the general scheme of Euclid's algorithm will be represented by a set of equations

$$\begin{aligned} a &= bq_1 + \epsilon_1 b_1 \\ b &= b_1 q_2 + \epsilon_2 b_2 \\ &\dots \dots \dots \\ b_{m-2} &= b_{m-1} q_m + \epsilon_m b_m \\ b_{m-1} &= b_m q_{m+1} \end{aligned}$$

where $\epsilon_1, \epsilon_2, \dots, \epsilon_m$ are positive or negative units, as we please, and $b > b_1 > b_2 > \dots > b_m > 0$.

Of the possible arrangements of Euclid's algorithm, that in which the least remainders are always used is especially important. We shall call such an arrangement the "least remainder algorithm" (abbreviated L.R.A.). For instance, the following two schemes represent the ordinary method and the L.R.A.:

253 = 122 · 2 + 9	253 = 122 · 2 + 9
122 = 9 · 13 + 5	122 = 9 · 14 - 4
9 = 5 · 1 + 4	9 = 4 · 2 + 1
5 = 4 · 1 + 1	4 = 1 · 4
4 = 1 · 4	

The L.R.A. in the above example, and in all others we may try, certainly is not longer than the ordinary algorithm. That this is a general and valuable property of the L.R.A. was stated first by Kronecker. Presently we shall prove this property of the L.R.A., but at first it is necessary to establish an auxiliary proposition.

Leopold Kronecker (1823-1891) was one of the greatest representatives of algebra and number theory in the nineteenth century.

3. Lemma. Let a and a_1 be positive integers and $2a_1 \leq a$. Then the L.R.A. for the pair a, a_1 is not longer than the L.R.A. for the pair a and $a - a_1$.

PROOF. Suppose, at first, $a = 2$; then necessarily $a_1 = 1$. Then the least remainder algorithms for the two pairs will coincide, since the pairs are identical. Let $a = 3$; then the only choice for a_1 is 1, and the L.R.A. for the pairs 3, 1 and 3, 2 are respectively

$$\begin{aligned} 3 &= 1 \cdot 3 + 0, & 3 &= 1 \cdot 2 + 1 \\ 2 &= 1 \cdot 2 + 0 \end{aligned}$$

the first being shorter. Next take $a = 4$; then $a_1 = 1$ or $a_1 = 2$. In the latter case the two algorithms are again identical. For the pairs 4, 1 and 4, 3 they are respectively

$$\begin{aligned} 4 &= 4 \cdot 1 + 0; & 4 &= 3 \cdot 1 + 1 \\ 3 &= 1 \cdot 3 + 0 \end{aligned}$$

and the first is shorter again.

We have shown the lemma is true when $a = 2, 3, 4$. Suppose now that this lemma has been verified for *all* values of a which are *less* than a given number L . Then, if we can prove that the lemma is true when $a = L$, it will be proved to be universally true. For, when this crucial point has been established, we may take $a = 5$, and the lemma will be true since it is true for $a = 2, 3, 4$. Being true for $a = 2, 3, 4, 5$, it will be true for $a = 6$, and so on.

Now suppose that $a = L$, $2a_1 \leq L$, and let the beginning of the L.R.A. for a, a_1 be

$$a = a_1q_1 + \epsilon_1a_2, \quad 2a_2 \leq a_1.$$

As to the beginning of the L.R.A. for the pair $a, a - a_1$, we have to distinguish two cases: $a \geq 3a_1$ and $a < 3a_1$.

Case 1. $a \geq 3a_1$. The first step in the L.R.A. for the pair $a, a - a_1$ is

$$a = (a - a_1)1 + a_1$$

since

$$2a_1 \leq a - a_1$$

by hypothesis. The next step will lead to

$$a - a_1 = a_1(q_1 - 1) + \epsilon_1a_2,$$

and from this point the L.R.A. for both pairs a, a_1 and $a, a - a_1$ will be identical. Thus in Case 1 the L.R.A. for a, a_1 is shorter than that for $a, a - a_1$.

Case 2. $a < 3a_1$. This case must be subdivided into two subcases: $2a$, when $a < \frac{5}{2}a_1$, and $2b$, when $a \geq \frac{5}{2}a_1$.

Subcase 2_a. Here we have $q_1 = 2$, $\epsilon_1 = 1$. In fact

$$a = 2a_1 + (a - 2a_1) = 2a_1 + a_2$$

and

$$2(a - 2a_1) < a_1,$$

this inequality being equivalent to $2a < 5a_1$, which was assumed. On the other hand, the first step in the L.R.A. applied to $a, a - a_1$ will lead to

$$a = 2(a - a_1) - (a - 2a_1) = 2(a - a_1) - a_2,$$

since

$$2a_2 = 2a - 4a_1 < a - a_1,$$

which is true by virtue of the supposed inequality $a < 3a_1$. Now if it happens that $a_2 = 0$, both algorithms consist of one

step. If, however, $a_2 > 0$, then, since $a - a_1 = a_1 + a_2$, the next steps in the two algorithms will be, respectively,

$$a_1 = a_2q_2 + \epsilon_2a_3; \quad a_1 + a_2 = a_2(q_2 + 1) + \epsilon_2a_3,$$

and from this point on both algorithms will be identical. Thus, in Case 2_a the L.R.A. for the pairs a, a_1 and $a, a - a_1$ are of the same length.

Subcase 2_b. Now $q_1 = 3$ and $\epsilon_1 = -1$. In fact

$$a = 3a_1 - (3a_1 - a) = 3a_1 - a_2$$

and

$$2(3a_1 - a) = 6a_1 - 2a \leq a_1,$$

which amounts to $2a \geq 5a_1$, as was supposed. On the other hand,

$$a - a_1 = 2a_1 - a_2, \quad a - 2a_1 = a_1 - a_2;$$

hence the first step in the L.R.A. for the pair $a, a - a_1$ is

$$a = 2(2a_1 - a_2) - (a_1 - a_2).$$

The continuation of this algorithm will consist of exactly as many steps as are required in the L.R.A. for the pair $a_1, a_1 - a_2$, since $2a_1 - a_2 = a_1 + (a_1 - a_2)$. On the other hand, the continuation of the L.R.A. for the pair a, a_1 requires as many steps as the L.R.A. for a_1, a_2 . Now $a_1 < L$, and consequently, by hypothesis, the L.R.A. for a_1, a_2 is not longer than that for $a_1, a_1 - a_2$. Finally we have that the L.R.A. for a, a_1 is not longer than that for $a, a - a_1$.

Thus, assuming the lemma to be true for all $a < L$, in all cases it remains true for $a = L$ and, according to what has been said previously, the lemma is universally valid. This method of reasoning by *induction* is often resorted to in the number theory where even the propositions themselves are not seldom discovered by observation or induction.

4. Kronecker's Theorem. Now that the lemma is proved, the proof of Kronecker's theorem can be achieved in a few words. It can be stated as follows: Let a and a_1 be two positive integers and $a_1 < a$; then the least remainder algorithm is not longer than any other Euclid's algorithm applied to the pair a, a_1 .

PROOF. The theorem is evident if a_1 divides a . The smallest a not divisible by any number less than it is $a = 3$, and then we must take $a_1 = 2$. In this case there are only two Euclid's algorithms,

$$\begin{array}{ll} 3 = 2 \cdot 1 + 1 & 3 = 2 \cdot 2 - 1 \\ 2 = 1 \cdot 2 + 0 & 2 = 1 \cdot 2 + 0 \end{array}$$

both being L.R.A. and of equal length. When $a = 4$ we must take $a_1 = 3$. Then there are exactly three Euclid's algorithms,

$$\begin{array}{lll} 4 = 3 \cdot 1 + 1 & 4 = 3 \cdot 2 - 2 & 4 = 3 \cdot 2 - 2 \\ 3 = 1 \cdot 3 + 0 & 3 = 2 \cdot 1 + 1 & 3 = 2 \cdot 2 - 1 \\ & 2 = 1 \cdot 2 + 0 & 2 = 1 \cdot 2 + 0 \end{array}$$

of which the first is the L.R.A. and shorter than the two others. When $a = 5$, we may associate $a_1 = 2, 3, 4$ and have the following Euclid's algorithms:

$$\begin{array}{ll} 5 = 2 \cdot 2 + 1 & 5 = 2 \cdot 3 - 1 \\ 2 = 1 \cdot 2 + 0 & 2 = 1 \cdot 2 + 0 \end{array}$$

$$\begin{array}{lll} 5 = 3 \cdot 1 + 2 & 5 = 3 \cdot 1 + 2 & 5 = 3 \cdot 2 - 1 \\ 3 = 2 \cdot 1 + 1 & 3 = 2 \cdot 2 - 1 & 3 = 1 \cdot 3 + 0 \\ 2 = 1 \cdot 2 + 0 & 2 = 1 \cdot 2 + 0 & \end{array}$$

$$\begin{array}{llll} 5 = 4 \cdot 1 + 1 & 5 = 4 \cdot 2 - 3 & 5 = 4 \cdot 2 - 3 & 5 = 4 \cdot 2 - 3 \\ 4 = 1 \cdot 4 + 0 & 4 = 3 \cdot 1 + 1 & 4 = 3 \cdot 2 - 2 & 4 = 3 \cdot 2 - 2 \\ & 3 = 1 \cdot 3 + 0 & 3 = 2 \cdot 1 + 1 & 3 = 2 \cdot 2 - 1 \\ & & 2 = 1 \cdot 2 + 0 & 2 = 1 \cdot 2 + 0. \end{array}$$

In all these cases, when besides the L.R.A. there are others, these others are longer than the L.R.A. Thus the theorem is true for $a = 2, 3, 4, 5$. The theorem will then be proved by induction if, assuming it to be true for all cases when $a < L$, we shall succeed in extending the proof to $a = L$.

Let the result of the division of a by a_1 with the least remainder be

$$a = a_1q_1 + \epsilon_1a_2, \quad 2a_2 \leq a_1,$$

and let

$$a = a_1q'_1 + \epsilon'_1a'_2$$

be the beginning of any Euclid's algorithm. If $a'_2 = a_2$, then the continuation of this algorithm will require at least as many steps as the L.R.A. applied to a_1, a_2 , since $a_1 < L$ and the theorem is supposed to be true for all pairs of numbers in which the greater number is $< L$. Thus in this case the theorem is true for the pair $a = L, a_1 < L$. If, on the contrary, $a'_2 > a_2$, then necessarily

$$q'_1 = q_1 + \epsilon_1, \quad a'_2 = a_1 - a_2.$$

In this case the continuation of the algorithm, by hypothesis, will require not less operations than the L.R.A. applied to the numbers $a_1, a_1 - a_2$. But, by the preceding lemma, this L.R.A. is not shorter than the one applied to a_1, a_2 . Thus the theorem is true for $a = L, a_1 < L$ in all cases. The L.R.A. may be of the same length as some other Euclid's algorithm, not proceeding by least remainders, as the following example shows:

$$\begin{array}{ll} 33 = 13 \cdot 3 - 6 & 33 = 13 \cdot 2 + 7 \\ 13 = 6 \cdot 2 + 1 & 13 = 7 \cdot 2 - 1 \\ 6 = 1 \cdot 6 + 0 & 7 = 1 \cdot 7 + 0. \end{array}$$

Exercises and Problems

1. Show that the L.R.A. applied to a pair a, b where $b < a$ requires less divisions than

$$\frac{2}{3}(p + \frac{1}{2})$$

where p is the number of digits in b .

Indication of Proof: Let $b_1, b_2, b_3, \dots, b_n$ be the remainders, taken positively, in the L.R.A. applied to a, b . Then

$$b \geq 2b_1 + b_2, \quad b_1 \geq 2b_2 + b_3, \quad \dots, \quad b_{n-2} \geq 2b_{n-1} + b_n, \\ b_{n-1} \geq 2b_n$$

and

$$0.82(1 + \sqrt{2})^n < b.$$

2. If b is the smaller of two relatively prime numbers a, b , then the number of Euclid's algorithms for this pair is independent of a and $-b$.

Indication of Proof: Denoting the number of Euclid's algorithms for the pair a, b by $\varphi(a, b)$ and setting

$$a = bq + r, \quad 0 < r < a,$$

show first that

$$\varphi(a, b) = \varphi(b, r) + \varphi(b, b - r);$$

then reason by induction.

5. **Indeterminate Equations of the First Degree.** By admitting negative dividends, divisors, and remainders, any Euclid's algorithm may be put in the form

$$a = bq_1 + r_1 \\ b = r_1q_2 + r_2 \\ r_1 = r_2q_3 + r_3 \\ \dots \\ r_{n-2} = r_{n-1}q_n + r_n,$$

where r_n divides r_{n-1} and may differ from the greatest common divisor of a and b only in sign. From the first equation we get

$$r_1 = a - bq_1 = aQ_1 - bP_1$$

if we set

$$P_1 = q_1, \quad Q_1 = 1.$$

By substituting this expression for r_1 into the second equation and solving for r_2 , we have

$$r_2 = (P_1q_2 + 1)b - Q_1q_2a = -(aQ_2 - bP_2),$$

where, for abbreviation, we set

$$P_2 = q_2P_1 + 1, \quad Q_2 = q_2Q_1.$$

The same procedure applied to the third equation yields

$$r_3 = (q_3Q_2 + Q_1)a - (q_3P_2 + P_1)b = aQ_3 - bP_3,$$

where

$$P_3 = q_3P_2 + P_1, \quad Q_3 = q_3Q_2 + Q_1.$$

It is clear now that in general we can set

$$r_k = (-1)^{k-1}(aQ_k - bP_k).$$

Writing down r_{k-1} and r_{k+1} in a similar way and making use of the expression

$$r_{k+1} = r_{k-1} - r_kq_{k+1},$$

we see that P_{k+1} , Q_{k+1} depend on P_k , Q_k ; P_{k-1} , Q_{k-1} in the following manner:

$$\begin{aligned} P_{k+1} &= q_{k+1}P_k + P_{k-1} \\ Q_{k+1} &= q_{k+1}Q_k + Q_{k-1} \end{aligned}$$

and such relations will hold for $k = 1, 2, \dots, n - 1$ if, for the sake of uniformity, we set

$$P_0 = 1, \quad Q_0 = 0.$$

This means that the two sequences of integers

$$\begin{aligned} P_0, P_1, P_2, \dots, P_n \\ Q_0, Q_1, Q_2, \dots, Q_n \end{aligned}$$

are determined in a recurrent manner starting with

$$\begin{aligned} P_0 &= 1, & Q_0 &= 0 \\ P_1 &= q_1, & Q_1 &= 1 \end{aligned}$$

and determining each pair through two preceding ones by means of the recurrence relations

$$\begin{aligned} P_{k+1} &= q_{k+1}P_k + P_{k-1} \\ Q_{k+1} &= q_{k+1}Q_k + Q_{k-1}. \end{aligned}$$

The last remainder r_n in the ordinary Euclid's algorithm coincides with the g.c.d., taken positively, of a and b and for other Euclid's algorithms will be either d or $-d$, so that in all cases we may set

$$r_n = \epsilon d,$$

where $\epsilon = \pm 1$ is a known unit. Now

$$r_n = (-1)^{n-1}(aQ_n - bP_n);$$

consequently, putting

$$x = \epsilon(-1)^{n-1}Q_n, \quad y = \epsilon(-1)^n P_n,$$

we have

$$ax + by = d.$$

In other words, integers x and y can always be found so as to make the linear form $ax + by$ equal to the g.c.d. of its coefficients a, b . This important conclusion can be generalized: If there are several integers a, b, c, \dots, k with g.c.d. d , then integers x, y, z, \dots, v can be found, so that

$$ax + by + cz + \dots + kt = d.$$

The proof of the last statement will be developed for three integers a, b, c , and it can easily be extended to any number. Let e be the g.c.d. of a and b , then $d = (e, c)$, and two integers t and z can be found so that

$$et + cz = d.$$

On the other hand, with two properly chosen integers u, v ,

$$au + bv = e,$$

whence, setting $x = ut, y = vt$,

$$ax + by + cz = d.$$

6. Continuation. An equation of the first degree with two unknowns

$$ax + by = c,$$

when nothing limits the choice of x , y , is an indeterminate equation in the sense that to y we can attribute an arbitrary value and then find a corresponding x , provided $a \neq 0$. The problem in such generality is a trivial one. But on setting the additional requirement that the values of the unknowns should be integers, we have the simplest example of an extensive class of problems requiring the solution of indeterminate equations of various types (or indeterminate systems of equations), the study of which constitutes an important part of the theory of numbers. Indeterminate equations, to be solved in integers, are often called "Diophantine equations" in honor of Diophantus, a Greek mathematician who lived probably in the third century A.D. and left a work on arithmetic in which he dealt with the solution of indeterminate equations in rational numbers and sometimes in integers.

In dealing with an indeterminate equation

$$\begin{array}{l} \text{www.dbraulibrary.org.in} \\ ax + by = c \end{array}$$

to be solved in integers, we assume explicitly that a , b , c are given integers and a , b are not both equal to 0. The complete solution consists of two parts: first, to inquire under what conditions the solution in integers is possible; and, second, to give a method which allows us to exhibit all such solutions.

Now it is clear that the necessary condition for the existence of integral solutions is that the g.c.d. of a and b should divide c , and this necessary condition is, at the same time, sufficient. For let $(a, b) = d$ and

$$a = d\alpha, \quad b = d\beta, \quad c = d\gamma;$$

then, since d is the g.c.d. of a and b , by Sec. 5 two integers ξ , η can be found so that

$$a\xi + b\eta = d.$$

Clearly $x = \gamma\xi$, $y = \gamma\eta$ will satisfy the proposed equation. Suppose now that one pair of integers, say x_0, y_0 , satisfying the proposed equation, is found so that

$$ax_0 + by_0 = c,$$

and let

$$ax + by = c$$

for some other pair of integers x, y . Then, by subtraction,

$$a(x - x_0) + b(y - y_0) = 0,$$

or

$$\frac{a}{d}(x - x_0) = -\frac{b}{d}(y - y_0).$$

Since

$$\frac{a}{d}(x - x_0)$$

is divisible by b/d and a/d is relatively prime to the divisor, $x - x_0$ must be divisible by b/d . Hence

$$x - x_0 = \frac{b}{d}t,$$

where t is an integer, and at the same time

$$y - y_0 = -\frac{a}{d}t.$$

It follows that any solution x, y can be presented thus:

$$x = x_0 + \frac{b}{d}t, \quad y = y_0 - \frac{a}{d}t$$

with t an integer. Conversely, for an arbitrary integer t , integers x, y satisfy the proposed equation.

Our problem now is completely solved, and the process described in Sec. 5 provides an excellent practical method for finding one particular solution. It is hardly necessary to

mention that the least remainder algorithm, as the shortest, is preferable to others, though it may introduce negative integers. If it is desirable to deal with positive remainders, only then should the ordinary Euclid's algorithm be used.

Example 1. Solve the equation $91x + 221y = 1,053$. Making use of the ordinary Euclid's algorithm, we find:

$$\begin{aligned} 91 &= 221 \cdot 0 + 91 \\ 221 &= 91 \cdot 2 + 39 \\ 91 &= 39 \cdot 2 + 13 \\ 39 &= 13 \cdot 3. \end{aligned}$$

Hence 13 is the g.c.d. of 91 and 221, and since 13 divides 1,053 (with the quotient 81), the equation can be solved in integers. The process described in Sec. 5 can be arranged in practice as follows:

$$\begin{array}{cccc} & q_2 = 2 & q_3 = 2 & \\ P_0 = 1 & P_1 = 0 & P_2 = 1 & P_3 = 2 \\ Q_0 = 0 & Q_1 = 1 & Q_2 = 2 & Q_3 = 5. \end{array}$$

Consequently $\xi = 5$, $\eta = -2$ satisfy the equation

$$91\xi + 221\eta = 13$$

and

$$x_0 = 81 \cdot 5 = 405, \quad y_0 = -81 \cdot 2 = -162$$

satisfy the proposed equation. All the solutions of this equation will be given by

$$x = 405 + 17t, \quad y = -162 - 7t$$

for any arbitrary integer t . To get more convenient formulas we divide 405 by 17, finding the quotient 23 and remainder 14, and set $t = \tau - 23$; then the expressions for x , y become

$$x = 14 + 17\tau, \quad y = -1 - 7\tau.$$

But are there any solutions in positive integers? To answer this question we must see whether it is possible to choose τ so as to have

$$14 + 17\tau > 0, \quad -1 - 7\tau > 0$$

or

$$\tau > -\frac{14}{17} \quad \text{or} \quad \tau \geq 0$$

and

$$\tau < -\frac{1}{7} \quad \text{or} \quad \tau \leq -1.$$

Since these requirements cannot be satisfied, there is no solution of the equation

$$91x + 221y = 1,053$$

in positive integers.

Example 2. Solve the equation $158x + 57y = 20,000$ in positive integers.

In this example we shall make use of the least remainder algorithm

$$\begin{aligned} 158 &= 57 \cdot 3 - 13 \\ 57 &= -13 \cdot -4 + 5 \\ -13 &= 5 \cdot -3 + 2 \\ 5 &= 2 \cdot 2 + 1. \end{aligned}$$

Since 158 and 57 are relatively prime, the equation is soluble in integers. By the process of Sec. 5 we find

$$\begin{array}{cccccc} & q_2 = -4 & q_3 = -3 & q_4 = 2 & & \\ P_0 = 1 & P_1 = 3 & P_2 = -11 & P_3 = 36 & P_4 = 61 & \\ Q_0 = 0 & Q_1 = 1 & Q_2 = -4 & Q_3 = 13 & Q_4 = 22 & \end{array}$$

and

$$158 \cdot -22 + 57 \cdot 61 = 1.$$

Hence one pair of numbers satisfying the proposed equation is

$$\begin{aligned} x_0 &= -22 \cdot 20,000 = -440,000 \\ y_0 &= 61 \cdot 20,000 = 1,220,000, \end{aligned}$$

and all the others will be found from the formulas

$$x = -440,000 + 57t, \quad y = 1,220,000 - 158t;$$

or, setting $t = 7,719 + \tau$,

$$x = -17 + 57\tau, \quad y = 398 - 158\tau,$$

τ being an arbitrary integer. Positive solutions are obtained if

$$\tau > \frac{17}{57} \quad \text{or} \quad \tau \geq 1$$

and

$$\tau < \frac{398}{158} \quad \text{or} \quad \tau \leq 2.$$

Hence there are only two positive solutions

$$\begin{aligned} x &= 40, & y &= 240 \\ x &= 97, & y &= 82 \end{aligned}$$

corresponding to $\tau = 1$ and $\tau = 2$.

7. Nonnegative Solutions of Linear Indeterminate Equations. The problem of finding nonnegative solutions of an equation

$$ax + by = c,$$

in which a, b, c are positive integers, can be attacked in a different way. On dividing x and y , respectively, by b and a , we have

$$x = b\xi + r, \quad y = a\eta + s,$$

where ξ, η, r, s are nonnegative integers, and $r < b, s < a$ and the substitution of these expressions yields

$$ab(\xi + \eta) + ar + bs = c.$$

By division we can represent c as

$$c = abq + R, \quad 0 \leq R < ab,$$

whence, together with the preceding equation, it follows

$$ar + bs - R = ab(\xi + \eta).$$

This shows that $ar + bs - R$ is divisible by ab , but

$$ar + bs < 2ab;$$

consequently

$$ar + bs - R < 2ab,$$

and on the other hand

$$ar + bs - R > -ab,$$

and so the integer

$$\frac{ar + bs - R}{ab}$$

is > -1 and < 2 . It can only be 0 or 1; that is,

$$ar + bs = R \quad \text{or} \quad ar + bs = R + ab,$$

and correspondingly

$$\xi + \eta = q \quad \text{or} \quad \xi + \eta = q - 1.$$

Now, if a and b are relatively prime, as we can legitimately suppose, of the two equations

$$ar + bs = R \quad \text{and} \quad ar + bs = R + ab,$$

one and only one admits of a solution in nonnegative integers $r < b$ and $s < a$. To prove this let us denote by r_0, s_0 some particular solution of the first equation. Then all the solutions of this equation will be given by

$$r = r_0 - bt, \quad s = s_0 + at,$$

and among them there is one and only one in which $0 \leq r < b$. The corresponding value of s is necessarily less than a because $bs \leq R < ab$. Moreover $s > -a$, since

$$bs \geq -ar > -ab.$$

Now if it happens that $s \geq 0$, then the equation

$$ar + bs = R$$

has a solution of the required kind and the solution is unique. But then it is impossible to satisfy the other equation in the same manner. For $r + b, s$ will satisfy this equation, and all other solutions of it will be given by

$$r + b - bt, \quad s + at,$$

and the only way to make the first number nonnegative and less than b is to take $t = 1$, but then the second number will be $\geq a$. If, on the contrary, $s < 0$, then numbers r and $s + a$, both nonnegative and less than b and a , respectively, will satisfy the second equation.

Thus there are only two cases to consider: (1) when the equation $ar + bs = R$ is solvable in nonnegative integers $r < b, s < a$; (2) when it is not solvable in this manner.

In the first case, equation

$$\xi + \eta = q$$

has exactly $q + 1$ solutions in nonnegative integers

$$\begin{aligned}\xi &= 0, 1, 2, \dots, q \\ \eta &= q, q - 1, q - 2, \dots, 0\end{aligned}$$

and correspondingly there are $q + 1$ solutions of the equation $ax + by = c$ in nonnegative integers. In the second case,

$$\xi + \eta = q - 1$$

has exactly q solutions in nonnegative integers

$$\begin{aligned}\xi &= 0, 1, 2, \dots, q - 1 \\ \eta &= q - 1, q - 2, q - 3, \dots, 0\end{aligned}$$

to which correspond again q solutions of the proposed equation in nonnegative integers.

The result of this discussion can be summarized as follows: The equation

$$ax + by = c$$

www.dbraulibrary.org.in

in which a, b, c are positive integers, the first two relatively prime, has $q + 1$ or q solutions according as the equation

$$ar + bs = R$$

has solutions in nonnegative integers $r < b, s < a$ or not. Here q and R denote, respectively, the quotient and the remainder in the division of c by ab .

Example. Let us solve the equation

$$158x + 57y = 20,000$$

in nonnegative integers by the method of this section. We have $q = 2$, $R = 1,988$. All the solutions of the equation

$$158r + 57s = 1,988$$

are given by

$$r = -43,736 + 57t, \quad s = 121,268 - 158t.$$

Corresponding to $t = 768$ we have $r = 40$, $s = -76$; consequently we have the second case and the equation

$$158r + 57s = 1,988 + 9,006$$

is satisfied in the desired manner by $r = 40$, $s = 158 - 76 = 82$. Correspondingly

$$x = 57\xi + 40, \quad y = 158\eta + 82$$

and

$$\begin{aligned} \xi &= 0, 1 \\ \eta &= 1, 0. \end{aligned}$$

That is, there are two solutions in nonnegative integers

$$\begin{aligned} x &= 40, & y &= 240 \\ x &= 97, & y &= 82 \end{aligned}$$

as we found before.

8. Equations in Several Unknowns and Systems of Equations. The solution in integers of linear indeterminate equations with several unknowns as well as systems of such equations can always be reduced to the solution of a number of equations with two unknowns. Without going into the general theory, we shall show how to do this in the case of one or two equations with three unknowns.

Let us consider the equation

$$ax + by + cz = e,$$

where a, b, c, e are given integers. Instead of y and z let us introduce another pair of numbers t, u , so that

$$\begin{aligned} y &= \alpha t + \beta u \\ z &= \gamma t + \delta u, \end{aligned}$$

where $\alpha, \beta, \gamma, \delta$ are four arbitrary integers chosen so that $\alpha\delta - \beta\gamma = 1$. It is obvious that to integral values of t and u will correspond integral values of y and z . But also to integral values of y and z will correspond integral values of t and u , since

$$\begin{aligned} t &= \delta y - \beta z \\ u &= -\gamma y + \alpha z. \end{aligned}$$

When we substitute for y, z their expressions in t, u , the equation takes the form

$$ax + (b\alpha + c\gamma)t + (b\beta + c\delta)u = e,$$

and the solution of this equation in integers x, t, u is entirely equivalent to the solution of the original equation in integers x, y, z . But by proper choice of $\alpha, \beta, \gamma, \delta$, the transformed equation can be made to contain two unknowns only. We may suppose, of course, that b and c are not equal to 0 simultaneously. If so we may choose β and δ so as to satisfy the condition

$$b\beta + c\delta = 0.$$

To this end, if $(b, c) = d$, it suffices to take

$$\beta = -\frac{c}{d}, \quad \delta = \frac{b}{d}.$$

Then α, γ should be found from

$$\alpha\frac{b}{d} + \gamma\frac{c}{d} = 1$$

or

$$ab + \gamma c = d,$$

which equation is solvable in integers α, γ .

With $\alpha, \beta, \gamma, \delta$ determined as specified, the transformed equation

$$ax + dt = e$$

involves only two unknowns, x and t . If it is solvable, all of its solutions in integers will be given by the set of formulas

$$\begin{aligned} x &= r + fv \\ t &= s + gv, \end{aligned}$$

where r, s, f, g are known integers, while v is an arbitrary integer. Finally x, y, z will be given by formulas of the type

$$x = x_0 + Au + Bv, \quad y = y_0 + Cu + Dv, \\ z = z_0 + Eu + Fv$$

involving two arbitrary integers u, v .

Example. To solve in integers

$$3x - 6y + 16z = 1$$

we note $b = -6, c = 16, d = 2$. Correspondingly

$$\beta = -8, \quad \delta = -3$$

and α, γ satisfy the equation

$$-6\alpha + 16\gamma = 2.$$

We can take $\alpha = -3, \gamma = -1$, so that

$$y = -3t - 8u, \quad z = -t - 3u.$$

The general solution of the transformed equation

$$3x + 2t = 1$$

is $x = 1 + 2v, \quad t = -1 - 3v,$

whence

$$x = 1 + 2v, \quad y = 3 + 9v - 8u, \quad z = 1 + 3v - 3u$$

with two arbitrary integers u, v .

If it is required to solve two simultaneous equations

$$ax + by + cz = e \\ fx + gy + hz = k,$$

the procedure is obvious. We solve the first equation, obtaining for x, y, z expressions involving linearly two arbitrary integers u, v . On substituting these expressions into the second equation, we get an indeterminate equation in two unknowns u, v .

Example. Solve in integers the system

$$3x - 6y + 16z = 1 \\ 2x + 5y - 6z = 2.$$

The first is satisfied in the most general way by

$$x = 1 + 2v, \quad y = 3 + 9v - 8u, \quad z = 1 + 3v - 3u.$$

On substituting these expressions into the second, we get

$$31v - 22u = -9,$$

whence

$$v = -1 + 22w, \quad u = -1 + 31w.$$

Finally

$$x = -1 + 44w, \quad y = 2 - 50w, \quad z = 1 - 27w$$

with an arbitrary integer w .

Exercises and Problems

1. Solve in positive integers $101x + 753y = 100,000$.

$$\text{Ans. } x = 170, y = 110; \text{ and } x = 923, y = 9.$$

2. Find the smallest positive integer a for which the equation $1001x + 770y = 1,000,000 + a$ is possible and show that it has then 100 solutions in positive integers.

3. Find a multiple of 7 which, when divided by 2, 3, 4, 5, and 6, has for remainders 1, 2, 3, 4, and 5, respectively.

$$\text{Ans. } 119 + 420t.$$

4. Solve in positive integers $31x + 257y = 100,000$.

$$\text{Ans. Twelve solutions, one of which is } x = 233, y = 361.$$

5. Solve in positive integers the system

$$7x + 3y + 19z = 2,530$$

$$8x + 6y + 33z = 3,753.$$

$$\text{Ans. Four solutions, one of which is } x = 162, y = 41, z = 67.$$

6. Solve in positive integers $7x + 5y + 15z + 12t = 149$.

$$\text{Ans. Fifty-seven solutions, one of which is } x = 2, y = 3, z = 4, t = 5.$$

7. A man received a check for a certain amount of money, but on cashing it the cashier mistook the number of dollars for the number of cents and conversely. Not noticing this, the man then spent 68 cts. and discovered to his amazement that he had twice as much money as the check was originally drawn for. Determine the smallest amount of money for which the check could have been written.

$$\text{Ans. } \$10.21.$$

8. A customer buys an article for 48 cts. He has a \$1 bill and 3 pennies, while the shopkeeper has 6 dimes and 7 nickels. How can the change be arranged?

9. Suppose the conditions are the same as in Problem 8 except that the article costs 49 cts. The change could not be arranged between the

buyer and the shopkeeper, so they ask a hanger-on in the store, who has 2 dimes, a nickel, and 3 2-ct. stamps, to help them. The customer and the shopkeeper agree to take stamps. How can they arrange the change?

Ans. The change can be arranged in 28 ways.

10. A yardstick divided into inches is again divided into 70 equal parts. Where are the shortest divisions located?

Ans. The left end points of two divisions correspond to 1 and 19 in., and the right end points of the other two correspond to 17 and 35 in.

11. Two church bells begin ringing at the same time. The strokes of one follow regularly at intervals of $1\frac{1}{3}$ sec., while the intervals between two strokes of the second are $1\frac{3}{4}$ sec. How many strokes are heard during 15 min. if 2 strokes following each other in an interval of $\frac{1}{2}$ sec. or less are perceived as one sound?

Ans. 772.

12. In how many ways can change for \$1 be made with pennies, nickels, dimes, and quarters?

Ans. In 242 ways.

13. Solve the equation $(n+1)^2x - n^2y = 1$.

Ans. One solution: $x = 1 - 2n$, $y = -3 - 2n$.

14. Solve $nx + (n+1)y + (n+2)z = n^2$ and show that there is always a solution in positive integers if $n \geq 5$.

15. The number of nonnegative solutions of the equation

$$x + 2y + 3z = n$$

$$x + 2y + 3z = n$$

is the nearest integer to $(n+3)^2/12$.

16. Solve the same problem for the equation

$$x + 2y + 4z = n.$$

Ans. Nearest integer to $\frac{(n+2)(n+5)}{16} + (-1)^n \frac{n}{16}$.

17. Find the greatest number c for which the equation

$$5x + 7y = c$$

has exactly nine solutions in nonnegative integers.

Ans. 338.

18. The total number of solutions of the equations

$$x + 2y = n, \quad 2x + 3y = n - 1, \quad 3x + 4y = n - 2, \quad \dots, \\ nx + (n+1)y = 1$$

in nonnegative integers is n .

19. Let a , b be positive relatively prime integers and N a positive integer $< ab$. Divide N by a and b , and call the remainders, respectively,

r and ρ and set $N_1 = N - r - \rho$; divide again N_1 by a and b , and call the remainders respectively r_1 and ρ_1 , and set $N_2 = N_1 - r_1 - \rho_1$ and continue the same process. Prove that the equation

$$ax + by = N$$

is soluble in nonnegative integers if and only if 0 occurs in the series of decreasing integers N, N_1, N_2, \dots

www.dbraultlibrary.org.in

Downloaded from www.dbraultlibrary.org.in

CHAPTER IV

ON PRIME NUMBERS

1. Prime and Composite Numbers. Perhaps one of the most significant early advances in the development of a scientific number theory was the distinction, already made in the Pythagorean school, between prime and composite numbers. Numbers like 2, 3, 5, 7, 11, . . . are divisible only by the number one and themselves, while other numbers like 4, 6, 8, 9, . . . possess divisors other than the two mentioned. A number p , distinct from 1, is a *prime number* or simply *prime* if it has no other divisors than 1 and p . A number m , which has divisors > 1 and $< m$ is a *composite number*. The characteristic property of a composite number, therefore, consists in the possibility of representing it as a product of two factors:

$$m = ab$$

each of which is greater than 1, while such a representation is impossible for a prime.

Exercises

1. Show that for $n > 1$, $n^2 + 4$ is a composite number.
2. Show that $2^{4n+2} + 1$ is a composite number if $n \geq 1$.
3. A number of the form $2^a - 1$ cannot be prime if a is a composite number. HINT: The proof depends on the identity

$$x^m - 1 = (x - 1)(x^{m-1} + x^{m-2} + \dots + x + 1).$$

2. A Test of Primality. We may show that every number which is not a unit is divisible by a prime. For, of all the

divisors of a given number $a > 1$, let us select the smallest p which is still greater than 1. Now p must be a prime; otherwise p has a divisor $q > 1$ and $< p$, and q would be a divisor of a , which is > 1 and $< p$ contrary to the assumption that p , of all the divisors > 1 of a , was the smallest.

Every composite number a is divisible by a prime $\leq \sqrt{a}$. For a , being a composite number, can be represented in the form

$$a = bc,$$

where $b > 1, c > 1$. We can suppose $b \leq c$ and then $b \leq \sqrt{a}$. Now if $b > 1$ has a prime divisor $p \leq b \leq \sqrt{a}$, at the same time p will be a prime divisor of a . This remark gives the first practical test to ascertain whether a given number is prime or not. It suffices to divide this number by primes not exceeding its square root, and if one division succeeds without a remainder, then the proposed number is composite; otherwise it will be prime. Let us test, for example, 787. Primes not exceeding $\sqrt{787}$ are

$$2, 3, 5, 7, 11, 13, 17, 19, 23,$$

and on trial we find that none of them divides 787. Hence 787 is a prime number.

This simplest test of primality is quite workable and convenient when the numbers to be tested are not large; but with the increasing size of the numbers, the trials become too numerous and burdensome. To obviate this inconvenience other, more expeditious, methods have been devised to ascertain whether a number is prime or not. An account of some of these methods will be given later. At this time we can add only that with all the refinements and improvements these methods become inadequate when testing numbers exceeding, say, 100,000,000,000.

3. The Sieve of Eratosthenes. Eratosthenes, who lived between 276 and 194 B.C. and was reputed to be one of the most

erudite men of antiquity, devised a simple method of, so to speak, sifting primes out of a series of integers not extending beyond any proscribed limit. Suppose we want to segregate all primes from among the numbers $2, 3, \dots, N$ and suppose we know already all primes not exceeding \sqrt{N} . Then we begin by striking out the smallest prime 2 and all of its multiples; next we strike out 3 and all of its multiples, and continue in the same way until all primes not exceeding \sqrt{N} and their multiples are stricken out of the series $2, 3, \dots, N$. The remaining numbers will all be primes $> \sqrt{N}$ and not exceeding N . To prove this it suffices to observe that only such numbers can remain which are not divisible by any prime not greater than their square roots. Consequently the remaining numbers will all be primes.

Now, having found all primes $> \sqrt{N}$ and $\leq N$ and combining them with the primes $\leq \sqrt{N}$, we get a table of all primes $\leq N$. For example, to have all primes less than 100 it suffices to find by actual test primes not exceeding 10, which are 2, 3, 5, 7. Having found all primes less than 100, we can continue the table of primes up to 10,000 and so on.

With some modifications and refinements and with the help of mechanical devices, the Eratosthenes sieve was used for compilation of large tables of primes. The most extensive and the best of such tables is the one published by D. N. Lehmer.¹ Another important publication of the same author² gives the smallest prime divisors of all integers up to 10,000,000.

Exercises

1. By means of Eratosthenes' sieve compile a list of primes not exceeding 200.

¹ D. N. LEHMER, List of Prime Numbers from 1 to 10,006,721. *Carnegie Institute, Washington, Pub. 165* (1914).

² D. N. LEHMER, Factor Table for the First Ten Millions. *Carnegie Institute, Washington, Pub. 105* (1909).

2. Which of the numbers 1,567, 1,829, 5,671 are primes and which are not?

4. Unique Factorization Theorem. Every number, if not prime, can be factorized into the product of primes. For if we let N be a composite number, then it has a prime divisor p (Sec. 2) and we can set

$$N = pN_1, \quad N_1 < N.$$

The statement is proved if N_1 is a prime number. Otherwise N_1 has a prime divisor p_1 and

$$N_1 = p_1N_2, \quad N_2 < N_1.$$

If N_2 is another composite number, it is divisible by a prime p_2 and

$$N_2 = p_2N_3, \quad N_3 < N_2.$$

Continuing in the same manner, we must come to an equation

$$N_{n-1} = p_{n-1}N_n,$$

in which N_n is a prime $= p_n$, since the series of decreasing integers

$$N > N_1 > N_2 > N_3 > \dots$$

cannot continue indefinitely. On eliminating N_{n-1} , N_{n-2} , \dots , N_1 we reach the desired representation of N :

$$N = p_1p_2 \dots p_n$$

as a product of primes. Of course the primes in this representation need not be different. For example,

$$220 = 2 \cdot 110 = 2 \cdot 2 \cdot 55 = 2 \cdot 2 \cdot 5 \cdot 11.$$

It is extremely remarkable and important that the factorization into a product of primes is unique. This depends on the following property of prime numbers which, on account of its usefulness, we shall state as a theorem.

THEOREM. A prime dividing the product of several integers divides at least one of them.

PROOF. If p is a prime number and a an arbitrary integer, then either p divides a or p and a are relatively prime numbers. For the g.c.d. of p and a , as divisor of the prime p , is either p , in which case a is divisible by p , or 1, in which case a and p are relatively prime numbers. Now let the product ab be divisible by a prime p . Then if a is not divisible by p , a and p are relatively prime; hence (Chap. 2, Sec. 6, Theorem 5) b is divisible by p . If the product of three factors abc is divisible by a prime p and if a is not divisible by p , then bc must be divisible by p , by the preceding proof, and for the same reason one at least of the numbers b , c must be divisible by p . In the same manner the theorem can be proved for four, five, and in general any number of factors.

THEOREM OF UNIQUE FACTORIZATION. An integer other than the unit integer can be factorized into the product of primes in one way only; that is, if for the same integer there are two representations

$$N = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$$

where $p_1, p_2, \dots, p_r; q_1, q_2, \dots, q_s$ are primes, then $s = r$ and q_1, q_2, \dots, q_s are, save for order, the same primes as p_1, p_2, \dots, p_r .

PROOF. We can assume that $s \leq r$. The product

$$p_1 p_2 \cdots p_r$$

being divisible by a prime q_1 , one of its factors, say p_1 , will be divisible by q_1 . But because p_1 is a prime, we must have $p_1 = q_1$. Canceling the equal factors p_1 and q_1 on both sides,

$$p_2 \cdots p_r = q_2 \cdots q_s,$$

and for the same reason as before we may assume $p_2 = q_2$. Canceling equal factors on both sides again, we shall have

$$p_3 \cdots p_r = q_3 \cdots q_s,$$

and we can continue in the same way until all the factors on the right side are canceled. Now, if $r > s$, we shall reach an impossible equation

$$p_{s+1} \cdots p_r = 1.$$

Consequently $r = s$, but then it follows that with proper notation

$$p_1 = q_1, \quad p_2 = q_2, \quad \dots, \quad p_r = q_r,$$

and this proves the uniqueness theorem.

In the unique factorization of N

$$N = p_1 p_2 \cdots p_n$$

into the product of prime factors, some primes may occur repeatedly. Suppose that among the primes p_1, p_2, \dots, p_n there are

α primes equal to p

β primes equal to q

\dots www.dbrapuliLibrary.org.in

λ primes equal to t .

Then

$$N = p^\alpha q^\beta \cdots t^\lambda$$

is represented as a product of powers of different primes, and such representation will be unique. Thus primes appear as fundamental building stones out of which every integer can be built up by multiplication in a unique manner.

5. Criterion of Divisibility. The theorem of unique factorization leads immediately to an important criterion whereby it is possible to say by inspection, without performing the actual division, whether one integer is divisible by another or not. Suppose that a is divisible by b , so that

$$a = bc$$

where c is an integer, and let

$$b = p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}$$

be the factorization of b into the product of powers of different primes. Since some of the primes p_1, p_2, \dots, p_s may also occur in the factorization of c , it is clear, by virtue of the unique factorization theorem, that p_1, p_2, \dots, p_s will occur in the factorization of a and in the powers, respectively, not less than $\alpha_1, \alpha_2, \dots, \alpha_s$. Thus for the divisibility of a by b it is necessary that all prime factors of b enter into a in powers not less than those in which they enter into b . But this necessary condition is also sufficient for the divisibility of a by b . For, if it is fulfilled, we may set

$$a = p_1^{\beta_1} p_2^{\beta_2} \cdots p_s^{\beta_s} A,$$

where A is an integer and $\beta_1 \geq \alpha_1, \beta_2 \geq \alpha_2, \dots, \beta_s \geq \alpha_s$. Now

$$a = b p_1^{\beta_1 - \alpha_1} p_2^{\beta_2 - \alpha_2} \cdots p_s^{\beta_s - \alpha_s} A$$

and

$$c = p_1^{\beta_1 - \alpha_1} p_2^{\beta_2 - \alpha_2} \cdots p_s^{\beta_s - \alpha_s} A$$

is an integer.

To apply this criterion to an example, suppose we want to know whether 40,320 is divisible by 84 without actually performing the division. Since

$$84 = 2^2 \cdot 3 \cdot 7, \quad 40,320 = 2^7 \cdot 3^2 \cdot 5 \cdot 7,$$

by mere inspection we conclude that 40,320 is divisible by 84, the quotient being

$$2^5 \cdot 3 \cdot 5 = 480.$$

6. Divisors of Numbers. When an integer is factored into prime factors, it is easy to find all its divisors. Let

$$a = p_1^{\beta_1} p_2^{\beta_2} \cdots p_s^{\beta_s}$$

be the factorization of a . From the criterion of the preceding section it follows that every divisor d of a is of the form

$$d = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$$

where $0 \leq \alpha_1 \leq \beta_1$, $0 \leq \alpha_2 \leq \beta_2$, . . . , $0 \leq \alpha_s \leq \beta_s$ and vice versa, every number of this form is a divisor of a . Thus we have all the divisors of a and each only once if we let the exponents α_i ($i = 1, 2, \dots, s$) run independently through $0, 1, 2, \dots, \beta_i$.

For example, all the divisors of $360 = 2^3 \cdot 3^2 \cdot 5$ are exhibited in the table

1	2	2^2	2^3
3	$2 \cdot 3$	$2^2 \cdot 3$	$2^3 \cdot 3$
3^2	$2 \cdot 3^2$	$2^2 \cdot 3^2$	$2^3 \cdot 3^2$
5	$2 \cdot 5$	$2^2 \cdot 5$	$2^3 \cdot 5$
$3 \cdot 5$	$2 \cdot 3 \cdot 5$	$2^2 \cdot 3 \cdot 5$	$2^3 \cdot 3 \cdot 5$
$3^2 \cdot 5$	$2 \cdot 3^2 \cdot 5$	$2^2 \cdot 3^2 \cdot 5$	$2^3 \cdot 3^2 \cdot 5$.

Arranged in an increasing order of magnitude, these divisors are 1, 2, 3, 4, 5, 6, 8, 9, 10, 12, 15, 18, 20, 24, 30, 36, 40, 45, 60, 72, 90, 120, 180, 360—altogether, 24 divisors.

Very simple rules serve to find the g.c.d. and the l.c.m. of several numbers factorized into prime factors. Let p_1, p_2, \dots, p_s be all the distinct prime factors of the numbers a, b, \dots, m so that, admitting zero exponents, we can set

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$$

$$b = p_1^{\beta_1} p_2^{\beta_2} \dots p_s^{\beta_s}$$

$$\dots$$

$$m = p_1^{\mu_1} p_2^{\mu_2} \dots p_s^{\mu_s}.$$

The greatest common divisor of a, b, c, \dots, m will be given by the product

$$p_1^{f_1} p_2^{f_2} \dots p_s^{f_s}$$

where f_1, f_2, \dots, f_s are the greatest numbers consistent with the conditions

$$f_1 \leq \alpha_1, \quad f_1 \leq \beta_1, \quad \dots, \quad f_1 \leq \mu_1$$

$$f_2 \leq \alpha_2, \quad f_2 \leq \beta_2, \quad \dots, \quad f_2 \leq \mu_2$$

$$\dots$$

$$f_s \leq \alpha_s, \quad f_s \leq \beta_s, \quad \dots, \quad f_s \leq \mu_s.$$

Hence, in general, f_i (for $i = 1, 2, \dots, s$) must be taken as the smallest of the exponents $\alpha_i, \beta_i, \dots, \mu_i$. On the contrary, if g_i for $i = 1, 2, \dots, s$ is taken as the greatest of the exponents $\alpha_i, \beta_i, \dots, \mu_i$, then the number

$$p_1^{g_1} p_2^{g_2} \cdots p_s^{g_s}$$

will be a common multiple of a, b, \dots, m and of all the common multiples of these numbers the smallest.

7. The Number and Sum of Divisors. A function defined for positive integral values of the argument may be called a "numerical function" in a general sense. The number of divisors and the sum of divisors are the simplest numerical functions of interest in the number theory. We shall denote by $\tau(n)$ the number of divisors and by $\sigma(n)$ the sum of divisors of a positive integer n . Clearly $\tau(1) = 1, \sigma(1) = 1$. To find $\tau(n)$ and $\sigma(n)$ for $n > 1$, we suppose known the factorization of n into prime factors:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}.$$

All the divisors of n , and each only once, are represented by the terms of the expanded product

$$(1 + p_1 + \cdots + p_1^{\alpha_1})(1 + p_2 + \cdots + p_2^{\alpha_2}) \cdots (1 + p_s + \cdots + p_s^{\alpha_s}).$$

Consequently $\sigma(n)$ is equal to this product. But

$$1 + p + \cdots + p^\alpha = \frac{p^{\alpha+1} - 1}{p - 1},$$

for $p > 1$; thus we can present $\sigma(n)$ as

$$\sigma(n) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \cdots \frac{p_s^{\alpha_s+1} - 1}{p_s - 1}.$$

The number of terms of the above product is $\tau(n)$. If we notice that for $p_1 = p_2 = \cdots = p_s = 1$ each term of this product reduces to 1, it is clear that

$$\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_s + 1).$$

Let us take for example $n = 360 = 2^3 \cdot 3^2 \cdot 5$; then

$$\begin{aligned}\tau(360) &= (3 + 1)(2 + 1)(1 + 1) = 24; \\ \sigma(360) &= \frac{2^4 - 1}{2 - 1} \cdot \frac{3^3 - 1}{3 - 1} \cdot \frac{5^2 - 1}{5 - 1} = 1,170.\end{aligned}$$

8. Numerical Functions Depending on Divisors. The numerical functions $\tau(n)$ and $\sigma(n)$ are particular cases of a general class of functions defined as follows. Let $f(n)$ be any numerical function and $F(n)$ another numerical function defined by

$$F(n) = \sum_d f(d)$$

where the summation extends over all the divisors d of n . Then $F(n)$ for $f(n) = 1$ and $f(n) = n$ coincides, respectively, with $\tau(n)$ and $\sigma(n)$. We say that $f(n)$ is a *factorable numerical function* if for any two relatively prime integers n, n'

$$f(nn') = f(n)f(n').$$

We shall prove now that $F(n)$ will be factorable if such is the case for $f(n)$. Denoting by d and d' divisors of n and n' , respectively, we have

$$F(n)F(n') = \sum_d f(d) \sum_{d'} f(d') = \sum_{d, d'} f(d)f(d'),$$

the last summation extending over all combinations of divisors d, d' . Since d and d' , as divisors of two relatively prime integers n and n' , are relatively prime, we have

$$f(d)f(d') = f(dd')$$

because $f(n)$ is a factorable function by hypothesis. Hence

$$F(n)F(n') = \sum_{d, d'} f(dd').$$

The product dd' is a divisor of nn' , which is obvious. Conversely, every divisor D of nn' can be represented as a product of some divisor of n by some divisor of n' . To prove this, let $(D, n) = d$ and $n = \nu d$, $D = dd'$. Then $\nu dn'$ is divisible by dd' ; that is, $\nu n'$ is divisible by d' . But ν and d' are relatively prime numbers; consequently d' is a divisor of n' . Thus, if we let d and d' run through all divisors of n and n' , respectively, the product dd' will run through all the divisors of nn' , and it is important to show that each of these divisors will occur only once. Suppose that

$$dd' = d_1 d'_1$$

where d, d_1 are divisors of n and d', d'_1 are divisors of n' . Since d' and d_1 are relatively prime, d is divisible by d_1 . Also d_1 is divisible by d , since d'_1 and d are relatively prime. Consequently $d_1 = d$ and $d'_1 = d'$, and this proves the assertion.

Since dd' , for all combinations of d and d' , represents all divisors D of nn' and each only once, it is clear that the sum

$$\sum_{d, d'} f(dd')$$

is the same as the sum

$$\sum_D f(D) = F(nn')$$

extended over all the divisors D of nn' . Hence, for any two relatively prime integers n, n' ,

$$F(nn') = F(n)F(n'),$$

that is, $F(n)$ is a factorable numerical function.

By repeated application of this property, we conclude that for a set of integers a, b, c, \dots, k , relatively prime in pairs,

$$F(abc \dots k) = F(a)F(b) \dots F(k)$$

and, in particular,

$$F(n) = F(p_1^{\alpha_1})F(p_2^{\alpha_2}) \cdots F(p_s^{\alpha_s})$$

if

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$$

is a prime factorization of n . Thus to evaluate $F(n)$ in general we need only to evaluate this function in case its argument is a power of a prime p^α . But since divisors of p^α are $1, p, p^2, \dots, p^\alpha$ by the definition of $F(p^\alpha)$, we have

$$F(p^\alpha) = f(1) + f(p) + f(p^2) + \cdots + f(p^\alpha).$$

Applying these general considerations to the particular cases $f(n) = 1$ and $f(n) = n$, of course we get the same expressions for $\tau(n)$ and $\sigma(n)$ as before.

9. Euler's Recurrence Formula. As an example of a more recondite arithmetical truth we shall mention here the famous recurrence formula for the sum of divisors, discovered and proved by Euler by means of analytical considerations.

L. Euler (1707–1783) was one of the greatest mathematicians of the eighteenth century. His work, covering most varied fields of pure and applied mathematics, left a profound impression on the subsequent development of mathematical science. When most of his great contemporaries such as Daniel Bernoulli, Clairaut, and D'Alembert devoted their efforts to the advancement of applied mathematics, Euler spent considerable time in cultivating the theory of numbers with signal success.

Numbers of the form

$$\frac{3k^2 - k}{2}$$

for $k = \pm 1, \pm 2, \pm 3, \dots$ go by the name of generalized pentagonal numbers. Arranged in increasing order of magnitude they are

$$1, 2, 5, 7, 12, 15, 22, 26, 35, 40, \dots$$

Now consider the sum

$$\sigma(n) - \sigma(n-1) - \sigma(n-2) + \sigma(n-5) + \sigma(n-7) \\ - \sigma(n-12) - \sigma(n-15) + \dots$$

in which the signs of the terms follow an obvious law and the arguments are n and this number diminished by consecutive pentagonal numbers as long as the resulting numbers are positive. Euler discovered a remarkable fact about this sum: it is 0 when n is not a pentagonal number, and it is $(-1)^{k-1}n$ if n is a pentagonal number

$$n = \frac{3k^2 - k}{2}.$$

Without distinguishing these two cases, the same can be stated as

$$\sigma(n) - \sigma(n-1) - \sigma(n-2) + \sigma(n-5) + \sigma(n-7) \\ - \sigma(n-12) - \sigma(n-15) + \dots = 0$$

if the series is extended as long as the arguments do not become negative and the meaningless symbol $\sigma(0)$, when it appears, is replaced by n .

This celebrated formula can be conveniently used in forming a table of the sums of divisors without factorization of the numbers into primes.

Though discovered by analytical means, Euler's recurrence formula can be proved in various ways by very elementary methods. The exposition of these must be deferred to other chapters of this book.

10. Perfect Numbers. The problem of perfect numbers, a favorite with ancient Greeks, owes its origin to the number mysticism of the Pythagoreans. The number 6 has divisors 1, 2, 3, 6. Excluding, as ancients always did, the number itself from the set of divisors, it is easy to observe that $6 = 1 + 2 + 3$. Again, the divisors of 28 with the exclusion of the

number itself are 1, 2, 4, 7, 14 and $28 = 1 + 2 + 4 + 7 + 14$. Thus 6 and 28 both possess the property of being equal to the sum of their aliquot parts, and on this account were considered as "perfect numbers."

In the infancy of science the speculation on such perfect numbers enjoyed a certain amount of popularity, which is evidenced by the fact that in Euclid a rule is given for obtaining even perfect numbers. Euclid's rule amounts to the statement that

$$2^{p-1}(2^p - 1)$$

is a perfect number if $2^p - 1$ is a prime. To verify it is an easy matter. In fact the divisors of Euclid's number, excluding the number itself, are

$$\begin{array}{ccccccc} 1, & 2, & 2^2, & \dots, & 2^{p-1} \\ 2^p - 1, & 2(2^p - 1), & 2^2(2^p - 1), & \dots, & 2^{p-2}(2^p - 1) \end{array}$$

and their sum is

$$\begin{aligned} 1 + 2 + 2^2 + \dots + 2^{p-1} + (2^p - 1)(1 + 2 \\ + \dots + 2^{p-2}) &= 2^p - 1 + (2^p - 1)(2^{p-1} - 1) \\ &= 2^{p-1}(2^p - 1). \end{aligned}$$

It is not difficult to show that all even perfect numbers are necessarily of Euclid's type. This problem amounts to finding for what even n the following equation holds:

$$\sigma(n) = 2n.$$

Since n is supposed to be even, we can set

$$n = 2^{p-1}m, \quad p > 1$$

where m is odd. Then, since

$$\sigma(n) = (2^p - 1)\sigma(m),$$

the condition of the problem is

$$(2^p - 1)\sigma(m) = 2^pm.$$

Now 2^p and $2^p - 1$ are relatively prime numbers; consequently

$$m = (2^p - 1)r$$

$$\sigma(m) = 2^p r,$$

where r is a certain integer. Numbers r and m are two distinct divisors of m , and their sum

$$r + (2^p - 1)r = 2^p r$$

makes up already what should be the sum of all divisors of m . Consequently m has only two divisors; that is, m is prime, which is possible only when $r = 1$ and $2^p - 1$ is prime. Thus an even perfect number must be of the form

$$2^{p-1}(2^p - 1).$$

Numbers of the form $2^p - 1$ are called Mersenne's numbers because of a statement made concerning them in the preface to his "Cogitata physico-mathematica," published in 1644. Mersenne implied that the only values of p , not greater than 257, for which $2^p - 1$ is prime are

2, 3, 5, 7, 13, 17, 19, 31, 67, 127, and 257.

Whether this statement followed a detailed analysis of the problem or is more or less a conjecture is not known. Subsequent analysis, including the work of present-day investigators, has yielded the following results:

For the values

2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, and 127

$2^p - 1$ is certainly a prime number. For all other primes not exceeding 257, Mersenne's numbers are composite except perhaps for some of the following six values:

157, 167, 193, 199, 227, 229,

for which the character of $2^p - 1$ is as yet unknown.¹

¹ The authors are indebted for these results to Professor D. H. Lehmer, whose contributions to this subject are well known.

Exercises and Problems

1. Find the smallest numbers with 10, 18, 24 divisors, respectively.
Ans. 48, 180, and 360.

2. Show that $\sigma(N) = 4N$ when $N = 30,240$.

3. Two numbers are said to be "amicable" (or "friendly") if each equals the sum of the aliquot parts of the other. Hence, if M and N are amicable, we have

$$\sigma(M) = \sigma(N) = M + N.$$

Show that the number pairs 284, 220; and 17,296, 18,416 are amicable.

4. A chain of numbers is said to be "sociable" if each is the sum of the aliquot parts of the preceding number, the last being considered as preceding the first number of the chain. Show that the following numbers form a sociable chain:

$$14,288 \quad 15,472 \quad 14,536 \quad 14,264 \quad 12,496$$

5. The only numbers which are not sums of consecutive integers are powers of 2.

6. Prove that the sum of reciprocals of the divisors of a perfect number is equal to 2.

7. Show that the number of divisors of an integer is odd if and only if this integer is a square.

8. Prove that the product of all divisors of n is $n^{\frac{1}{2}\tau(n)}$.

9. In how many ways can an integer be factored into relatively prime factors? *Ans.* If ν is the number of distinct prime factors of the integer, then the number of the required factorizations is $2^{\nu-1}$.

10. Find the expression for the sum of the r th powers of the divisors of an integer.

11. Show that an integer N can be represented as a difference of two squares if it is either odd or divisible by 4, otherwise not. The representation is unique if and only if N is a prime number.

12. Find all the positive integers x which make $x(x+180)$ a square.

$$\text{Ans. } x = 12, 16, 60, 144, 320, 588, 1,936.$$

13. Represent in all possible ways 1,547 and 1,768 as a difference of two squares.

$$\text{Ans. (a) } 1,547 = 774^2 - 773^2 = 114^2 - 107^2 = 66^2 - 53^2 = 54^2 - 37^2.$$

$$(b) 1,768 = 443^2 - 441^2 = 223^2 - 219^2 = 47^2 - 21^2 = 43^2 - 9^2.$$

14. Prove that

$$\sum_{d/n} \tau(d)^2 = \left[\sum_{d/n} \tau(d) \right]^2$$

where the summations extend over divisors of n . *HINT:* Both members are factorable numerical functions.

15. How would one find out whether a given fraction a/b , in smallest terms, can be split into two unit fractions; that is, whether the equation

$$\frac{a}{b} = \frac{1}{x_1} + \frac{1}{x_2}$$

can be solved in positive integers x_1, x_2 ? *Indication of Solution:* Let m be a divisor of b without square factors (that is, m nondivisible by any square except 1). Seek, if possible, such factorizations of b/m

$$\delta\delta' = \frac{b}{m}$$

www.dbraulibrary.org.in

that $\delta \leq \delta'$ and $\delta + \delta'$ is divisible by a . If $\delta + \delta' = ac$, then

$$x_1 = mc\delta, \quad x_2 = mc\delta'$$

16. Split $\frac{46}{455}$ and $\frac{59}{70}$ into as few unit fractions as possible.

17. Devise a method for solving the Diophantine equation

$$x^4 + px^3 + qx^2 + rx + s = y^2$$

in integers x, y . The coefficients p, q, r, s are given integers. *Indication of Solution:* The proposed equation can be presented thus

$$\begin{aligned} \left(x^2 + \frac{1}{2}px + \frac{1}{2}q - \frac{1}{8}p^2 + y\right) \left(x^2 + \frac{1}{2}px + \frac{1}{2}q - \frac{1}{8}p^2 - y\right) \\ = \frac{1}{4} \left(q - \frac{p^2}{4}\right)^2 - s + \left(\frac{pq}{2} - \frac{p^3}{8} - r\right)x \end{aligned}$$

whence, with both signs \pm ,

$$\left|x^2 + \frac{1}{2}px + \frac{1}{2}q - \frac{1}{8}p^2 \pm y\right| \leq 8 \left| \left(\frac{pq}{2} - \frac{p^3}{8} - r\right)x + \frac{1}{4} \left(q - \frac{p^2}{4}\right)^2 - s \right|$$

unless the right-hand side equals 0. Consequently

$$\left| x^2 + \frac{1}{2}px + \frac{1}{2}q - \frac{p^2}{8} \right| \leq 8 \left| \left(\frac{pq}{2} - \frac{p^2}{8} - r \right) x + \frac{1}{4} \left(q - \frac{p^2}{4} \right)^2 - s \right|$$

whereby the number of possible values of x is limited.

13. Solve in integers

$$(a) \quad x^4 + x^3 + x^2 + x + 1 = y^2,$$

$$(b) \quad x^4 + 2x^3 + 8x + 8 = y^2,$$

$$(c) \quad x(x+1)(x+2)(x+3) + 1 = y^2.$$

Ans. (a) $x = -1, 0, 3$; (b) no solution; (c) all integers are solutions.

11. **Number of Primes Infinite.** It is quite natural to ask the question: Is the series of primes infinite like the series of integers themselves? That this question can be answered in the affirmative was known to the ancient Greeks. In fact Euclid, in his "Elements," gives a remarkably simple proof of the following proposition. www.dbraulibrary.org.in

THEOREM. To any given set of primes a prime not belonging to the set can be added. We express this by saying that the series of primes is infinite.

PROOF. Let p be the greatest prime of the set, then primes

$$2, 3, 5, \dots, p$$

taken in their natural order comprise the given set of primes. With Euclid we form the number

$$P = 2 \cdot 3 \cdot 5 \cdots p + 1.$$

If this number is prime, it is not contained in the set, since it is greater than p . If P is composite, it has a prime divisor π which is different from 2, 3, 5, \dots , p . For if π were identical with one of these primes, both P and $2 \cdot 3 \cdot 5 \cdots p$ as well as their difference 1 would be divisible by it, which is impossible. Thus a prime can always be produced which does not belong to any given set of primes.

The same can be expressed in a different way. Let

$$p_1 = 2, \quad p_2 = 3, \quad p_3 = 5, \quad p_4 = 7, \dots$$

be primes in their natural order so that p_n denotes the n th prime. From Euclid's proof it follows that between p_n and $p_1 p_2 p_3 \cdots p_n + 1$ inclusive there is at least one prime. If there are several the smallest will be p_{n+1} so that

$$p_{n+1} \leq p_1 p_2 p_3 \cdots p_n + 1.$$

Of course this inequality can be slightly improved by considering

$$p_1 p_2 \cdots p_n - 1$$

instead of Euclid's number P , only then we must suppose $n > 1$. Thus, with a slight modification of Euclid's reasoning, we have a slightly better result

$$p_{n+1} \leq p_1 p_2 \cdots p_n - 1$$

for $n > 1$.

It was very difficult to improve on the above result. The first notable success in this direction was achieved by the great Russian mathematician Tshebysheff (1821-1894) who in 1851 was able to prove the following result: between a and $2a - 2$ for any $a > \frac{1}{2}$ there is always at least one prime. From this it follows immediately that for $n \geq 1$

$$p_{n+1} < 2p_n.$$

Though Tshebysheff's proof is rather elementary it is long and requires some preparations, and for these reasons we do not give it here. Instead we shall give a very simple proof of the inequality

$$p_{n+1}^2 < p_1 p_2 \cdots p_n$$

for $n \geq 4$, due to Bonse. This inequality is not nearly so sharp as $p_{n+1} < 2p_n$ but it maintains a certain interest on account of the simplicity of the proof.

Now every prime divisor of N , being different from p_1, p_2, \dots, p_n , must be $\geq p_{n+1}$; moreover, $l \leq p_i$, and consequently

$$p_{n+1} \leq N \leq p_1 p_2 \cdots p_{i-1} p_i - 1.$$

Hence

$$p_{n+1} < p_1 p_2 \cdots p_{i-1} p_i$$

provided

$$n - i + 1 < p_i.$$

Let i be the smallest number satisfying the above inequality. Then

$$n - (i - 1) + 1 \geq p_{i-1}$$

or

$$n - i \geq p_{i-1} - 2.$$

On the other hand,

$$p_{i-1} - 2 \geq i$$

if $i \geq 5$. In fact, if this inequality is true for some value of i , it will be true after replacing i by $i + 1$. For $p_i \geq p_{i-1} + 2$, $p_i - 2 \geq p_{i-1} \geq 2 + i > i + 1$. But for $i = 5$ the inequality is verified, and so it holds for all $i \geq 5$.

Now if $n \geq 10$, the smallest value of i for which $n - i + 1 < p_i$ or $n < p_i + i - 1$ must be ≥ 5 because if it were ≤ 4 then n would be $< p_4 + 3 = 7 + 3 = 10$. Thus, if $n \geq 10$ we have necessarily

$$n - i \geq i.$$

Comparing the products

$$p_1 p_2 \cdots p_i \quad p_{i+1} \cdots p_n,$$

we see that the second consists of at least as many factors as the first, and besides

$$p_{i+1} > p_1, \quad p_{i+2} > p_2, \quad \dots, \quad p_{2i} > p_i.$$

Consequently

$$p_1 p_2 \cdots p_i < p_{i+1} p_{i+2} \cdots p_n$$

and

$$(p_1 p_2 \cdots p_i)^2 < p_1 p_2 \cdots p_n.$$

Since, on the other hand,

$$p_{n+1} < p_1 p_2 \cdots p_i$$

we shall have

$$p_{n+1}^2 < p_1 p_2 \cdots p_n$$

for $n \geq 10$. But this inequality is true already for $n \geq 4$, as can be verified directly.

13. A Property of 30. Examining the small numbers $n = 2, 3, 4, 5, \dots$ one discovers that in the following cases:

$$n = 2, 3, 4, 6, 8, 12, 18, 24, 30$$

the numbers less than n and relatively prime to n are unity and primes. After 30, no matter how far we go, no more numbers with this property occur, and one may suspect that 30 is the greatest number possessing this property, that numbers less than and relatively prime to it are either one or primes. This guess can be proved by using the inequality established in the preceding section.

Let $n > 4$ be a number possessing the requisite property and let p_k be the greatest prime not exceeding \sqrt{n} , so that

$$p_k^2 \leq n < p_{k+1}^2.$$

Then n must be divisible by p_1, p_2, \dots, p_k and consequently by their product. For suppose that n is not divisible by p_α ($\alpha = 1, 2, \dots, k$), then n is prime to p_α and to p_α^2 ; that is, there is a composite number p_α^2 less than n and relatively prime to it. Since n is divisible by p_1, p_2, \dots, p_k , we have

$$p_1 p_2 \cdots p_k \leq n.$$

On the other hand

$$n < p_{k+1}^2$$

and so

$$p_{k+1}^2 > p_1 p_2 \cdots p_k.$$

But this is impossible for $k \geq 4$; consequently $k \leq 3$ and $n < p_4^2 = 49$. Since there are no numbers of the requisite property between 30 and 48, 30 must be the greatest of them.

14. Remarks on the Distribution of Primes. Even casual examination of tables of primes reveals that primes are distributed in the series of integers in the most irregular manner. As far as we can go, over and over again we find consecutive primes with the smallest difference 2. Whether there are infinitely many of these so-called "twin primes" nobody knows; this is one of the most difficult unsolved problems concerning primes. On the other hand, consecutive primes often have large differences. That pairs of consecutive primes with arbitrarily large differences must occur can be shown very simply. For consider the $n - 1$ consecutive integers

$$n! + 2, \quad n! + 3, \quad \dots, \quad n! + n.$$

They are all composite, and it follows that there are two consecutive primes differing by more than any given number. On account of the great irregularity in the distribution of primes, it is hardly possible to expect that the number of primes not exceeding a given limit can be exactly represented by any simple formula. However, a remarkable expression exists which gives the approximate number of primes not exceeding a given limit x . Denote the number of primes $\leq x$ by $\pi(x)$; then approximately

$$\pi(x) = \int_2^x \frac{dt}{\log t} = Li(x).$$

The integral on the right-hand side is a function of comparatively simple nature, the so-called "integral logarithm," and it is amazing that it can approximately represent such an irregular function as $\pi(x)$. The following table gives some idea as to how close $\pi(x)$ is represented by the integral logarithm:

x	$\pi(x)$	$Li(x)$	Discrepancy
500,000	41,539	41,606	67
1,000,000	78,499	78,628	129
1,500,000	114,156	114,263	107
2,000,000	148,934	149,055	121
2,500,000	183,073	183,245	172
3,000,000	216,817	216,971	154
4,000,000	283,147	283,352	205
5,000,000	348,514	348,638	124
6,000,000	412,850	413,077	227
7,000,000	476,649	476,827	178
8,000,000	539,778	540,000	222
9,000,000	602,490	602,676	186
10,000,000	664,580	664,918	338

That the integral logarithm represents approximately the number of primes not exceeding x gives a limit is not merely a fact of observation but has been proved theoretically, though by very intricate analytical investigation. Let us set

$$\pi(x) = \int_2^x \frac{dt}{\log t} + R(x).$$

The best result hitherto proved concerning the error $R(x)$ is that the ratio of $R(x)$ to

$$xe^{-k\sqrt{\log x \log \log x}},$$

where k is a certain numerical constant, remains bounded as x tends to infinity, which implies that $R(x)$ for large x becomes insignificant in comparison to $Li(x)$ and in this sense $Li(x)$ is an approximation to $\pi(x)$. If it is true, which appears very probable but remains as yet unproved, that a certain transcendental function introduced by Riemann has only real roots, then it can be shown that the ratio of $R(x)$ to $\sqrt{x} \log x$ remains bounded or, speaking roughly, $R(x)$ for large x is comparable to

\sqrt{x} . On the other hand $R(x)$, as far as the order of magnitude is concerned, cannot be very much smaller than \sqrt{x} . In fact it has been proved that with a certain constant K there are values of x as large as we please, such that

$$R(x) > K \frac{\sqrt{x}}{\log x}$$

and also

$$R(x) < -K \frac{\sqrt{x}}{\log x}.$$

How important it is to have everything proved rigorously in investigations of this nature and not to rely on observations, no matter how extensive they are, is shown by the following fact. In the whole extent of existing tables of primes the inequality

$$\pi(x) < Li(x)$$

has been verified constantly; that is, many millions of times. Yet it is not true in general. It has been proved that for infinitely many x as large as we please we may have either

$$\pi(x) < Li(x)$$

or

$$\pi(x) > Li(x).$$

Values of x for which the last inequality holds are, however, far beyond the limits of the existing tables.

Of necessity we must confine ourselves in regard to the fascinating problem of the distribution of primes to mere statements of facts. Their proofs belong to the analytical theory of numbers, a very vast and very difficult branch of our science in which properties of numbers are investigated by methods involving transcendental notions such as continuity, etc.

15. Primes in Arithmetic Progressions. Since primes, except 2, are odd numbers, the fact that the series of primes

is infinite is equivalent to the statement that the arithmetic progression $2x + 1$, of odd numbers, contains infinitely many primes. Looking at the matter from this point of view, it is quite natural to inquire whether an arithmetic progression $ax + b$, whose first term b and difference a are relatively prime numbers, contains infinitely many primes or not. For instance, all odd numbers fall into two progressions: one containing numbers of the form $4x + 1$,

$$1, 5, 9, 13, 17, \dots,$$

and the other numbers of the form $4x - 1$,

$$3, 7, 11, 15, 19, \dots$$

Also all odd numbers nondivisible by 3 fall into two progressions: one containing numbers of the form $6x + 1$,

$$1, 7, 13, 19, 25, 31, \dots$$

and the other numbers of the form $6x - 1$,

$$5, 11, 17, 23, \dots$$

Each of these progressions contains prime numbers, but does each of them contain infinitely many primes?

By extremely ingenious analytical methods Dirichlet, in 1837, was able to prove that every arithmetic progression whose first term and difference are relatively prime numbers contains infinitely many primes. In other words, there are infinitely many primes of the form $ax + b$ where a and b are arbitrary relatively prime integers. As yet no arithmetical proofs of this general proposition have been discovered, although there are such proofs for some particular progressions.

16. Some Unsolved Problems Concerning Primes. On the subject of primes it is much easier to set problems than to solve them. We shall mention some such unsolved problems.

1. Are there infinitely many pairs of twin primes?
2. Are there infinitely many primes of the form $x^2 + 1$?
3. Is it true that between any two consecutive squares n^2 and $(n + 1)^2$ there is always at least one prime?
4. An obscure mathematician of the eighteenth century, Goldbach, stated that every even number > 4 is a sum of two primes. Is this true in general?

Quite recently, in 1937, Vinogradov by analytical methods of extreme subtlety was able to prove that every sufficiently large odd number is a sum of three primes. Of course this will be true for all odd numbers > 7 if Goldbach's statement holds in general.

Exercises and Problems

1. Prove that 24 is the largest number divisible by all numbers not exceeding its square root.

2. Prove that for $n \geq 5$

$$p_{n+1} < p_1 p_2 \cdots p_n$$

$$p_{n+1}^3 < p_1 p_2 \cdots p_n$$

HINT: $p_{i-1} \geq 2i + 2$ for $i \geq 10$.

3. Prove that there are infinitely many primes of the form $4x - 1$.
HINT: Take a group of primes of this form 3, 7, 11, . . . , p and consider the number $P = 4 \cdot 3 \cdot 7 \cdot 11 \cdots p - 1$. Notice that primes of the form $4x + 1$, when multiplied, produce a number of the same form.

4. Prove that there are infinitely many primes of the form $6x - 1$.

5. Prove that there are infinitely many primes by observing that in the series

$$2^2 + 1, 2^{2^2} + 1, 2^{2^3} + 1, 2^{2^4} + 1, \dots$$

every two numbers are relatively prime.

6. Prove that the factorial $1 \cdot 2 \cdot 3 \cdot 4 \cdots n$ for $n > 1$ cannot be a square or cube or any other power of an integer. HINT: There is always a prime between $n/2$ and n if $n \geq 4$.

17. Integral Part of a Real Number. On many occasions it is necessary to consider the greatest integer not exceeding a given real number x . This integer is denoted by $E(x)$ or by $[x]$, the last notation being almost universally adopted at the

present time. The integer $[x]$, by its very definition, satisfies the inequalities

$$[x] \leq x < [x] + 1$$

and may be called "integral part of x " or "integer contained in x ." For example

$$[2\frac{1}{2}] = 2, \quad [\sqrt{2}] = 1, \quad [-\sqrt{2}] = -2.$$

The inequalities serving to define $[x]$ are equivalent to the representation of x in the form

$$x = [x] + \theta$$

where $0 \leq \theta < 1$ and θ may be called the "fractional part of x ."

A few properties of $[x]$ follow almost immediately from its definition:

(a) $[x + m] = [x] + m$, if m is an integer.

(b) $[x] + [-x] = 0$ or -1 , according as x is an integer or not.

(c) $[x + y] \geq [x] + [y]$.

(d) $\left[\frac{[x]}{n} \right] = \left[\frac{x}{n} \right]$, if n is a positive integer.

Property (a) may be considered as evident. So is property (b) if x is an integer. To prove it when x is not an integer, we notice that in this case

$$x = [x] + \theta, \quad 0 < \theta < 1;$$

consequently

$$-x = -[x] - 1 + (1 - \theta)$$

and $0 < 1 - \theta < 1$, whence

$$[-x] = -[x] - 1,$$

which is the same as (b). To prove (c) let

$$\begin{aligned} x &= [x] + \theta; & 0 \leq \theta < 1 \\ y &= [y] + \theta'; & 0 \leq \theta' < 1. \end{aligned}$$

Then

$$x + y = [x] + [y] + \theta + \theta',$$

whence, by using property (a),

$$[x + y] = [x] + [y] + [\theta + \theta'].$$

Now $0 \leq \theta + \theta' < 2$, whence $[\theta + \theta'] = 0$ or 1 according as $\theta + \theta' < 1$ or $\theta + \theta' \geq 1$, and correspondingly

$$[x + y] = [x] + [y]$$

or

$$[x + y] = [x] + [y] + 1.$$

To prove (d), let q and r be respectively the quotient and the remainder in the division of $[x]$ by n , so that

$$[x] = nq + r; \quad 0 \leq r \leq n - 1.$$

Then

$$x = nq + r + \theta, \quad 0 \leq \theta < 1$$

and

$$\frac{x}{n} = q + \frac{r + \theta}{n}.$$

But

$$0 \leq \frac{r + \theta}{n} < 1,$$

whence it follows that

$$\left[\frac{x}{n} \right] = q = \left[\frac{[x]}{n} \right].$$

Other useful properties of the symbol $[x]$ will be found in the exercises.

From the definition of $[x]$ it follows that the number of integers m satisfying the inequalities

$$y < m \leq x$$

is always given correctly by

$$[x] - [y].$$

Hence, in particular, $[x]$ is the number of positive integers not exceeding x .

One must not confuse the integral part of x with the "nearest integer to x ." The latter is defined as an integer a satisfying the inequality

$$|x - a| \leq \frac{1}{2}.$$

Unless x is equal to an integer $+ \frac{1}{2}$, the nearest integer is uniquely determined; otherwise there are two nearest integers, $x - \frac{1}{2}$, $x + \frac{1}{2}$, both distant from x by $\frac{1}{2}$. We leave it to the reader to prove that in all cases

$$\left[x + \frac{1}{2} \right]$$

is the nearest integer to x .

Exercises and Problems

1. Prove that

$$[2x] - 2[x] = 0 \text{ or } 1$$

according as the fractional part of x is $< \frac{1}{2}$ or $\geq \frac{1}{2}$.

2. According as the fractional part of x is $< \alpha$ or $\geq \alpha$ ($0 < \alpha < 1$),

$$[x] - [x - \alpha] = 1 \text{ or } 0.$$

3. Prove that

$$[2x] + [2y] \geq [x] + [y] + [x + y].$$

4. Prove that for a positive integer n and any real x

$$[x] + \left[x + \frac{1}{n} \right] + \left[x + \frac{2}{n} \right] + \cdots + \left[x + \frac{n-1}{n} \right] = [nx].$$

5. Prove that for an integer x

$$\left[\frac{x - 15 - \left[\frac{x - 17}{25} \right]}{3} \right] = \left[\frac{8x + 13}{25} \right] - 5.$$

6. If P and Q are two positive relatively prime integers, then

$$\sum_{1}^{P-1} \left[\frac{Qx}{P} \right] = \frac{(P-1)(Q-1)}{2},$$

and if $(P, Q) = d$

$$\sum_1^{P-1} \left[\frac{Qx}{P} \right] = \frac{(P-1)(Q-1)}{2} + \frac{d-1}{2}.$$

HINT: Notice that

$$\sum_1^{P-1} \left[\frac{Qx}{P} \right] = \sum_{x=1}^{P-1} \left[\frac{Q(P-x)}{P} \right].$$

7. Show that

$$[(1 + \sqrt{3})^{2n}] + 1 \quad \text{and} \quad [(1 + \sqrt{3})^{2n+1}]$$

are both divisible by 2^{n+1} . Is this the highest power of 2 dividing either of the numbers? HINT: $(1 + \sqrt{3})^n + (1 - \sqrt{3})^n$ is an integer and $-1 < 1 - \sqrt{3} < 0$.

8. Show that the nearest integer to $(3 + \sqrt{5})^n$ for $n > 2$ is divisible exactly by 2^n if n is not divisible by 3, and by 2^{n+1} if n is divisible by 3.

9. Two series of numbers

$$[ax], [bx] \text{ for } x = 1, 2, 3, \dots$$

comprise all integers $1, 2, 3, \dots$ without repetition if a and b are positive irrational numbers such that

$$\frac{1}{a} + \frac{1}{b} = 1.$$

10. Prove that

$$\sum_{d=1}^n (2d-1) \left[\frac{n}{d} \right] = \sum_1^n \left[\frac{n}{d} \right]^2.$$

HINT: Express the sum

$$\sum \delta,$$

extended over all solutions of the inequality $d\delta \leq n$ in positive integers, in two ways.

11. Show that

$$\tau(1) + \tau(2) + \dots + \tau(n) = \sum_{d=1}^n \left[\frac{n}{d} \right].$$

HINT: Count in two ways the number of solutions of the inequality $d\delta \leq n$ in positive integers.

12. Show that

$$\tau(1) + \tau(2) + \cdots + \tau(n) = 2 \sum_{d=1}^{\sqrt{n}} \left[\frac{n}{d} \right] - [\sqrt{n}]^2.$$

HINT: The number of divisors of m is twice the number of solutions of the equation

$$d(d + \delta) = m$$

in positive integers, augmented by 1 in case m is a square.

18. The Highest Power of a Prime Contained in a Factorial.

Let $n! = 1 \cdot 2 \cdot 3 \cdots n$ be a factorial and p a given prime. Clearly p does not divide the factorial if $n < p$, and we may say, in this case, that p enters in $n!$ in the 0 power. If $p \leq n$, then $n!$ is divisible by p and it is interesting to find the highest power in which p enters in $n!$. Let us denote the exponent of this power by $\nu(n)$. Among the numbers $1, 2, 3, \dots, n$ only $p, 2p, 3p, \dots$ are divisible by p ; moreover, the greatest number divisible by p and not exceeding n is $n_1 p$ where

$$n_1 = \left[\frac{n}{p} \right].$$

Consequently $\nu(n)$ is the exponent of the highest power in which p enters in the product

$$p \cdot 2p \cdot 3p \cdots n_1 p = p^{n_1} \cdot 2 \cdot 3 \cdots n_1.$$

But in $1 \cdot 2 \cdots n_1$, the prime p occurs in power with the exponent $\nu(n_1)$; hence

$$\nu(n) = n_1 + \nu(n_1).$$

In the same way we find

$$\nu(n_1) = n_2 + \nu(n_2)$$

$$\nu(n_2) = n_3 + \nu(n_3)$$

$$\dots \dots \dots$$

where

$$n_2 = \left[\frac{n_1}{p} \right], \quad n_3 = \left[\frac{n_2}{p} \right], \quad \dots$$

are decreasing positive integers and n_k , for some k , becomes $< p$. Then $\nu(n_k) = 0$, and eliminating n_{k-1}, n_{k-2}, \dots from the system

$$\begin{aligned} \nu(n_{k-1}) &= n_k \\ \nu(n_{k-2}) &= n_{k-1} + \nu(n_{k-1}) \\ &\dots \\ \nu(n) &= n_1 + \nu(n_1), \end{aligned}$$

we find

$$\nu(n) = n_1 + n_2 + \dots + n_k.$$

By property (d), Sec. 17,

$$n_2 = \left[\frac{n}{p^2} \right], \quad n_3 = \left[\frac{n}{p^3} \right], \quad \dots$$

and so finally

$$\nu(n) = \left[\frac{n}{p} \right] + \left[\frac{n}{p^2} \right] + \left[\frac{n}{p^3} \right] + \dots,$$

the sum terminating as soon as the first term equal to 0 occurs, though nothing prevents us from continuing it farther if desirable.

Example. To find the highest power of 7 dividing $1,000!$ we determine

$$\left[\frac{1,000}{7} \right] = 142, \quad \left[\frac{1,000}{49} \right] = 20, \quad \left[\frac{1,000}{343} \right] = 2$$

$$\nu(1,000) = 142 + 20 + 2 = 164.$$

Thus 7^{164} is the highest power of 7 dividing $1,000!$

19. Some Applications. As an application we shall prove the

THEOREM. The product of n consecutive integers is divisible by $1 \cdot 2 \cdot 3 \cdot \dots \cdot n$.

PROOF. We are to prove that

$$G = \frac{(a+1)(a+2) \cdots (a+n)}{1 \cdot 2 \cdots n}$$

is an integer if a is an integer. It suffices to suppose that a is a positive integer. The statement can be proved in two ways.

First, G is the well-known expression for the number of combinations of $a+n$ elements taken n at a time; consequently it is an integer. If this meaning of G is not known, then we can reason as follows. If we write G as

$$G = \frac{(a+n)!}{n! a!}$$

then the exponents of the highest powers of any prime p , dividing $(a+n)!$, $n!$, $a!$, are, respectively,

$$\begin{aligned} & \left[\frac{a+n}{p} \right] + \left[\frac{a+n}{p^2} \right] + \cdots \\ & \left[\frac{n}{p} \right] + \left[\frac{n}{p^2} \right] + \cdots \\ & \left[\frac{a}{p} \right] + \left[\frac{a}{p^2} \right] + \cdots, \end{aligned}$$

all three sums being carried to the same number of terms. Now by property (c), Sec. 17,

$$\left[\frac{a+n}{p^i} \right] \geq \left[\frac{n}{p^i} \right] + \left[\frac{a}{p^i} \right],$$

and so

$$\sum_{i=1, 2, 3, \dots} \left[\frac{a+n}{p^i} \right] \geq \sum_{i=1, 2, \dots} \left[\frac{n}{p^i} \right] + \sum_{i=1, 2, \dots} \left[\frac{a}{p^i} \right].$$

That is, the prime p enters in the numerator $(a+n)!$ in power not lower than in the denominator $n! a!$ of the fraction repre-

sending G . Consequently, the numerator is divisible by the denominator and G is an integer.

As a second application we shall prove that the fraction

$$H = \frac{1 \cdot 3 \cdot 5 \cdots (2n-1)}{2 \cdot 4 \cdot 6 \cdots 2n},$$

when reduced to its simplest terms, is of the form

$$\frac{a}{2^\omega}$$

where a is odd and $\omega < 2n$. In fact

$$H = \frac{(2n)!}{2^{2n} n!} = \frac{1}{2^{2n}} \frac{(n+1)(n+2) \cdots (n+n)}{1 \cdot 2 \cdots n}$$

and

$$\frac{(n+1)(n+2) \cdots (n+n)}{1 \cdot 2 \cdot 3 \cdots n}$$

is an integer by the preceding theorem. Consequently the denominator of H , when reduced to simplest terms, is a power of 2. On the other hand, the exponents of the highest power of 2 occurring in $(2n)!$ and $n!$ are, respectively,

$$\sum \left[\frac{2n}{2^i} \right] \quad \text{and} \quad \sum \left[\frac{n}{2^i} \right], \quad i = 1, 2, 3, \dots$$

and

$$\omega = 2n + 2 \sum \left[\frac{n}{2^i} \right] - \sum \left[\frac{2n}{2^i} \right] = \sum \left[\frac{n}{2^i} \right] + n.$$

But

$$\sum_{i=1, 2, 3, \dots} \left[\frac{n}{2^i} \right] < \frac{n}{2} + \frac{n}{4} + \frac{n}{8} + \cdots = n,$$

and so $\omega < 2n$.

Exercises and Problems

1. Let n be represented in the scale with base (the prime p ; then

$$n = b_0 p^a + b_1 p^{a-1} + \dots + b_a;$$

$$0 \leq b_i < p; \quad i = 0, 1, 2, \dots, a; \quad b_a > 0$$

and the exponent of the highest power of p dividing $n!$ is

$$\nu(n) = \frac{n - (b_0 + b_1 + \dots + b_a)}{p - 1}.$$

2. Find the highest powers of 2, 3, 11 contained in 1,000!

3. With how many zeros does 253! end?

4. If a and b are positive integers, prove that

$$\frac{(2a)!(2b)!}{a!b!(a+b)!}$$

is an integer.

5. Show that

$$\frac{(a+b)!}{a!b!}$$

is an integer if a and b are positive integers.

6. Show that

$$G = \frac{n!}{a!b! \dots l!}$$

is an integer if a, b, c, \dots, l are positive integers with sum equal to n .

7. Show that under the same conditions

$$H = \frac{(n-1)!}{a!b! \dots l!}$$

is an integer if a, b, \dots, l are without common divisor. Hint: aH, bH, \dots, lH are integers.

8. Develop the method for finding the smallest value of n for which $n!$ is divisible exactly by a given power p^ω of a prime p . Apply to the numerical examples: (a) $p = 3, \omega = 100$, and (b) $p = 5, \omega = 41$. *Indication of Solution.* The requisite n must be divisible by p . When we set $n = px$, the problem reduces to solving the equation

$$x + \left[\frac{x}{p} \right] + \left[\frac{x}{p^2} \right] + \dots = \omega.$$

Express ω in the scale with p as a base

$$\omega = c_0 p^m + c_1 p^{m-1} + \dots + c_m$$

and seek x in the form

$$x = b_0 p^m + b_1 p^{m-1} + \dots + b_m;$$

$$0 \leq b_i < p; \quad i = 0, 1, 2, \dots, m.$$

If

$$\omega \geq p^m + p^{m-1} + \dots + p + 1,$$

the first digit

$$b_0 = \left[\frac{\omega(p-1)}{p^{m+1}-1} \right]$$

is > 0 . Set

$$x = b_0 p^m + x';$$

then x' is determined from the equation

$$x' + \left[\frac{x'}{p} \right] + \left[\frac{x'}{p^2} \right] + \dots = \omega'$$

where $\omega' < \omega$.

If

$$\omega < p^m + p^{m-1} + \dots + p,$$

then $b_0 = 0$ and

$$b_1 = \left[\frac{\omega(p-1)}{p^m-1} \right],$$

and, on setting

$$x = b_1 p^{m-1} + x',$$

x' satisfies the equation

$$x' + \left[\frac{x'}{p} \right] + \left[\frac{x'}{p^2} \right] + \dots = \omega'$$

with $\omega' < \omega$. The problem is impossible if

$$\omega = p^m + p^{m-1} + \dots + p.$$

Answers for Examples: (a) Problem impossible; (b) $n = 170$.

CHAPTER V

A GENERAL COMBINATORIAL THEOREM AND ITS APPLICATIONS

1. Combinatorial Theorem. Suppose we have a collection of objects which may or may not possess one or more of the characteristics A_1, A_2, \dots, A_n . Our problem is to find how many objects do not possess any of the characteristics A_1, A_2, \dots, A_n . Let N be the total number of objects in the collection, $N(A_i)$ the number of objects possessing a given character A_i , $N(A_i A_j)$ the number of objects possessing two given characters A_i and A_j , and so on. For example, let the objects be a collection of ten numbers $1, 2, 3, \dots, 10$, and let the three characters A_1, A_2, A_3 be the respective divisibility by 2, 3, and 5. Then evidently

$$\begin{aligned} N &= 10, & N(A_1) &= 5, & N(A_2) &= 3, & N(A_3) &= 2 \\ N(A_1 A_2) &= 1, & N(A_1 A_3) &= 1, & N(A_2 A_3) &= 0, \\ & & N(A_1 A_2 A_3) &= 0. \end{aligned}$$

With these notations adopted we have the following theorem:

THEOREM. The number of objects not possessing any of the characters A_1, A_2, \dots, A_n is

$$\begin{aligned} N - \sum_i N(A_i) + \sum_{i,j} N(A_i A_j) - \sum_{i,j,k} N(A_i A_j A_k) + \dots \\ + (-1)^n N(A_1 A_2 \dots A_n) \end{aligned}$$

where the summation is extended over all combinations of the subscripts $1, 2, \dots, n$ in groups of one, two, three, and so on, and the signs of the terms alternate.

PROOF. The number of objects with character A_1 is $N(A_1)$; so, subtracting it from N , we have

$$N - N(A_1)$$

objects left not possessing the character A_1 . This agrees with the general formula for $n = 1$. To find the number of objects not possessing any of the characters A_1, A_2 , we notice that the number of objects with character A_2 is $N(A_2)$, and among them there are objects with both characters A_1 and A_2 . Consequently

$$N(A_2) - N(A_1A_2)$$

is the number of objects with character A_2 and without A_1 . Subtracting this number from the number of all objects without character A_1 , we have left

$$N - N(A_1) - N(A_2) + N(A_1A_2)$$

objects not possessing characters A_1 and A_2 in agreement with the general formula for $n = 2$. Again the number of objects possessing character A_3 and not possessing characters A_1 and A_2 is

$$N(A_3) - N(A_1A_3) - N(A_2A_3) + N(A_1A_2A_3).$$

Subtracting this number from the number of objects devoid of characters A_1 and A_2 , we get

$$N - N(A_1) - N(A_2) - N(A_3) + N(A_1A_2) + N(A_1A_3) \\ + N(A_2A_3) - N(A_1A_2A_3)$$

as the number of objects devoid of characters A_1, A_2, A_3 . Though the first three steps give a clear insight as to the validity of the general statement, we can present a formal proof by resorting to induction.

Assume as true that the number of objects devoid of characters A_1, A_2, \dots, A_{m-1} is given by

$$N - \sum_i N(A_i) + \sum_{i,j} N(A_iA_j) - \dots$$

where i runs through the numbers $1, 2, \dots, m-1$; where i, j run over all combinations of them in groups of two; and so on. The number of objects with character A_m but devoid of characters A_1, A_2, \dots, A_{m-1} , by virtue of our assumption, is

$$N(A_m) - \sum_i N(A_i A_m) + \sum_{i,j} N(A_i A_j A_m) - \dots,$$

the extent of summation being the same as before. The number of objects devoid of characters A_1, A_2, \dots, A_m will be

$$N - N(A_m) - \sum_i N(A_i) + \sum_i N(A_i A_m) + \sum_{i,j} N(A_i A_j) - \dots$$

But clearly

$$N(A_m) + \sum_i N(A_i)$$

is the sum

$$\sum_i N(A_i)$$

where i now runs through $1, 2, \dots, m$. Also

$$\sum_i N(A_i A_m) + \sum_{i,j} N(A_i A_j)$$

is

$$\sum_{i,j} N(A_i A_j)$$

where i, j run through all combinations of the numbers $1, 2, \dots, m$ in groups of two; and so on. Thus if the expression given in the theorem is true for $n = m - 1$, it will be true for $n = m$ and therefore, being true for $n = 1$, will be true in general.

2. Euler's Function $\varphi(n)$. The general combinatorial formula of the preceding section will prove very useful in deriving the expression for the number of positive integers

not exceeding n and relatively prime to n . This number, denoted by Euler by the sign $\varphi(n)$, is an important numerical function called "Euler's φ -function." From the definition it follows that $\varphi(1) = 1$. To find $\varphi(n)$ for $n > 1$ we suppose that n is factored into a product of powers of primes

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}.$$

An integer will be prime to n if and only if it is not divisible by any of the primes p_1, p_2, \dots, p_s . Therefore $\varphi(n)$ is the number of integers in the collection $1, 2, \dots, n$ which are not divisible by any of these primes. Now let A_1, A_2, \dots, A_s stand for divisibility, respectively, by p_1, p_2, \dots, p_s . Then $\varphi(n)$ is the number of integers $1, 2, \dots, n$ devoid of characters A_1, A_2, \dots, A_s and, as such, can be determined by the general formula of Sec. 1.

To find out how many integers possess one or more of the given characters, we must first find how many integers $1, 2, \dots, n$ are divisible by a number of the form

$$P = p_i p_j \cdots p_l$$

where i, j, \dots, l is some combination of the subscripts $1, 2, \dots, s$. Now all the integers divisible by P are Pt with $t = 1, 2, 3, \dots$, and among them those which are $\leq n$ correspond to

$$t = 1, 2, \dots, \frac{n}{P}.$$

Thus with the notation of Sec. 1

$$N(A_i A_j \cdots A_l) = \frac{n}{p_i p_j \cdots p_l},$$

and consequently

$$\begin{aligned} \varphi(n) = n - \sum_i \frac{n}{p_i} + \sum_{i, j} \frac{n}{p_i p_j} - \sum_{i, j, k} \frac{n}{p_i p_j p_k} + \cdots \\ + (-1)^s \frac{n}{p_1 p_2 \cdots p_s}. \end{aligned}$$

This expression is equivalent to the product

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_s}\right).$$

Notice that in case n is a power of a prime: $n = p^\alpha$, the formula for $\varphi(p^\alpha)$ becomes

$$\varphi(p^\alpha) = p^\alpha \left(1 - \frac{1}{p}\right) = p^\alpha - p^{\alpha-1},$$

and in the general case

$$\varphi(n) = \varphi(p_1^{\alpha_1}) \varphi(p_2^{\alpha_2}) \cdots \varphi(p_s^{\alpha_s}),$$

which shows that $\varphi(n)$ is a factorable numerical function.

Example. Let $n = 360 = 2^3 \cdot 3^2 \cdot 5$; then

$$\varphi(360) = 360 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right) = 96.$$

3. Moebius's Function $\mu(n)$. The first expression for $\varphi(n)$ can be put into more condensed form. Let a denote the divisors of $p_1 p_2 \cdots p_s$, including 1, which are composed of an even number of prime factors; also let b denote the divisors of the same number composed of an odd number of prime factors. Then a and b together represent all square-free divisors (that is, divisors not divisible by a square except 1) of n , and the formula for $\varphi(n)$ can be presented thus

$$\varphi(n) = n \sum_a \frac{1}{a} - n \sum_b \frac{1}{b},$$

the suffixes a and b indicating that the respective summations are extended over all divisors a and b .

The same formula can be exhibited in a still more condensed and elegant way by introducing a new numerical function $\mu(n)$, Moebius's function, with the following definition

$$\mu(1) = 1$$

$$\mu(n) = 0 \text{ if } n \text{ is divisible by a square } > 1.$$

$$\mu(n) = +1 \text{ if } n \text{ is square-free and contains an even number of primes.}$$

$$\mu(n) = -1 \text{ if } n \text{ is square-free and contains an odd number of primes.}$$

Thus, for example,

$$\begin{aligned} \mu(1) = 1, \mu(2) = -1, \mu(3) = -1, \mu(4) = 0, \mu(5) = 1, \\ \mu(6) = +1, \mu(7) = -1, \mu(8) = 0, \mu(9) = 0. \end{aligned}$$

With the help of the Moebius function, $\varphi(n)$ can be exhibited thus:

$$\varphi(n) = n \sum_{d|n} \frac{\mu(d)}{d},$$

where now the summation extends over all divisors of n . In fact terms corresponding to divisors which are divisible by squares > 1 are zeros, and the other terms correspond to square-free divisors previously denoted by a and b ; but by definition $\mu(a) = +1$ and $\mu(b) = -1$.

At first sight Moebius's function appears only as a means to write the expression for $\varphi(n)$ in an abbreviated and elegant form. But it is much more than that, as the following observation shows. It has been found empirically and verified up to $n = 500,000$ that the sum

$$\mu(1) + \mu(2) + \mu(3) + \cdots + \mu(n)$$

numerically is constantly less than \sqrt{n} . If it is true, though it has never been proved, that

$$\frac{\mu(1) + \mu(2) + \cdots + \mu(n)}{\sqrt{n}}$$

remains bounded for all n , then it would follow that the roots of the transcendental function mentioned in Sec. 14, Chap. IV,

are all real, and that would entail a tremendous advance in the study of the distribution of primes. Thus Moebius's function is intimately linked with the most important and as yet unsolved problems of number theory.

Exercises and Problems

1. Prove that

$$\varphi(ab) = \varphi(a)\varphi(b)\frac{c}{\varphi(c)}$$

if c is the product of distinct primes common to a and b .

2. Form a table of solutions of the equation $\varphi(x) = n$ for $n \leq 50$.

3. Develop a method for solving the equation $\varphi(x) = \lambda x$ where λ is a given fraction < 1 . Consider the numerical cases (a) $\lambda = \frac{2}{7}$; (b) $\lambda = \frac{40}{77}$.
Ans. (a) $x = 2^\alpha 3^\beta 7^\gamma$; (b) $x = 3^\alpha 7^\beta 11^\gamma$.

4. By considering the Eulerian function, prove that the number of primes is infinite. *HINT:* If p is the greatest prime, then there is only one number less than and prime to $2 \cdot 3 \cdot 5 \cdots p$.

5. Find the sum of all integers $\leq n$ and prime to n . *Ans.* $\frac{1}{2}n\varphi(n)$.

6. Prove that the number of irreducible fractions ≤ 1 and with denominators not surpassing n is

$$\frac{1}{2} \sum_{d=1}^n \mu(d) \left\{ \left[\frac{n}{d} \right]^2 + \left[\frac{n}{d} \right] \right\}.$$

7. Show that

$$\frac{1}{\varphi(n)} = \frac{1}{n} \sum_{d/n} \frac{\mu^2(d)}{\varphi(d)}$$

where the summation extends over divisors of n .

4. Fundamental Property of $\mu(n)$. Moebius's function, by its very definition, is a factorable numerical function. This simple remark will enable us to establish at once the fundamental property of $\mu(n)$, expressed as follows: The sum

$$F(n) = \sum_{d/n} \mu(n)$$

extended over all divisors of n is 0 if $n > 1$ and 1 if $n = 1$. The second part of the statement is obvious. To prove the first, we observe (Sec. 8, Chap. IV) that $F(n)$ is a factorable function. Hence it remains to prove that

$$F(p^\alpha) = 0$$

if p is a prime. Now

$F(p^\alpha) = \mu(1) + \mu(p) + \mu(p^2) + \cdots + \mu(p^\alpha) = \mu(1) + \mu(p)$, since for $\alpha > 1$ terms $\mu(p^2), \dots, \mu(p^\alpha)$ are all equal to 0. But $\mu(1) = 1$ and $\mu(p) = -1$, and so $F(p^\alpha) = 0$, and consequently $F(n) = 0$ for $n > 1$.

Exercises and Problems

1. Show that for a real $x \geq 1$

$$\sum_{n=1}^x \mu(n) \left[\frac{x}{n} \right] = 1.$$

HINT: Consider the sum

$$\sum \mu(d)$$

extended over all positive integers d, δ satisfying the inequality $d\delta \leq x$.

2. Show that for $x \geq 1$

$$\left| \sum_{n=1}^x \frac{\mu(n)}{n} \right| \leq 1.$$

HINT: Use the preceding problem.

3. Liouville's function $\lambda(n)$ is defined as follows: $\lambda(1) = 1$, $\lambda(n) = +1$ or -1 , according as the number of equal or unequal prime factors of n is even or odd. Show that $\sum_{d/n} \lambda(d) = 0$ if n is not a square and $= 1$ if n is a square.

4. Show that for a real $x \geq 1$

$$\sum_{n=1}^x \lambda(n) \left[\frac{x}{n} \right] = [\sqrt{x}].$$

5. A Property of $\varphi(n)$.—THEOREM. If $1, d, d', d'', \dots$ are all divisors of n , then

$$\varphi(1) + \varphi(d) + \varphi(d') + \dots = n$$

or, with the usual notation, in a more condensed form,

$$\sum_{d|n} \varphi(d) = n.$$

FIRST PROOF. This proof is based on the explicit expression for $\varphi(n)$ and on the fact that $\varphi(n)$ is a factorable function. The function

$$F(n) = \sum_{d|n} \varphi(d)$$

is factorable and for a prime p

$$F(p^\alpha) = \varphi(1) + \varphi(p) + \dots + \varphi(p^\alpha) = 1 + (p-1) + (p-1)p + \dots + (p-1)p^{\alpha-1} = p^\alpha.$$

Consequently, if

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$$

is a factorization of n into a product of powers of primes,

$$F(n) = F(p_1^{\alpha_1}) F(p_2^{\alpha_2}) \dots F(p_s^{\alpha_s}) = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s} = n.$$

SECOND PROOF. In this proof we do not need any information about $\varphi(n)$ except its definition. Numbers $1, 2, 3, \dots, n$ can be distributed into classes referring to the same class numbers which have the same g.c.d. with n . Evidently the number of classes will be exactly equal to the number of divisors of n . Numbers belonging to the class with the same g.c.d. d with n are multiples of d :

$$dk; \quad k = 1, 2, 3, \dots, \frac{n}{d}$$

with k relatively prime to n/d . Hence there are exactly $\varphi(n/d)$ numbers belonging to the class characterized by the divisor d , and in all classes there will be exactly

$$\sum_{d/n} \varphi\left(\frac{n}{d}\right)$$

numbers. But since all numbers $1, 2, \dots, n$ are classified in all classes, we find n numbers; that is,

$$\sum_{d/n} \varphi\left(\frac{n}{d}\right) = n.$$

As d runs through the set of all divisors of n , n/d also will run through the same set; hence

$$\sum_{d/n} \varphi(d) = \sum_{d/n} \varphi\left(\frac{n}{d}\right) = n.$$

On comparing the two proofs we must give preference to the second, for it is based on more general principles and can be used in cases to which the principles of the first proof cannot be adapted.

6. Inversion Formula. The property of $\varphi(n)$ established in the preceding section characterizes this function completely and may be used to find its value for any given n . In fact, taking in succession $n = 1, 2, 3, \dots$ we have the system of equations

$$\begin{aligned} \varphi(1) &= 1, & \varphi(1) + \varphi(2) &= 2, & \varphi(1) + \varphi(3) &= 3, \\ \varphi(1) + \varphi(2) + \varphi(4) &= 4, & \dots & & & \end{aligned}$$

from which $\varphi(2), \varphi(3), \varphi(4), \dots$ can be determined step by step. The values of $\varphi(n)$ resulting from the solution of this system can be written down by means of a general inversion formula which we shall proceed to explain.

Let $f(n)$ and $F(n)$ be two numerical functions such that for $n = 1, 2, 3, \dots$

$$F(n) = \sum_{d/n} f(d); \tag{A}$$

then conversely

$$f(n) = \sum_{d/n} \mu(d) F\left(\frac{n}{d}\right), \quad (B)$$

the summations in both cases referring to divisors of n . To prove this formula it suffices to observe that (A) determines the values $f(1), f(2), f(3), \dots$ through $F(1), F(2), F(3), \dots$ without ambiguity, and to prove that the values $f(1), f(2), f(3), \dots$ as given by (B) actually satisfy (A). Taking d instead of n in (B), we have

$$f(d) = \sum_{d'/n} \mu(d') F\left(\frac{d}{d'}\right),$$

the summation being extended now over all representations of d in the form

$$d = d' d''$$

with positive integer factors d', d'' . On substituting into the sum

$$\sum_{d/n} f(d),$$

we have

$$\sum_{d/n} f(d) = \sum_{d'/n} \mu(d') F(d''),$$

the summation on the right-hand side being extended over all representations of n in the form

$$n = \delta d' d''$$

with positive integer factors δ, d', d'' . When we collect terms with the same d'' , the result is

$$F(d'') \sum \mu(d'),$$

where the summation is extended over all representations of n/d'' in the form

$$\frac{n}{d''} = \delta d',$$

and the result of the summation, by the fundamental property of $\mu(n)$, is 0 unless $n/d'' = 1$, in which case it is $F(n)$. Thus with the value $f(n)$ given by (B), we have

$$\sum_{d/n} f(d) = F(n),$$

and the inversion formula is proved.

Applying this formula to the relation

$$\sum_{d/n} \varphi(d) = n,$$

we have another proof of the formula

$$\varphi(n) = n \sum_{d/n} \frac{\mu(d)}{d}$$

established in Sec. 3.

Exercises and Problems

1. Prove that

$$\sum_{d=1}^n \varphi(d) \left[\frac{n}{d} \right] = \frac{n(n+1)}{2}.$$

HINT: Consider the sum

$$\sum \varphi(d)$$

extended over all solutions of the inequality $d\delta \leq n$ in positive integers d, δ .

2. Let $s_k(n)$ denote the sum of the k th powers of integers not exceeding n and relatively prime to n . Show that

$$\sum_{d/n} \frac{s_k(d)}{d^k} = \frac{1^k + 2^k + \dots + n^k}{n^k}.$$

3. By using the inversion formula determine $s_1(n)$, $s_2(n)$, $s_3(n)$.

Ans. For $n > 1$

$$s_1(n) = \frac{1}{2}n\varphi(n)$$

$$s_2(n) = \frac{1}{6}n^2\varphi(n) + \frac{1}{6}n(1-p_1)(1-p_2)\cdots(1-p_s)$$

$$s_3(n) = \frac{1}{24}n^3\varphi(n) + \frac{1}{24}n^2(1-p_1)(1-p_2)\cdots(1-p_s)$$

if

$$n = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s}.$$

4. If

$$F(n) = \sum_{d/n} f(d),$$

then $f(n)$ is a factorable function if $F(n)$ is factorable.

5. If

$$F(n) = \prod_{d/n} f(d)$$

where the product is extended over divisors of n and $f(n) = 0$ for no value of n , then conversely

$$f(n) = \prod_{d/n} F\left(\frac{n}{d}\right)$$

6. Show that the product $\omega(n)$ of integers $\leq n$ and prime to n is given by

$$\omega(n) = n^{\varphi(n)} \prod_{d/n} \left(\frac{d!}{d^d}\right)^{\mu(n/d)}$$

7. **Another Application of the Combinatorial Formula.** As a second application of the general formula in Sec. 1, let us derive an expression for the number of odd integers not divisible by the given odd primes p_1, p_2, \dots, p_m and not exceeding a given limit x . First of all we must find how many odd integers below this limit are divisible by a given number P . There are evidently as many such integers as there are integers k for which

$$(2k-1)P \leq x$$

or

$$k \leq \frac{x}{2P} + \frac{1}{2}.$$

The number of integers k satisfying this condition is

$$\left[\frac{x}{2P} + \frac{1}{2} \right],$$

which is at the same time the nearest integer to $x/2P$ taking, in case there are two nearest integers, the greater of them. To denote this nearest integer we shall use the symbol

$$\left\{ \frac{x}{2P} \right\}.$$

After these preliminary remarks the rest of our reasoning is quite similar to the reasoning in Sec. 2, and the result can be presented thus: Let a and b represent, respectively, divisors including 1 of $p_1 p_2 \dots p_m$ containing an even and an odd number of primes; then the number of odd integers not exceeding x and not divisible by any of the primes p_1, p_2, \dots, p_m is expressed as follows:

$$\sum_a \left\{ \frac{x}{2a} \right\} - \sum_b \left\{ \frac{x}{2b} \right\}.$$

If p_1, p_2, \dots, p_m are the first m odd primes, we shall use the symbol $\phi(x, m)$ to indicate the number of odd integers $\leq x$ not divisible by the first m odd primes. Then

$$\phi(x, m) = \sum_a \left\{ \frac{x}{2a} \right\} - \sum_b \left\{ \frac{x}{2b} \right\}.$$

In particular if $m = \pi(\sqrt{x}) - 1$; that is, if p_1, p_2, \dots, p_m are all odd primes not exceeding \sqrt{x} , then all odd integers not divisible by them are primes $> \sqrt{x}$ and $\leq x$ and 1; in other words, in this case

$$\phi(x, m) = \pi(x) - m = \pi(x) - \pi(\sqrt{x}) + 1,$$

and on comparison with the preceding expression for the same number we have the formula

$$\pi(x) = \pi(\sqrt{x}) + \sum_a \left\{ \frac{x}{2a} \right\} - \sum_b \left\{ \frac{x}{2b} \right\} - 1,$$

which may be used to compute the number of primes not exceeding x when all the primes not exceeding \sqrt{x} are known.

The use of this formula is facilitated by auxiliary tables of numbers a and b . We give here such a table corresponding to $m = 5$.

a				b			
1	15	21	33	3	5	7	11
35	39	55	65	13	105	165	195
77	91	143	1,155	231	273	385	429
1,365	2,145	3,003	5,005	455	715	1,001	15,015

Example 1. To find the number of primes not exceeding 100. Picking from the preceding tables numbers divisible only by 3, 5, 7, we have

$$\left\{ \frac{50}{a} \right\} = 50, 3, 2, 1; \quad \left\{ \frac{50}{b} \right\} = 17, 10, 7$$

$$50 + 3 + 2 + 1 = 56; \quad 17 + 10 + 7 = 34.$$

Consequently

$$\pi(100) = 3 + 56 - 34 = 25.$$

Example 2. To find the number of primes not exceeding 300. The greatest prime less than $\sqrt{300}$ is 17; hence there are six primes, 3, 5, 7, 11, 13, 17, below this limit. Our tables correspond to $m = 5$. To avoid the necessity of making larger tables, we may use the almost evident formula

$$\phi(x, m) = \phi(x, m-1) - \phi\left(\frac{x}{p_m}, m-1\right).$$

In fact, to have all odd integers $\leq x$ nondivisible by the m first odd primes, we have to remove from the odd integers $\leq x$ nondivisible by the $m-1$ first primes those which are divisible by p_m , and the latter occur in number

$$\phi\left(\frac{x}{p_m}, m-1\right) = \phi\left(\left[\frac{x}{p_m}\right], m-1\right).$$

In our case we have

$$\phi(300, 6) = \phi(300, 5) - \phi(17, 5).$$

To compute the first term we may use our tables and find

$$\left\{\frac{150}{a}\right\} = 150, 10, 7, 5, 4, 4, 3, 2, 2, 2, 1; \quad \text{sum } 190$$

$$\left\{\frac{150}{b}\right\} = 50, 30, 21, 14, 12, 1, 1, 1, 1, 1; \quad \text{sum } 132.$$

Thus

$$\phi(300, 5) = 190 - 132 = 58,$$

and, on the other hand,

$$\phi(17, 5) = 2,$$

so that

$$\phi(300, 6) = 56.$$

Finally

$$\pi(300) = 56 + 6 = 62.$$

Since the number of primes less than 100 is 25, there are $62 - 25 = 37$ primes between 100 and 300. And indeed, by direct count, 21 primes are found between 100 and 200 and 16 primes between 200 and 300.

8. Meissel's Formula. The labor involved in computing the number of primes below a given limit becomes quite prohibitive when this limit is large, on account of the great many values of a and b to be used. Nevertheless, by another very ingenious arrangement of calculation, Meissel succeeded in overcoming these difficulties to a certain extent.

Let p_ν be the largest prime not exceeding $\sqrt[3]{x}$, so that

$$\nu + 1 = \pi(\sqrt[3]{x}).$$

Then $p_{\nu+1} > \sqrt[3]{x}$ and

$$\frac{x}{p_{\nu+1}} < \sqrt[3]{x^2}, \quad \sqrt{\frac{x}{p_{\nu+1}}} < \sqrt[3]{x}.$$

Since $\pi(x)$ is a nondecreasing function,

$$\pi\left(\sqrt{\frac{x}{p_{\nu+1}}}\right) \leq \pi(\sqrt[3]{x}) = \nu + 1.$$

Now

$$\pi\left(\sqrt{\frac{x}{p_{\nu+s}}}\right)$$

can only decrease with an increasing s , and therefore, for $s \geq 1$ we shall have

$$\pi\left(\sqrt{\frac{x}{p_{\nu+s}}}\right) \leq \nu + s. \quad (A)$$

When we set $m = \nu + \mu$, the largest prime not exceeding \sqrt{x} will be $p_{\nu+\mu}$. For $s \leq \mu$ a fortiori

$$p_{\nu+s} \leq \sqrt{x}, \quad \frac{x}{p_{\nu+s}} \geq \sqrt{x}$$

and

$$\pi\left(\frac{x}{p_{\nu+s}}\right) \geq \mu + \nu + 1 > \mu + \nu,$$

whence

$$\pi\left(\frac{x}{p_{\nu+s}}\right) > \nu + s. \quad (B)$$

The inequalities (A) and (B) hold for $s = 1, 2, \dots, \mu$.

Consider now the meaning of the symbol $\phi(n, a)$ where

$$\pi(\sqrt{n}) \leq a + 1 \leq \pi(n).$$

By virtue of these inequalities the last prime of the sequence $p_1 = 3, p_2 = 5, \dots, p_{a+1}$ is $\geq \sqrt{n}$ and $p_a \leq n$. Consequently $\phi(n, a)$ represents the number of primes which are greater than p_a and do not exceed n , augmented by 1; that is,

$$\phi(n, a) = \pi(n) - a.$$

By virtue of the inequalities (A) and (B), these conditions will be satisfied if we take

$$n = \frac{x}{p_{\nu+s}} \quad \text{and} \quad a = \nu + s - 1.$$

Then

$$\phi\left(\frac{x}{p_{\nu+s}}, \nu + s - 1\right) = \pi\left(\frac{x}{p_{\nu+s}}\right) - (\nu + s - 1)$$

and, since

$$\phi(x, \nu + s) = \phi(x, \nu + s - 1) - \phi\left(\frac{x}{p_{\nu+s}}, \nu + s - 1\right)$$

we shall have

$$\phi(x, \nu + s) = \phi(x, \nu + s - 1) + \nu + s - 1 - \pi\left(\frac{x}{p_{\nu+s}}\right)$$

for $s = 1, 2, \dots, \mu$. Now we sum up these equations and, after due cancellations, get

$$\phi(x, m) = \phi(x, \nu) + \mu\nu + \frac{\mu(\mu - 1)}{2} - \sum_{s=1}^{\mu} \pi\left(\frac{x}{p_{\nu+s}}\right).$$

But

$$\phi(x, m) = \pi(x) - \pi(\sqrt{x}) + 1,$$

whence we obtain finally the formula due to Meissel:

$$\pi(x) = \phi(x, \nu) + \mu\nu + \frac{(\mu - 2)(\mu + 1)}{2} + \pi(\sqrt{x}) - \sum_{s=1}^{\mu} \pi\left(\frac{x}{p_{\nu+s}}\right).$$

By means of this formula, but after laborious calculation, Meissel found that below 100,000,000 there are 5,761,460 primes.

Example. Let us find the number of primes not exceeding 8,000. First we find

$$\sqrt[3]{8,000} = 20 \quad \sqrt{8,000} = 89.443$$

$$\pi(20) = 8 \quad \pi(89) = 24$$

whence

$$\nu = 7, \quad \mu = 16.$$

Thus we have to compute $\phi(8,000, 7)$, and this is the most laborious part of the calculation. In order to be able to use the auxiliary table, we resort to the following relations

$$\begin{aligned} \phi(8,000, 7) &= \phi(8,000, 6) - \phi(421, 6) \\ \phi(8,000, 6) &= \phi(8,000, 5) - \phi(470, 5) \\ \phi(421, 6) &= \phi(421, 5) - \phi(24, 5) = \phi(421, 5) - 4. \end{aligned}$$

We have

$$\left\{ \frac{210.5}{a} \right\} = 211, 14, 10, 6, 6, 5, 4, 3, 3, 2, 1; \quad \text{sum } 265.$$

$$\left\{ \frac{210.5}{b} \right\} = 70, 42, 30, 19, 16, 2, 1, 1, 1, 1, 1; \quad \text{sum } 184.$$

$$\begin{aligned} \phi(421, 5) &= 81; \quad \phi(421, 6) = 77 \\ \phi(8,000, 7) &= \phi(8,000, 6) - 77. \end{aligned}$$

Again

$$\left\{ \frac{235}{a} \right\} = 235, 16, 11, 7, 7, 6, 4, 4, 3, 3, 2; \quad \text{sum } 298$$

$$\left\{ \frac{235}{b} \right\} = 78, 47, 34, 21, 18, 2, 1, 1, 1, 1, 1, 1; \quad \text{sum } 207$$

$$\begin{aligned} \phi(470, 5) &= 91 \\ \phi(8,000, 6) &= \phi(8,000, 5) - 91. \end{aligned}$$

Finally

$$\phi(8,000, 7) = \phi(8,000, 5) - 168.$$

To have $\phi(8,000, 5)$ we use the following numbers:

$$\left\{ \frac{4,000}{a} \right\} = 4,000, 267, 190, 121, 114, 103, 73, 62, 52, 44, 28, 3, 3, 2, 1, 1;$$

sum 5,064

$$\left\{ \frac{4,000}{b} \right\} = 1,333, 800, 571, 364, 308, 38, 24, 21, 17, 15, 10, 9, 6, 4;$$

sum 3,529

$$\phi(8,000, 5) = 5,064 - 3,529 = 1,535$$

$$\phi(8,000, 7) = 1,535 - 168 = 1,367.$$

Again

$$\mu\nu + \frac{(\mu - 2)(\mu + 1)}{2} = 231$$

$$\frac{\pi(89) = 24}{\text{sum} = 255}$$

and so

$$\phi(8,000, 7) + 255 = 1,622.$$

It remains now to subtract from this number the sum

$$S = \sum_{p_i}^{23} \pi\left(\frac{8,000}{p_i}\right),$$

www.dbrlibrary.org.in

the terms of which are found by direct count in a small table of primes:

$\pi(347) = 69$	$\pi(135) = 32$
$\pi(275) = 58$	$\pi(131) = 32$
$\pi(258) = 55$	$\pi(119) = 30$
$\pi(216) = 47$	$\pi(112) = 29$
$\pi(195) = 44$	$\pi(109) = 29$
$\pi(186) = 42$	$\pi(101) = 26$
$\pi(170) = 39$	$\pi(96) = 24$
$\pi(150) = 35$	$\pi(89) = 24.$

Adding these numbers, we have $S = 615$ and

$$\pi(8,000) = 1,622 - 615 = 1,007.$$

Thus there are 1,007 primes less than 8,000.

Exercises and Problems

1. By using Meissel's formula compute the number of primes in each of the first ten thousands.

Ans. 168, 135, 127, 120, 119, 114, 117, 107, 110, 112.

2. Denoting by $f(x, n)$ the number of integers not exceeding x and relatively prime to a given number n , show that

$$\sum_{d/n} f\left(\frac{x}{d}, \frac{n}{d}\right) = [x]$$

where the summation extends over the divisors of n .

3. By an appropriate application of the inversion formula to the result of the preceding problem, show that

$$f(x, n) = \sum_{d/n} \mu(d) \left[\frac{x}{d} \right]$$

4. Let $2, 3, 5, \dots, p$ be all the primes not exceeding $\sqrt{2n}$. Show that the number of primes $> n$ and not exceeding $2n$ is expressed by

$$\sum_a \left\{ \frac{n}{a} \right\} - \sum_b \left\{ \frac{n}{b} \right\}$$

where the a 's are divisors (including 1) of $2n$ containing an even number of prime factors, and the b 's are divisors containing an odd number of prime factors. Compute by this formula the number of primes between 100 and 200 . Ans. 21.

Downloaded from www.digitallibrary.org in

CHAPTER VI

ON THE CONGRUENCE OF NUMBERS

1. Definition and Simple Properties of Congruences. In number theory we are often concerned with properties which are true for a whole class of integers differing from each other by multiples of a certain integer. Take, for instance, the fact that the square of an odd integer when divided by 8 leaves 1 for a remainder. Here we have a property holding for all odd numbers; that is, for a class of numbers differing from each other by multiples of 2. As another example, we see that when the last digit of a number, in decimal notation, is 6, then the last digit of its square will also be 6. Thus, in this simple example, we deal again with a property shared by integers differing by a multiple of an integer; namely, 10.

The consideration of properties holding for all integers differing from each other by a multiple of a certain integer leads in a natural way to the notion of *congruence*. Two integers a and b whose difference $a - b$ is divisible by a given number m (not 0) are said to be *congruent for the modulus m* or simply *congruent modulo m* . Gauss, who introduced the notion of congruence, proposed the notation

$$a \equiv b \pmod{m}$$

to designate the congruence of a and b modulo m . Thus, for example,

$$17 \equiv 5 \pmod{12}, \quad 7^2 \equiv -1 \pmod{5}.$$

Carl Friedrich Gauss (1777–1855), whom his contemporaries used to call “*Princeps Mathematicorum*” (Prince of Mathematicians), was

perhaps the greatest mathematical genius of all time, only Archimedes and Newton being comparable to him. One has only to read his scientific diary, now published in Vol. X of his "Collected Works," to be profoundly impressed by the rapid succession of great discoveries made by Gauss, especially in the period from 1796 to 1800. Not having had access to the literature of mathematics in his youth, Gauss in a short time rediscovered by himself all that had been done in the theory of numbers by his predecessors and far surpassed them by his own incomparable contributions. His great work "Disquisitiones arithmeticae," published in 1801, remarkable equally for its profundity and perfect form of exposition, will forever remain as the great classic of number theory. Though Gauss contributed to almost all branches of mathematics, number theory, or "higher arithmetic," as he called it, was his favorite science. To him is attributed the phrase: "Mathematics is the Queen of Sciences, but Arithmetic is the Queen of Mathematics."

As an immediate consequence of the definition of congruence, we have that congruent numbers when divided by the modulus leave the same remainders and, conversely, numbers with the same remainders are congruent numbers. In congruence notation the divisibility of a by m is expressed by the congruence

$$a \equiv 0 \pmod{m}.$$

Accordingly

$$a \equiv b \pmod{m}$$

means the same as

$$a - b \equiv 0 \pmod{m}.$$

The above-mentioned property of odd integers in congruence notation can be stated thus:

$$a^2 \equiv 1 \pmod{8}$$

if

$$a \equiv 1 \pmod{2}.$$

The congruence notation, like other notations, serves to simplify to a very considerable extent the exposition. But more than that: it naturally suggests new problems in number

theory which otherwise hardly ever could have been stated. On this account in number theory it is just as important and useful as the differential notation in the infinitesimal analysis. The very sign used to designate the congruence resembles the sign of equality, and it was chosen with good reason. For congruences with the same moduli possess many formal properties of equalities.

We shall enumerate now some of the simplest properties of congruences.

1. If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$. This property of "transitivity" is almost evident. For $a \equiv b \pmod{m}$ means that $a - b$ is divisible by m ; also $b \equiv c \pmod{m}$ means that $b - c$ is divisible by m . But then

$$a - c = (a - b) + (b - c)$$

is divisible by m ; that is, $a \equiv c \pmod{m}$.

2. Two congruences with the same moduli can be added or subtracted, member by member, like equalities. In other words, from two congruences

$$A \equiv a \pmod{m}, \quad B \equiv b \pmod{m}$$

it follows that

$$A \pm B \equiv a \pm b \pmod{m}.$$

In fact

$$(A \pm B) - (a \pm b) = (A - a) \pm (B - b),$$

but on the right-hand side both $A - a$ and $B - b$ are divisible by m ; consequently the left-hand side is also divisible by m . By repeated application of this property we derive the following general proposition: If

$$A \equiv a, \quad B \equiv b, \quad C \equiv c, \quad \dots \pmod{m},$$

then

$$A + B + C + \dots \equiv a + b + c + \dots \pmod{m}.$$

3. Two congruences with the same moduli can be multiplied, member by member, like equalities. In other words, from

$$A \equiv a \pmod{m}, \quad B \equiv b \pmod{m}$$

it follows that

$$AB \equiv ab \pmod{m}.$$

The difference $AB - ab$ can be written thus:

$$AB - ab = (A - a)B + a(B - b),$$

and, since $A - a$ and $B - b$ are divisible by m , it is clear that $AB - ab$ is divisible by m also. By repeated application of this property, we derive the following general proposition:

If

$$A \equiv a, \quad B \equiv b, \quad C \equiv c, \dots \pmod{m},$$

then

$$ABC \dots \equiv abc \dots \pmod{m}.$$

In particular, if

$$A \equiv a \pmod{m},$$

then

$$A^n \equiv a^n \pmod{m}$$

for any positive integer exponent.

Let

$$f(x) = p_0x^n + p_1x^{n-1} + \dots + p_n$$

be a polynomial with integer coefficients involving an *indeterminate* x ; that is, a letter without any numerical meaning with which we operate by the ordinary rules of algebra as if it were a number. As usual we shall denote by $f(a)$ the result of substitution of a *number* a instead of x in this polynomial. Then we can state the following simple but important proposition:

From the congruence

$$A \equiv a \pmod{m}$$

it follows that

$$f(A) \equiv f(a) \pmod{m}.$$

In fact

$$A^n \equiv a^n, \quad A^{n-1} \equiv a^{n-1}, \quad \dots, \quad A \equiv a \pmod{m},$$

and

$$\begin{aligned} p_0 A^n &\equiv p_0 a^n, & p_1 A^{n-1} &\equiv p_1 a^{n-1} & \dots \\ p_{n-1} A &\equiv p_{n-1} a, & p_n &\equiv p_n \pmod{m}, \end{aligned}$$

whence, by adding these congruences member by member, we have

$$p_0 A^n + p_1 A^{n-1} + \dots + p_n \equiv p_0 a^n + p_1 a^{n-1} + \dots + p_n \pmod{m};$$

that is,

$$f(A) \equiv f(a) \pmod{m}.$$

Before going farther it is well to show the use of the properties of congruences hitherto established in a few simple examples.

Example 1. Fermat stated, though confessing he did not possess a valid proof, that all numbers of the form

$$2^{2^n} + 1$$

are primes. This statement was refuted by Euler, who showed that the number

$$2^{32} + 1$$

is divisible by 641. Without writing it down the divisibility of this large number by 641 can be established with the help of congruences without much labor. In fact, we have

$$\begin{aligned} 2^2 &\equiv 4, & 2^4 &\equiv 16, & 2^8 &\equiv 256, & 2^{16} &\equiv 256^2 \equiv 154, \\ & & & & & & 2^{32} &\equiv 154^2 \equiv 640 \pmod{641}; \end{aligned}$$

that is,

$$2^{32} \equiv -1 \pmod{641}, \quad 2^{32} + 1 \equiv 0 \pmod{641}.$$

Example 2. Let us find the remainder obtained by dividing

by 101. In all cases when the exponent is large the operation will be greatly shortened by resorting to the fact that every integer is a sum of powers of 2. Thus in our case

$$100 = 64 + 32 + 4$$

and

$$3^{100} = 3^{64} \cdot 3^{32} \cdot 3^4.$$

Now

$$3^4 \equiv 81 \equiv -20, \quad 3^8 \equiv 20^2 \equiv -4, \quad 3^{16} \equiv 16, \quad 3^{32} \equiv -47, \\ 3^{64} \equiv 47^2 \equiv -13 \pmod{101},$$

and again

$$3^4 \cdot 3^{32} \equiv 20 \cdot 47 \equiv 31; \quad 3^4 \cdot 3^{32} \cdot 3^{64} \equiv -13 \cdot 31 \equiv 1 \pmod{101},$$

which shows that

$$3^{100} \equiv 1 \pmod{101},$$

and so 1 is the requested remainder.

Example 3. Familiar criteria of divisibility by 3, 9, 11 follow immediately from the properties of congruences. Let a number N be represented in the decimal notation thus:

$$N = a + 10b + 10^2c + 10^3d + \dots$$

Noticing that

$$10 \equiv 1, \quad 10^2 \equiv 1, \quad 10^3 \equiv 1, \quad \dots \pmod{9},$$

we have

$$N \equiv a + b + c + d + \dots \pmod{9}.$$

Hence a number is divisible by 9 if and only if the sum of its digits is divisible by 9. Since the congruence holding for a certain modulus evidently holds for any divisor of this modulus, we have also

$$N \equiv a + b + c + d + \dots \pmod{3},$$

which shows that a number is divisible by 3 if and only if the sum of its digits is divisible by 3.

With respect to the modulus 11, we have

$$10 \equiv -1, \quad 10^2 \equiv 1, \quad 10^3 \equiv -1, \quad \dots \pmod{11},$$

and so

$$N \equiv a - b + c - d + \dots \pmod{11}.$$

The number N , consequently, is divisible by 11 if and only if the alternate sum

$$a - b + c - d + \dots$$

of its digits is divisible by 11.

Since congruent numbers leave the same remainders when divided by the modulus, the preceding congruences can be used in finding remainders in divisions by 3, 9, 11.

Exercises

1. Find the remainders obtained in dividing

$$2^{46}, 7^{126}, 8^{130},$$

respectively, by the primes 47, 127, 131.

2. Show that the congruences

$$a \equiv \pm 1 \quad \text{and} \quad a \equiv \pm 3 \pmod{8}$$

imply, respectively,

$$a^2 \equiv 1 \quad \text{and} \quad a^2 \equiv 9 \pmod{16}.$$

3. Derive a criterion of divisibility by 7.
4. Show that all odd numbers satisfy the congruences

$$a^4 \equiv 1 \pmod{16}, \quad a^8 \equiv 1 \pmod{32}, \quad a^{16} \equiv 1 \pmod{64}$$

and in general

$$a^{2^n} \equiv 1 \pmod{2^{n+2}}.$$

2. **Elementary Properties of Congruences Continued.** From an equality

$$na = nb$$

by canceling n on both sides we get a true equality

$$a = b$$

provided n is not 0. Not so with congruences: from a congruence

$$na \equiv nb \pmod{m}$$

in general we cannot conclude

$$a \equiv b \pmod{m}$$

even if n is not divisible by m . The first congruence means that $na - nb = n(a - b)$ is divisible by m . Let d be the g.c.d. of n and m ; then

$$\frac{n}{d}(a - b)$$

is divisible by m/d and, since n/d and m/d are relatively prime, $a - b$ must be divisible by m/d . Thus from the congruence

$$na \equiv nb \pmod{m}$$

it follows only that

$$a \equiv b \pmod{\frac{m}{d}}.$$

In case, however, $d = 1$; that is, n and m are relatively prime, we have

$$a \equiv b \pmod{m}.$$

Thus the rule of cancellation holds for congruences on the condition that the canceled factor is relatively prime to the modulus.

Several congruences

$$M \equiv N \pmod{a}, M \equiv N \pmod{b}, \dots, M \equiv N \pmod{l}$$

amount to a single congruence

$$M \equiv N \pmod{\mu}$$

for the modulus which is the least common multiple μ of the moduli a, b, \dots, l . In fact, the given congruences show that $M - N$ is a common multiple of a, b, \dots, l and as such is divisible by μ or

$$M \equiv N \pmod{\mu}.$$

Conversely, M and N will be congruent for moduli dividing μ , in particular for moduli a, b, \dots, l . When a, b, \dots, l are relatively prime in pairs, $\mu = ab \cdots l$. Consequently, in this case, the system of congruences

$$M \equiv N \pmod{a}, \quad M \equiv N \pmod{b}, \quad \dots, \\ M \equiv N \pmod{l}$$

implies

$$M \equiv N \pmod{ab \cdots l},$$

and vice versa.

3. Distribution of Numbers in Classes Modulo m . In dealing with congruences we may confine ourselves to positive moduli, since a congruence holding for the modulus m holds also for the modulus $-m$. Of two numbers congruent for the modulus m , each is called a "residue" of the other modulo m .

Every integer is congruent modulo m to one and only one of the numbers

$$0, 1, 2, \dots, m-1. \quad (A)$$

When an integer x is divided by m , the remainder will be congruent to a and will be contained in the system (A). Thus the first part of the statement is proved. The second follows from the fact that no two distinct numbers of (A) are congruent modulo m , since their difference is numerically less than m and, being different from 0, cannot be divisible by m . The distribution of integers into classes modulo m is based on this simple remark. That is, if we put together in one class all integers congruent modulo m , integers will be distributed into m classes: one class will comprise integers congruent to 0; the second class, integers congruent to 1, and so on; and finally, the m th class will comprise integers congruent to $m-1$ modulo m . If, from each of the m classes into which all numbers are distributed modulo m , we pick up one number, the m numbers thus selected:

$$r_1, r_2, \dots, r_m$$

are representatives of these classes and constitute a so-called "complete system of residues modulo m ." Thus numbers of

the system (A) represent one particular complete system of residues—the system of *least positive* residues. By its very definition every complete system of residues comprises m incongruent modulo m numbers, and, vice versa, every system of m incongruent numbers is a complete system of residues modulo m . For m incongruent numbers necessarily are representatives of m classes modulo m .

4. Various Useful Complete Systems of Residues. If r_1, r_2, \dots, r_m represent some complete system of residues modulo m and n is an arbitrary integer, then the numbers

$$r_1 + n, r_2 + n, \dots, r_m + n,$$

being incongruent modulo m , constitute another complete system of residues. For instance, the numbers

$$n, n + 1, n + 2, \dots, n + m - 1,$$

form a complete system of residues. In particular, if we take $n = -(m - 1)/2$ and $n = -m/2 + 1$, respectively, for an odd and even m , two systems of numbers

$$\begin{aligned} &-\frac{m-1}{2}, -\frac{m-3}{2}, \dots, -1, 0, 1, \dots, \frac{m-3}{2}, \frac{m-1}{2} \\ &-\frac{m}{2} + 1, -\frac{m}{2} + 2, \dots, -1, 0, 1, \dots, \frac{m}{2} - 1, \frac{m}{2} \end{aligned}$$

represent complete systems of *absolutely least* residues for an odd and even modulus, respectively.

Let a be any integer relatively prime to m and r_1, r_2, \dots, r_m , some complete system of residues; then the numbers

$$ar_1, ar_2, \dots, ar_m$$

form another complete system of residues. It suffices to prove that no two distinct numbers of this system are congruent, and this is almost evident, since the congruence

$$ar_i \equiv ar_j \pmod{m}$$

implies

$$r_i \equiv r_j \pmod{m},$$

which is impossible. In particular

$$0, a, 2a, \dots, (m-1)a$$

with a relatively prime to m represent a complete system of residues modulo m .

Exercises and Problems

1. Show that the numbers

$$1, 3, 3^2, \dots, 3^{16} \text{ and } 0$$

form a complete system of residues modulo 17. Do the numbers

$$1, 2, 2^2, \dots, 2^{10} \text{ and } 0$$

constitute a complete system of residues modulo the same modulus?

2. If a is relatively prime to m , and b is an arbitrary integer, show that the remainders obtained by dividing the numbers

$$ax + b \quad \text{for} \quad x = 0, 1, 2, \dots, m-1$$

by m coincide with $0, 1, 2, \dots, m-1$, save for order. Hence prove that

$$\sum_{x=0}^{m-1} \left[\frac{ax + b}{m} \right] = \frac{(a-1)(m-1)}{2} + b.$$

3. If a is not relatively prime to m , but $(a, m) = d > 1$, and r is the remainder in the division of b by d , then the numbers

$$ax + b \quad \text{for} \quad x = 0, 1, 2, \dots, m-1$$

when divided by m leave the remainders

$$dx + r, \quad x = 0, 1, 2, \dots, \frac{m}{d} - 1,$$

each repeated exactly d times. Hence deduce

$$\sum_{x=0}^{m-1} \left[\frac{ax + b}{m} \right] = \frac{(a-1)(m-1)}{2} + \frac{d-1}{2} + b - r.$$

5. Generation of Complete System Modulo ab When $(a, b) = 1$. A complete system of residues modulo ab , where a and b are relatively prime numbers, can be generated by means of the complete systems of residues

$$r_1, r_2, \dots, r_a \quad (A)$$

$$s_1, s_2, \dots, s_b \quad (B)$$

for the moduli a and b , respectively, in the following two ways.

First, consider numbers of the form

$$ax + y,$$

where x and y run independently through the numbers (B) and (A), respectively. In this manner we have altogether ab numbers

$$as_i + r_j; \quad i = 1, 2, \dots, b; \quad j = 1, 2, \dots, a \quad (C)$$

which constitute a complete system of residues mod ab if we can prove that they are all *different mod ab* ; that is, that no two of them are congruent for this modulus. Now for relatively prime a and b the congruence

$$as_i + r_j \equiv as_k + r_l \pmod{ab}$$

is entirely equivalent to congruences (Sec. 2)

$$as_i + r_j \equiv as_k + r_l \pmod{a}$$

$$as_i + r_j \equiv as_k + r_l \pmod{b}.$$

The first implies

$$r_j \equiv r_l \pmod{a},$$

which is possible only if $r_j = r_l$, $l = j$. Then the second congruence, after canceling a on both sides (Sec. 2), becomes

$$s_i \equiv s_k \pmod{b},$$

which is possible only if $s_i = s_k$, $k = i$. Thus two numbers of the system (C) corresponding to two different combinations

of subscripts i, j are different modulo ab and, therefore, (C) represents a complete system of residues for this modulus.

Secondly, consider numbers of the form

$$ax + by,$$

where x and y run independently through numbers (B) and (A). The system of ab numbers

$$as_i + br_j; \quad i = 1, 2, \dots, b; \quad j = 1, 2, \dots, a \quad (D)$$

is a complete system of residues mod ab . For the numbers

$$br_1, br_2, \dots, br_a$$

by the concluding remarks of Sec. 3, form a complete system of residues mod a and can be taken instead of

www.dlib.informatics.org.in

The truth of the statement follows then from what has been already established.

6. Generation of Complete System of Residues Mod a^n .

Let

$$r_1, r_2, \dots, r_a$$

$$s_1, s_2, \dots, s_c$$

be complete systems of residues for the moduli a and $a^{n-1} = c$, respectively. Then $ca = a^n$ numbers

$$a^{n-1}r_i + s_j; \quad i = 1, 2, \dots, a; \quad j = 1, 2, \dots, c \quad (E)$$

constitute a complete system of residues mod a^n . It suffices to prove that these numbers are different modulo a^n . The congruence

$$a^{n-1}r_i + s_j \equiv a^{n-1}r_k + s_l \pmod{a^n}$$

implies

$$a^{n-1}r_i + s_j \equiv a^{n-1}r_k + s_l \pmod{a^{n-1}}$$

or

$$s_j \equiv s_l \pmod{a^{n-1}},$$

which requires $s_j = s_l, j = l$. But then

$$a^{n-1}r_i \equiv a^{n-1}r_k \pmod{a^n},$$

whence

$$r_i \equiv r_k \pmod{a}$$

and $r_i = r_k, i = k$. Thus the statement is proved.

7. An Application. In a subsequent chapter we shall deal with arithmetical properties of so-called Bernoullian numbers, and to this end we must investigate some properties of sums

$$S_n(a) = 0^n + 1^n + 2^n + \dots + (a-1)^n$$

of powers of consecutive integers—properties which afford a good illustration of principles laid down in the preceding sections of this chapter. Since the numbers $0, 1, 2, \dots, a-1$ constitute a complete system of residues modulo a and enter into $S_n(a)$ symmetrically, we shall have

$$S_n(a) \equiv r_1^n + r_2^n + \dots + r_a^n \pmod{a}$$

for any complete system of residues

$$r_1, r_2, \dots, r_a$$

modulo a . Let us combine this remark with the fact that the numbers

$$as_i + r_j$$

form a complete system of residues mod ab if a and b are relatively prime and

$$s_1, s_2, \dots, s_b$$

$$r_1, r_2, \dots, r_a$$

represent complete systems of residues for the moduli b and a , respectively. On account of this we have

$$S_n(ab) \equiv \sum_{i,j} (as_i + r_j)^n \pmod{ab}$$

and a fortiori

$$S_n(ab) \equiv \sum_{i,j} r_{ij}^n \equiv bS_n(a) \equiv bS_n(a) + aS_n(b) \pmod{a}.$$

In the same way we find the congruence

$$S_n(ab) \equiv bS_n(a) + aS_n(b) \pmod{b},$$

and, since both congruences hold for relatively prime moduli a, b , we conclude that

$$S_n(ab) \equiv bS_n(a) + aS_n(b) \pmod{ab}.$$

In other words

$$S_n(ab) = bS_n(a) + aS_n(b) + Kab,$$

where K is an integer. This equality shows that

$$\frac{S_n(ab)}{ab} - \frac{S_n(a)}{a} - \frac{S_n(b)}{b} = K,$$

for relatively prime a, b , is an integer.

If three integers a, b, c are relatively prime in pairs, then by the same property

$$\frac{S_n(abc)}{abc} - \frac{S_n(ab)}{ab} - \frac{S_n(c)}{c}$$

is an integer, and consequently

$$\frac{S_n(abc)}{abc} - \frac{S_n(a)}{a} - \frac{S_n(b)}{b} - \frac{S_n(c)}{c}$$

is an integer, also. Proceeding in the same way, we conclude that in general

$$\frac{S_n(abc \cdots l)}{abc \cdots l} - \frac{S_n(a)}{a} - \frac{S_n(b)}{b} - \cdots - \frac{S_n(l)}{l}$$

is an integer if a, b, c, \dots, l are integers relatively prime in pairs.

Let

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$$

be a prime factorization of m . Then $a = p_1^{\alpha_1}$, $b = p_2^{\alpha_2}$, . . . , $l = p_s^{\alpha_s}$ are numbers relatively prime in pairs; consequently

$$\frac{S_n(m)}{m} = \frac{S_n(p_1^{\alpha_1})}{p_1^{\alpha_1}} \frac{S_n(p_2^{\alpha_2})}{p_2^{\alpha_2}} \cdots \frac{S_n(p_s^{\alpha_s})}{p_s^{\alpha_s}}$$

is always an integer. This theorem can be simplified still more by considering $S_n(p^\alpha)$ where p is a prime. By the result established in Sec. 6,

$$S_n(p^\alpha) \equiv \sum_{i,j} (s_j + p^{\alpha-1} r_i)^n \pmod{p^\alpha},$$

where r_i runs through the numbers $0, 1, 2, \dots, p-1$ and s_j through $0, 1, 2, \dots, p^{\alpha-1}-1$; the respective complete system of residues for p and $p^{\alpha-1}$. By the binomial theorem

$$(s_j + p^{\alpha-1} r_i)^n = s_j^n + \frac{n}{1} s_j^{n-1} r_i p^{\alpha-1} + \frac{n(n-1)}{1 \cdot 2} s_j^{n-2} r_i^2 p^{2\alpha-2} + \cdots,$$

and in the case $\alpha > 1$, all the terms beginning with the third are divisible by p^α . Hence

$$(s_j + p^{\alpha-1} r_i)^n \equiv s_j^n + n s_j^{n-1} r_i p^{\alpha-1} \pmod{p^\alpha}.$$

Taking the sum for fixed j and running i , we have

$$\sum_i (s_j + p^{\alpha-1} r_i)^n \equiv p s_j^n + n s_j^{n-1} \frac{p(p-1)}{2} p^{\alpha-1} \pmod{p^\alpha}.$$

If p is an odd prime, the second term on the right-hand side is divisible by p^α , and so

$$\sum_i (s_j + p^{\alpha-1} r_i)^n \equiv p s_j^n \pmod{p^\alpha}.$$

Summing these congruences for the variable j , we get finally

$$S_n(p^\alpha) \equiv pS_n(p^{\alpha-1}) \pmod{p^\alpha},$$

which shows that

$$\frac{S_n(p^\alpha)}{p^\alpha} - \frac{S_n(p^{\alpha-1})}{p^{\alpha-1}}$$

for an odd prime and $\alpha > 1$ is an integer. By repeated application of this result, we come to the conclusion that for an odd prime p

$$\frac{S_n(p^\alpha)}{p^\alpha} - \frac{S_n(p)}{p}$$

is an integer.

For $p = 2$ we have

$$\sum_i (s_i + 2^{\alpha-1})^n \equiv 2S_n + 2^{\alpha-1}ns^{n-1} \pmod{2^\alpha},$$

whence

$$S_n(2^\alpha) \equiv 2S_n(2^{\alpha-1}) + 2^{\alpha-1}nS_{n-1}(2^{\alpha-1}) \pmod{2^\alpha}.$$

Now if $n > 1$,

$$S_{n-1}(2^{\alpha-1}) = 1^{n-1} + 2^{n-1} + \dots + (2^{\alpha-1} - 1)^{n-1}.$$

It is clearly an even number if $\alpha \geq 3$ and odd if $\alpha = 2$; hence for $\alpha > 2$ again

$$S_n(2^\alpha) \equiv 2S_n(2^{\alpha-1}) \pmod{2^\alpha},$$

but for $\alpha = 2$

$$S_n(2^2) \equiv 2S_n(2) + 2n \pmod{2^2}.$$

By the same reasoning as before we arrive at the conclusion that for $n > 1$ the difference

$$\frac{S_n(2^\alpha)}{2^\alpha} - \frac{S_n(2)}{2} - \frac{n}{2}$$

is an integer if $\alpha \geq 2$.

Combining these conclusions with the result previously established we derive the theorem due to Staudt:

If n is an even number and p_1, p_2, \dots, p_s are different primes dividing m , then the difference

$$\frac{S_n(m)}{m} - \frac{S_n(p_1)}{p_1} - \frac{S_n(p_2)}{p_2} - \dots - \frac{S_n(p_s)}{p_s}$$

is always an integer.

Chr. von Staudt (1798-1867), often called the "Euclid of the nineteenth century," was a famous German geometer. His treatment of projective geometry, without appeal to metrical considerations, and the purely geometrical introduction of imaginary elements, are achievements of the highest importance. Only a few of Staudt's papers are devoted to number theory, but they are as ingenious as the rest of his work.

8. Reduced System of Residues. All numbers of the same class modulo m have, with m , the same greatest common divisor. For if

$$A \equiv a \pmod{m}$$

and $(a, m) = d$, then

$$A \equiv a \equiv 0 \pmod{d};$$

that is, d is a common divisor of A and m and, as such, divides $(A, m) = d'$. But the same reasoning shows that d' divides d , and so $d = d'$. Classes of integers relatively prime to m are represented in any complete system of residues by members of this system relatively prime to m . If these members are

$$\rho_1, \rho_2, \dots, \rho_{\varphi(m)}$$

they constitute a so-called "reduced system of residues mod m ." Since in the complete system of residues

$$1, 2, 3, \dots, m$$

there are exactly $\varphi(m)$ members relatively prime to m , each reduced system of residues consists of exactly $\varphi(m)$ numbers.

This interpretation of the meaning of $\varphi(m)$ may be used to establish directly the fundamental property of $\varphi(m)$; namely, that

$$\varphi(ab) = \varphi(a)\varphi(b)$$

for relatively prime a and b . Let

$$r_1, r_2, \dots, r_a$$

$$s_1, s_2, \dots, s_b$$

be complete systems of residues for the moduli a and b , respectively. The complete system for the modulus ab is represented by ab numbers

$$as_i + br_j$$

To have a reduced system we must choose from among these numbers those which are relatively prime to ab or, what is the same, to a and b separately. Now

$$as_i + br_j$$

will be relatively prime to a if and only if r_j is relatively prime to a . That restricts the choice of r_j to $\varphi(a)$ numbers. The same number will be relatively prime to b if and only if s_i is relatively prime to b , which restricts the choice of s_i to $\varphi(b)$ numbers. Consequently the reduced system mod ab contains exactly $\varphi(a)\varphi(b)$ numbers; that is,

$$\varphi(ab) = \varphi(a)\varphi(b).$$

By virtue of this fundamental property the evaluation of $\varphi(m)$ is reduced to the particular case $m = p^\alpha$ where p is a prime. Now in the series

$$1, 2, 3, \dots, p^\alpha$$

the only numbers not relatively prime to p are

$$p, 2p, \dots, p^{\alpha-1}p;$$

hence

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p - 1).$$

It is instructive to compare this method of evaluating $\varphi(m)$ with the two methods expounded in Sec. 2 and Sec. 6 of Chap. V. The new method is based on principles of far greater generality than the former two and can be more easily extended to other investigations of similar nature.

Exercises and Problems

1. Let $f(x)$ be a polynomial with integer coefficients, and let $\psi(n)$ denote the number of values

$$f(0), f(1), \dots, f(n-1)$$

relatively prime to n . Show that

$$\psi(ab) = \psi(a)\psi(b)$$

for relatively prime a and b .

2. Show that

$$\psi(p^\alpha) = p^{\alpha-1}(p - \alpha_p)$$

where α_p is the number of integers

$$f(0), f(1), \dots, f(p-1)$$

divisible by the prime p .

3. In case $f(x) = (x - e_1)(x - e_2) \dots (x - e_r)$ where e_1, e_2, \dots, e_r are integers, show that α_p is equal to the number of distinct mod p integers in the series

$$e_1, e_2, \dots, e_r.$$

4. How many integers of the form (a) $x(x+1)$; (b) $x^2 - x$ for $x = 1, 2, \dots, n$ are relatively prime to n ?

5. How many integers of the form

$$(a) \frac{x(x+1)}{2}, \quad (b) \frac{x(x+3)}{2}$$

for $x = 1, 2, \dots, n$ are relatively prime to n ?

6. Supposing that a, b, c are three positive integers without common divisors, show that among the fractions

$$\frac{a}{c}, \frac{a+b}{c}, \frac{a+2b}{c}, \dots, \frac{a+(c-1)b}{c}$$

there are exactly $\frac{\varphi(bc)}{\varphi(b)}$ fractions in simplest terms.

7. Letting a and b assume independently the values $1, 2, \dots, n$, we have n^2 different pairs (a, b) . Show that the number of pairs satisfying the condition $(a, b, n) = 1$ is

$$n^2 \left(1 - \frac{1}{p_1^2}\right) \left(1 - \frac{1}{p_2^2}\right) \dots \left(1 - \frac{1}{p_r^2}\right),$$

p_1, p_2, \dots, p_r being distinct prime divisors of n .

9. **Theorems of Fermat and Euler.** In a letter dated October 18, 1640, addressed to his friend Frenicle, Fermat states a result of which an important theorem, now known as the "little Fermat theorem," is a consequence. In modern notation this theorem amounts to the statement that

$$a^{p-1} - 1$$

is divisible by a prime p if a is not divisible by p . As usual Fermat does not say how he arrived at the result. It was not until 1736 that Euler made public a proof of Fermat's theorem, though it is known now that an identical proof was contained in manuscripts of Leibnitz unpublished at the time. Later Euler discovered a more general theorem:

If a is relatively prime to m , then

$$a^{\varphi(m)} - 1$$

is divisible by m ; from which, in case m is a prime number and consequently $\varphi(m) = m - 1$, Fermat's theorem follows immediately.

The proof of Euler's theorem, depending on the notion of a reduced system of residues mod m , is quite simple. Let

$$\rho_1, \rho_2, \dots, \rho_{\varphi(m)}$$

be a reduced system of residues mod m . Since a is relatively prime to m , the numbers

$$a\rho_1, a\rho_2, \dots, a\rho_{\varphi(m)}$$

form another reduced system and consequently are congruent mod m to the numbers $\rho_1, \rho_2, \dots, \rho_{\varphi(m)}$ taken in a certain order. That is,

$$a\rho_\alpha \equiv \rho_\beta, \quad a\rho_\beta \equiv \rho_\gamma, \quad \dots, \quad a\rho_{\varphi(m)} \equiv \rho_\sigma \pmod{m}$$

where $\alpha, \beta, \dots, \sigma$ coincide in their totality with $1, 2, \dots, \varphi(m)$. On multiplying these congruences, we get

$$a^{\varphi(m)} \rho_1 \rho_2 \dots \rho_{\varphi(m)} \equiv \rho_1 \rho_2 \dots \rho_{\varphi(m)} \pmod{m},$$

and, after cancellation of $\rho_1 \rho_2 \dots \rho_{\varphi(m)}$, which is relatively prime to m ,

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

But this is Euler's theorem in congruence notation.

10. Another Proof. Originally Euler proved Fermat's theorem in a totally different way based on the use of the binomial expansion and the almost evident fact that the binomial coefficient

$$C_p^i = \frac{p(p-1) \dots (p-i+1)}{1 \cdot 2 \dots i}$$

for $i < p$ is divisible by a prime p . In fact

$$1 \cdot 2 \dots i C_p^i = p(p-1) \dots (p-i+1)$$

is divisible by p , but $1 \cdot 2 \dots i$, consisting of factors $< p$, is not divisible by p ; hence C_p^i is divisible by p .

Fermat's theorem implies that for an arbitrary integer a , divisible by p or not,

$$a^p \equiv a \pmod{p}.$$

This is obvious if a is divisible by p and for a nondivisible by p follows from the congruence

$$a^{p-1} \equiv 1 \pmod{p}$$

equivalent to Fermat's theorem. Conversely, this congruence follows from

$$a^p \equiv a \pmod{p}$$

if a is relatively prime to p . It suffices, therefore, to establish the last congruence. By the binomial theorem we have

$$(a+1)^p = a^p + \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + \cdots + 1,$$

and here all the terms excepting the extreme ones are divisible by p , whence

$$(a+1)^p \equiv a^p + 1 \pmod{p}$$

or

$$(a+1)^p - (a+1) \equiv a^p - a \pmod{p}.$$

By repeated application of this congruence, we conclude

$$a^p - a \equiv (a-1)^p - (a-1) \equiv \cdots \equiv 2^p - 2 \equiv 1^p - 1 \equiv 0 \pmod{p};$$

that is,

$$a^p \equiv a \pmod{p}$$

for any positive integer a . If a is a negative integer, it is congruent to a positive integer α . Now from

$$\alpha^p \equiv \alpha \pmod{p}, \quad \alpha \equiv a \pmod{p}$$

it follows that

$$a^p \equiv a \pmod{p}.$$

Another variant of the same proof is as follows: For two arbitrary integers A, B we have

$$(A + B)^p = A^p + \frac{p}{1}A^{p-1}B + \dots + B^p,$$

whence

$$(A + B)^p \equiv A^p + B^p \pmod{p};$$

again,

$$(A + B + C)^p \equiv (A + B)^p + C^p \equiv A^p + B^p + C^p \pmod{p},$$

and so in general

$$(A + B + \dots + K)^p \equiv A^p + B^p + \dots + K^p \pmod{p}$$

for any number of integers A, B, \dots, K . It suffices to take $A = B = \dots = K = 1$ and denote their number by a to get again

$$a^p \equiv a \pmod{p}.$$

By this method of proof Euler's theorem can be derived as a consequence of Fermat's theorem. The congruence

$$a^{p-1} \equiv 1 \pmod{p}$$

holding for a nondivisible by p amounts to

$$a^{p-1} = 1 + hp$$

with h an integer. Raising both sides to the power p , we have

$$a^{p(p-1)} = 1 + \frac{p}{1}hp + \dots + h^p p^p = 1 + h'p^2$$

with another integer h' . Raising both members to the power p again,

$$a^{p^2(p-1)} = 1 + \frac{p}{1}h'p^2 + \dots + h'^p p^{2p} = 1 + h''p^3$$

with integer h'' . Proceeding in the same way, we establish in general

$$a^{p^{\alpha-1}(p-1)} \equiv 1 \pmod{p^{\alpha}}.$$

Now let

$$m = p^{\alpha} q^{\beta} r^{\gamma} \cdots$$

be a prime factorization of m . Then, since $\phi(m)$ is divisible by $p^{\alpha-1}(p-1)$, raising both members of the preceding congruence to the power $\phi(m)/p^{\alpha-1}(p-1)$ we get

$$a^{\phi(m)} \equiv 1 \pmod{p^{\alpha}}$$

and similarly for a relatively prime to m

$$a^{\phi(m)} \equiv 1 \pmod{q^{\beta}}, \quad a^{\phi(m)} \equiv 1 \pmod{r^{\gamma}}, \quad \dots,$$

whence, because the moduli are relatively prime,
www.dbraulibrary.org.in

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

Exercises and Problems

1. It was surmised for some time that $2^{p-1} - 1$, though divisible by p , is never divisible by p^2 . This would entail important consequences were it true. Show that the surmise is false for $p = 1,093$.
2. There are composite integers n for which $a^{n-1} \equiv 1 \pmod{n}$. Verify this for $a = 2$, $n = 341$; $a = 3$, $n = 121$.
3. Prove that n is a prime number if for some a

$$a^{n-1} \equiv 1 \pmod{n}$$

while none of the congruences

$$a^{\frac{n-1}{p}} \equiv 1, \quad a^{\frac{n-1}{q}} \equiv 1, \quad a^{\frac{n-1}{r}} \equiv 1, \quad \dots \pmod{n},$$

where p, q, r, \dots are distinct prime divisors of $n-1$, holds. Test, in this manner, the number $n = 509$.

4. If $m = p^{\alpha} q^{\beta} r^{\gamma} \cdots$ and $\lambda(m)$ is the l.c.m. of $p^{\alpha-1}(p-1), q^{\beta-1}(q-1), r^{\gamma-1}(r-1), \dots$, then

$$a^{\lambda(m)} \equiv 1 \pmod{m}$$

for a relatively prime to m . The exponent $\lambda(m)$ may be considerably smaller than $\varphi(m)$.

5. Show that every prime number (except 2 and 5) is a factor of an unlimited number of integers all of whose digits are 9. HINT: By Fermat theorem $(10^p)^{p-1} \equiv 1 \pmod{p}$.

6. Show that $n^{13} - n$ for every n has the factor 2,730.

7. Show that "Fermat's quotient"

$$\frac{2^{p-1} - 1}{p}$$

may be a square only for the primes $p = 3$ and $p = 7$.

8. Prove Fermat's theorem by establishing first the congruence

$$(a + 1)^{p-1} - 1 \equiv a \cdot \frac{a^{p-1} - 1}{a + 1} \pmod{p}$$

holding for $a = 1, 2, \dots, p - 2$.

11. Residues of $S_n(p) \pmod{p}$. Let p be a prime, $n \geq 1$ and, as in Sec. 7,

$$S_n(p) = 1^n + 2^n + \dots + (p - 1)^n.$$

Then

$$S_n(p) \equiv 0 \pmod{p}$$

if n is not divisible by $p - 1$, and

$$S_n(p) \equiv -1 \pmod{p}$$

if n is a multiple of $p - 1$. The second part of this statement is a simple consequence of Fermat's theorem. In fact, in case $n \equiv 0 \pmod{p - 1}$

$$1^n \equiv 1, \quad 2^n \equiv 1, \quad \dots, \quad (p - 1)^n \equiv 1 \pmod{p}$$

and

$$S_n(p) \equiv p - 1 \equiv -1 \pmod{p}.$$

The first part will be proved by establishing certain linear relations connecting $S_1(p), S_2(p), \dots$. Take $x = 0, 1, 2, \dots, p - 1$ in the identity

$$(x + 1)^a - x^a = C_a^1 x^{a-1} + C_a^2 x^{a-2} + \dots + C_a^{a-1} x + 1$$

and sum the results. We get, then, for $a > 1$

$$p^a - p = C_a^1 S_{a-1}(p) + C_a^2 S_{a-2}(p) + \cdots + C_a^{a-1} S_1(p);$$

that is,

$$C_a^1 S_{a-1}(p) + C_a^2 S_{a-2}(p) + \cdots + C_a^{a-1} S_1(p) \equiv 0 \pmod{p}.$$

Take here $a = 2, 3, \dots, p-1$; from the resulting system of congruences

$$2S_1(p) \equiv 0$$

$$3S_2(p) + 3S_1(p) \equiv 0$$

$$4S_3(p) + 6S_2(p) + 4S_1(p) \equiv 0$$

$$\dots$$

$$(p-1)S_{p-2}(p) + \frac{(p-1)(p-2)}{2} S_{p-3}(p) + \cdots + (p-1)S_1(p) \equiv 0$$

it follows successively

$$S_1(p) \equiv 0, \quad S_2(p) \equiv 0, \quad \dots, \quad S_{p-2}(p) \equiv 0 \pmod{p},$$

and this proves the first part of the theorem for n nondivisible by p and less than $p-1$.

If n is not divisible by $p-1$ and $> p-1$, then, on dividing n by $p-1$, we have

$$n = (p-1)b + r$$

with $r < p-1$ and positive. By Fermat's theorem

$$K^n \equiv K^r \pmod{p}; \quad K = 1, 2, \dots, p-1$$

and

$$S_n(p) \equiv S_r(p) \equiv 0 \pmod{p}.$$

In Sec. 6 it was established that

$$\frac{S_{2n}(m)}{m} - \frac{S_{2n}(p_1)}{p_1} - \cdots - \frac{S_{2n}(p_s)}{p_s}$$

is an integer if p_1, p_2, \dots, p_s are all distinct prime divisors of m . By what is proved in the present section

$$\frac{S_{2n}(p)}{p}$$

is an integer if $2n$ is not divisible by $p - 1$ and

$$\frac{S_{2n}(p) + 1}{p}$$

is an integer if $2n$ is divisible by $p - 1$. Denoting therefore by a, b, c, \dots all distinct primes dividing m and such that $a - 1, b - 1, c - 1, \dots$ are divisors of $2n$, we conclude that

$$\frac{S_{2n}(m)}{m} + \frac{1}{a} + \frac{1}{b} + \frac{1}{c} + \dots$$

is always an integer. This elegant theorem is also due to Staudt.

12. Wilson's Theorem. An English mathematician of the eighteenth century, Waring, in his book "Meditationes algebraicae" (1770) reports a very interesting property of primes communicated to him by an amateur in science, a certain Wilson. It goes by the name of Wilson's theorem, though we know now that the same property was observed much earlier by Leibnitz, and consists in the fact that

$$1 \cdot 2 \cdot 3 \cdots (p - 1) + 1$$

is always divisible by a prime p or, in congruence notation,

$$1 \cdot 2 \cdot 3 \cdots (p - 1) + 1 \equiv 0 \pmod{p}.$$

Confessing his inability to prove this theorem, Waring adds that the proof must be very difficult because there is *no notation* to designate primes only. Of this Gauss observes that proofs of such truths must depend rather on *notions* than on notations. The first proof of Wilson's theorem was given by Lagrange in 1771.

Joseph Louis Lagrange (1736-1813), an Italian by birth, though he wrote only in French, was perhaps the greatest mathematician of the eighteenth century. Napoleon used to call him "Little Pyramid," and such he was indeed. Lagrange's merits are great and many. He was the first after Euler to devote considerable time, against the advice of his friend D'Alembert, to speculations in number theory. Lagrange was the first to prove that every integer is a sum of four squares and to lay a foundation to the arithmetical theory of binary quadratic forms.

We shall present here a very simple proof (based indeed on "notions") due to Gauss. If a is any number of the series

$$1, 2, \dots, p - 1,$$

then

$$a, 2a, \dots, (p - 1)a$$

form a complete system of residues mod p with the exclusion of 0. Consequently one and only one of the numbers is congruent to 1 mod p . In other words, to any $a = 1, 2, \dots, p - 1$ corresponds one and only one number in the same series, such that

$$aa' \equiv 1 \pmod{p}.$$

Such two numbers are called *associate numbers*. Numbers which are identical with their associates are 1 and $p - 1$. Indeed the congruence

$$a^2 \equiv 1 \pmod{p}$$

is equivalent to

$$(a - 1)(a + 1) \equiv 0 \pmod{p},$$

whence either $a \equiv 1 \pmod{p}$, that is, $a = 1$; or $a \equiv -1 \pmod{p}$, that is, $a = p - 1$. If we exclude 1 and $p - 1$, all the remaining numbers

$$2, 3, \dots, p - 2$$

can be combined in pairs of associate numbers, and we shall have as many congruences of the type

$$aa' \equiv 1 \pmod{p}$$

as there are such pairs. Multiplying all these congruences member by member, in the left-hand side we shall have the product $2 \cdot 3 \cdots (p - 2)$, while the right-hand side will be 1. Thus

$$2 \cdot 3 \cdots (p - 2) \equiv 1 \pmod{p},$$

and multiplying this by

$$1(p - 1) \equiv -1 \pmod{p},$$

we get

$$1 \cdot 2 \cdot 3 \cdots (p - 1) \equiv -1 \pmod{p},$$

which is equivalent to Wilson's theorem.

To illustrate this proof by an example, let us take $p = 13$. Then the associate pairs are: 2, 7; 3, 9; 4, 10; 5, 8; 6, 11; and

$$\begin{aligned} 2 \cdot 7 &\equiv 1, & 3 \cdot 9 &\equiv 1, & 4 \cdot 10 &\equiv 1, & 5 \cdot 8 &\equiv 1, \\ & & 6 \cdot 11 &\equiv 1 \pmod{13}. \end{aligned}$$

The product of the left-hand sides is $2 \cdot 7 \cdot 3 \cdot 9 \cdot 4 \cdot 10 \cdot 5 \cdot 8 \cdot 6 \cdot 11$, or, rearranging the factors, $2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \cdot 11$.

Wilson's theorem expresses a characteristic property of primes. For if p is a composite number, then there is a factorization

$$p = ab,$$

where $1 < a < p$. Then a occurs as a factor in the product $1 \cdot 2 \cdot 3 \cdots p - 1$, and the congruence

$$1 \cdot 2 \cdot 3 \cdots (p - 1) + 1 \equiv 0 \pmod{a}$$

is impossible; much less is it possible modulo p .

If p is an odd prime, we can write

$$\frac{p + 1}{2} = p - \frac{p - 1}{2} \equiv -\frac{p - 1}{2}$$

$$\frac{p + 3}{2} = p - \frac{p - 3}{2} \equiv -\frac{p - 3}{2}$$

$$\dots \dots \dots$$

$$p - 1 = p - 1 \equiv -1,$$

all modulo p . Consequently

$$\frac{p+1}{2} \cdot \frac{p+3}{2} \cdots (p-1) \equiv (-1)^{\frac{p-1}{2}} \cdot 1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2},$$

and on account of this, Wilson's congruence takes the form

$$(-1)^{\frac{p-1}{2}} \left(1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2} \right)^2 + 1 \equiv 0 \pmod{p}$$

or

$$\left(1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2} \right)^2 + (-1)^{\frac{p-1}{2}} \equiv 0 \pmod{p}.$$

Now we have to distinguish two cases: $p \equiv 1 \pmod{4}$ or else $p = 4n + 1$, and $p \equiv 3 \pmod{4}$ or else $p = 4n + 3$. In the former case

$$\left(1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2} \right)^2 + 1 \equiv 0 \pmod{p}.$$

This means that -1 is the residue of a square or *quadratic residue* if the modulus is a prime of the form $4n + 1$, a rather deep property of such primes.

If p is of the form $4n + 3$, then

$$\left(1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2} \right)^2 \equiv 1 \pmod{p}$$

and

$$1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2} \equiv \pm 1 \pmod{p}.$$

There is no simple rule which would permit us to decide a priori which of the two signs \pm holds in this congruence. For some primes it is $+$ and for some it is $-$, but whether the first or the second case occurs is not decided by some *simple* property of the prime itself. From quite a heterogeneous source Kronecker derived the following interesting rule:

Subtract from p squares of even numbers as far as one can go without getting negative numbers. Count how many differences

$$p - 2^2, p - 4^2, p - 6^2, \dots$$

are of the form

$$r^{4i+1}s^2$$

where r is a prime not dividing s and $i \geq 0$. If there are μ differences of this form, then

$$1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2} \equiv (-1)^\mu \pmod{p}.$$

For example, take $p = 127$. Then

$$\begin{aligned} 127 - 2^2 &= 3 \cdot 41; & 127 - 4^2 &= 3 \cdot 37; \\ 127 - 6^2 &= 7 \cdot 13; & 127 - 8^2 &= 7 \cdot 3^2; & 127 - 10^2 &= 3^3. \end{aligned}$$

In this example $\mu = 1$, corresponding to a single underlined equation; consequently

$$1 \cdot 2 \cdot 3 \cdots 63 \equiv -1 \pmod{127}.$$

Exercises and Problems

1. Can $1 \cdot 2 \cdot 3 \cdots (p-1) + 1$, which is divisible by the odd prime p , be a power of this prime?

Ans. This can be only for $p = 3$ and $p = 5$.

2. For a prime $p \equiv 1 \pmod{4}$

$$\left(1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2}\right)^2 + 1$$

is divisible by p . Can this number be a power of p ?

Ans. Only for $p = 5$.

3. Show that for p a prime and $0 < s < p$

$$(s-1)!(p-s)! + (-1)^{s-1} \equiv 0 \pmod{p}.$$

4. Show that

$$C_m^n \equiv C_{m_1}^{n_1} C_{\mu_1}^{r_1} \pmod{p}$$

where m_1, μ_1 and n_1, ν_1 are the respective quotients and remainders in the division of m and n by a prime p . The symbol C_m^n , when it occurs, means always 1. Apply this to $m = 1,000, n = 500, p = 11$.

Ans. $C_{11}^{500} \equiv 0 \pmod{13}$.

5. Prove that the coefficients c_1, c_2, c_3, \dots of the expansion

$$\frac{1 + x + x^2 + \dots + x^{p-1}}{(1-x)^{p-1}} = 1 + c_1x + c_2x^2 + \dots$$

are integers divisible by p if p is prime.

6. If r_1, r_2, \dots, r_p and s_1, s_2, \dots, s_p are two complete systems of residues modulo prime p , then p numbers $r_1s_1, r_2s_2, \dots, r_ps_p$ do not represent a complete system of residues.

7. Prove Wilson's theorem by using the well-known identity

$$(p-1)^{p-1} - C_{p-1}^1(p-2)^{p-1} + C_{p-1}^2(p-3)^{p-1} - \dots + (-1)^{p-2}C_{p-1}^{p-2} \cdot 1^{p-1} = 1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-1).$$

This identity itself results from the fact that the n th difference of any polynomial of degree n and with the leading coefficient 1 is $1 \cdot 2 \cdot 3 \cdot \dots \cdot n$ provided the increment of the argument is $= 1$.

APPENDIX

ON MAGIC SQUARES

1. Definition of Magic Squares. By a magic square we mean a square divided into n^2 cells in which numbers from 1 to n^2 are placed in such a manner that sums of the numbers in all horizontal and vertical rows, as well as both diagonals, are the same. The common value of these sums is

$$\frac{n(n^2 + 1)}{2}$$

since the sum of all numbers 1, 2, . . . , n^2 amounts to

$$\frac{n^2(n^2 + 1)}{2}$$

For example, the squares

8	1	6
3	5	7
4	9	2

1	14	15	4
12	7	6	9
8	11	10	5
13	2	3	16

are magic squares of 9 and 16 cells. Since remote times magic squares have been known in China and India, but it seems that their knowledge was not widespread in Europe until the fifteenth century. Later men such as Fermat and Euler did not deem it below their dignity to spend time on methods for constructing such squares. Despite innumerable efforts of men of science and amateurs, we do not possess methods for the construction of all possible magic squares, nor is their number known except for $n = 3$ and $n = 4$. But there are

numerous particular methods for their construction, and one of them, based on congruence properties of numbers, we shall endeavor to explain in the appendix. It affords a good illustration of rather abstract principles laid down in this chapter and may help to make these principles more attractive to beginners.

2. Auxiliary Squares. Every number k from 1 to n can be represented in a unique manner in the form

$$k = nr + s$$

where r coincides with one of the numbers $0, 1, 2, \dots, n-1$ and s with one of the numbers $1, 2, \dots, n$. We shall call r and s , respectively, the first and the second component of k . If we take the first and the second components of all the numbers in a magic square and place them in the same cells, we get two auxiliary squares, I and II. For instance, auxiliary squares corresponding to the magic square of nine cells shown above are

2	0	1
0	1	2
1	2	0

I

2	1	3
3	2	1
1	3	2

II

Similarly auxiliary squares to the above-shown magic square of 16 cells are

0	3	3	0
2	1	1	2
1	2	2	1
3	0	0	3

I

1	2	3	4
4	3	2	1
4	3	2	1
1	2	3	4

II

We notice in these examples that the auxiliary squares are also magic; that is, they have constant sums in all horizontal and vertical rows and in both diagonals. But it is not necessarily so for any magic square. Conversely, by constructing auxiliary magic squares, one made up of numbers $0, 1, 2, \dots, n-1$ and another of numbers $1, 2, 3, \dots, n$, we can make a magic square of n^2 cells by placing in each cell the product by n of the number occupying the same cell in the first auxiliary square and adding the number occupying the same cell in the second auxiliary square, *provided that the n^2 numbers thus obtained are different*. Because, if different, these numbers will be $1, 2, \dots, n^2$; moreover, sums in the horizontal and vertical rows as well as in the two diagonals will be equal if this is so in the auxiliary squares.

As to the construction of auxiliary magic squares, we must distinguish three cases according as n is odd, or divisible by 4, or only divisible by 2, the last case being the hardest.

3. Magic Squares for Odd n . Let us denote by symbols $(0), (1), (2), \dots, (n-1)$ the numbers $0, 1, 2, \dots, n-1$ taken in a certain order to be specified later. The symbol (k) , for an arbitrary integer k , will then be defined by the requirement $(k') = (k)$ if $k' \equiv k \pmod{n}$. Horizontal rows of cells from the top down will be denoted by $0, 1, 2, \dots, n-1$. Similarly, vertical columns of cells from left to right will be marked by the same numbers. Then each cell will be characterized by two integers i and j , corresponding to the row and column to which the cell belongs. To form the first auxiliary square we fill the cell (i, j) with $(i+j)$; then the square will be magic in rows and columns. In fact, since $i+j$ for a fixed i and variable j runs over a complete system of residues mod n , the cells of all horizontal rows will be filled with the numbers $(0), (1), (2), \dots, (n-1)$, and the same will hold for the vertical columns. On the descending diagonal $i=j$, so that its cells will be filled with the numbers $(0), (2),$

(4), . . . , $(2n - 2)$, which coincide save for order with (0), (1), (2), . . . $(n - 1)$, since for an odd n the numbers 0, 2, 4, . . . , $2n - 2$ form a complete system of residues. On the ascending diagonal $i + j = n - 1$, and its cells will all contain the same number $(n - 1)$. To make this diagonal magic, we must subject the symbol $(n - 1)$ to the condition

$$n(n - 1) = (0) + (1) + \cdots + (n - 1) = \frac{n^2 - n}{2};$$

that is, we must take $(n - 1) = \frac{n - 1}{2}$. As to the other symbols, they may be identified with the remaining numbers in any order. Under such circumstances the first auxiliary square will be magic. For example, for $n = 5$ we may take

$$(0) = 4, \quad (1) = 3, \quad (2) = 1, \quad (3) = 0, \quad (4) = 2.$$

Then the first auxiliary square is

4	3	0	1	2
3	0	1	2	4
0	1	2	4	3
1	2	4	3	0
2	4	3	0	1

The construction of the second auxiliary square is very similar. We denote by symbols $\langle 0 \rangle$, $\langle 1 \rangle$, . . . , $\langle n - 1 \rangle$ the numbers 1, 2, . . . , n taken in a certain order, and to define the symbol $\langle k \rangle$ for an arbitrary integer k we set forth the requirement $\langle k' \rangle = \langle k \rangle$ if $k' \equiv k \pmod{n}$. Now we place in cell (i, j) the number $\langle i - j \rangle$. Then, since $i - j$ for a fixed j and variable i , and also for a fixed i and variable j , runs over a complete system of residues mod n , the square will be magic in rows and columns. The ascending

diagonal is filled with numbers $\langle 2i + 1 \rangle$ which, save for order, coincide with $\langle 0 \rangle$, $\langle 1 \rangle$, \dots , $\langle n - 1 \rangle$; consequently it will be magic also. But all cells of the descending diagonal will be filled with $\langle 0 \rangle$. To make it magic the condition

$$n\langle 0 \rangle = 1 + 2 + 3 + \dots + n = \frac{n^2 + n}{2}$$

must be fulfilled, so that we must take $\langle 0 \rangle = \frac{n + 1}{2}$.

As for the other symbols, they may be identified with the remaining numbers in any order. If for $n = 5$ we take

$$\langle 0 \rangle = 3, \quad \langle 1 \rangle = 1, \quad \langle 2 \rangle = 4, \quad \langle 3 \rangle = 2, \\ \langle 4 \rangle = 5,$$

the second auxiliary square will be

3	5	2	4	1
1	3	5	2	4
4	1	3	5	2
2	4	1	3	5
5	2	4	1	3

Combining two auxiliary squares as explained above we get a square whose cell (i, j) is occupied by

$$n(i + j) + \langle i - j \rangle.$$

It remains to show that the numbers in different cells are different. If cells (i, j) and (i', j') contain the same number, then

$$n(i' + j') + \langle i' - j' \rangle = n(i + j) + \langle i - j \rangle$$

and

$$(i' + j') = (i + j), \quad \langle i' - j' \rangle = \langle i - j \rangle;$$

that is,

$$i' + j' \equiv i + j, \quad i' - j' \equiv i - j \pmod{n},$$

whence

$$2(i' - i) \equiv 0, \quad 2(j' - j) \equiv 0 \pmod{n}$$

or

$$i' - i \equiv 0, \quad j' - j \equiv 0 \pmod{n}.$$

This is possible only if $i' = i, j' = j$. Combining the auxiliary squares for $n = 5$, we get the magic square of 25 cells:

23	20	2	9	11
16	3	10	12	24
4	6	13	25	17
7	14	21	18	5
15	22	1	8	19

It is clear that by this method a great number of magic squares for the same n may be obtained. Also, the way of filling cells of auxiliary squares can be greatly generalized. This, however, we can not discuss here.

4. Magic Squares for n Divisible by 4. In case $n = 4m$, we may fill cell (i, j) of the first auxiliary square with $(i + 2mj)$. Then the square will be magic in columns and also magic in both diagonals. For on the descending diagonal $i = j$ and the numbers $(2m + 1)i$ for variable i form a complete system of residues mod $4m$ because $2m + 1$ is relatively prime to $4m$. On the ascending diagonal $j = 4m - 1 - i$, and the numbers $-(2m - 1)i + 2m(4m - 1)$ form a complete system of residues mod $4m$ for i variable. As to the rows, they will be magic on certain conditions. The i th row contains only symbols (i) and $(i + 2m)$, each repeated $2m$ times. In

order to make this row magic, the following condition must be fulfilled.

$$2m[(i) + (i + 2m)] = (0) + (1) + \dots + (4m - 1) \\ = 2m(4m - 1),$$

whence

$$(i) + (i + 2m) = 4m - 1.$$

We may identify (0) with any of the numbers 0, 1, 2, ..., $4m - 1$; then (2*m*) will be determined. Again (1) can be identified with any of the remaining numbers and (2*m* + 1) will be determined, and so on.

The cell (*i*, *j*) of the second auxiliary square we may fill with $\langle 2mi + j \rangle$. The square will be magic if the symbols $\langle j \rangle$ satisfy the condition

$$\langle j \rangle + \langle j + 2m \rangle = 4m + 1.$$

By combining the two auxiliary squares, we get a square whose cell (*i*, *j*) contains

$$4m(i + 2mj) + \langle 2mi + j \rangle.$$

Two cells (*i*, *j*) and (*i'*, *j'*) will contain different numbers, for otherwise we must have

$$i' + 2mj' \equiv i + 2mj \pmod{4m} \\ 2mi' + j' \equiv 2mi + j \pmod{4m}$$

or

$$i' - i + 2m(j' - j) \equiv 0 \pmod{4m} \\ 2m(i' - i) + j' - j \equiv 0 \pmod{4m},$$

whence

$$(4m^2 - 1)(i' - i) \equiv 0, \quad (4m^2 - 1)(j' - j) \equiv 0 \pmod{4m};$$

but $4m^2 - 1$ and $4m$ are relatively prime, and consequently

$$i' - i \equiv 0, \quad j' - j \equiv 0 \pmod{4m};$$

that is, $i' = i$, $j' = j$.

As an example, let us construct by this method the magic square of 16 cells. We may take $\langle 0 \rangle = 0$, $\langle 2 \rangle = 3$, $\langle 1 \rangle = 2$, $\langle 3 \rangle = 1$. The resulting first auxiliary square will be

0	3	0	3
2	1	2	1
3	0	3	0
1	2	1	2

If we take $\langle 0 \rangle = 1$, $\langle 2 \rangle = 4$, $\langle 1 \rangle = 3$, $\langle 3 \rangle = 2$, the second auxiliary square will be

1	3	4	2
4	2	1	3
1	3	4	2
4	2	1	3

and, by combining both auxiliary squares, we get the following magic square of 16 cells:

1	15	4	14
12	6	9	7
13	3	16	2
8	10	5	11

5. Magic Squares for n Divisible by 2 Only. The construction of magic squares in case $n = 2m$ and m is an odd number is not so simple as in the two preceding cases. We begin by filling cell (i, j) of the two auxiliary squares with the numbers

$$\left(mi + j + m \left[\frac{i}{m} \right] \right), \quad \left\langle i + mj + m \left[\frac{j}{m} \right] \right\rangle$$

and choose the symbols (k) and $\langle k \rangle$ so that

$$\begin{aligned} (k) + (m + k) &= 2m - 1, & k &= 0, 1, 2, \dots, m - 1, \\ \langle k \rangle + \langle m + k \rangle &= 2m + 1, \\ k &= 0, 1, 2, 3, \dots, m - 1. \end{aligned}$$

If the numbers occupying a certain cell in the first and second auxiliary squares are (a) and $\langle b \rangle$, the double symbol (ab) is defined by

$$(ab) = n(a) + \langle b \rangle.$$

With our method of filling cells of auxiliary squares, all n^2 double symbols will be different. To prove this, suppose that the double symbols corresponding to cells (i, j) and (i', j') are identical. This requires the fulfillment of the two congruences

$$\begin{aligned} i' - i + m(j' - j) &\equiv m \left[\frac{j'}{m} \right] - m \left[\frac{j}{m} \right] \pmod{2m} \\ m(i' - i) + j' - j &\equiv m \left[\frac{i}{m} \right] - m \left[\frac{i'}{m} \right] \pmod{2m}. \end{aligned}$$

For the modulus m we have

$$i' - i \equiv 0, \quad j' - j \equiv 0 \pmod{m},$$

and so

$$i' - i = m\epsilon, \quad j' - j = m\eta,$$

where

$$\epsilon = 0, 1, -1; \quad \eta = 0, 1, -1.$$

Correspondingly,

$$\left[\frac{i'}{m} \right] = \epsilon + \left[\frac{i}{m} \right], \quad \left[\frac{j'}{m} \right] = \eta + \left[\frac{j}{m} \right],$$

and, on substituting these expressions into the original congruences mod $2m$ and dividing both sides and modulus by m , we get

$$\epsilon + (m + 1)\eta \equiv 0, \quad (m + 1)\epsilon + \eta \equiv 0 \pmod{2}.$$

But m is an odd number; so $\epsilon \equiv 0, \eta \equiv 0 \pmod{2}$, and that is possible only for $\epsilon = 0, \eta = 0$; that is, $i' = i, j' = j$. Thus our statement is proved.

The first auxiliary square, as can easily be seen, is magic in rows and diagonals, but not in columns. Similarly, the second square is magic in columns and diagonals but not in rows. In case $n = 6$, the auxiliary squares are

(A)

(0)	(1)	(2)	(3)	(4)	(5)
(3)	(4)	(5)	(0)	(1)	(2)
(0)	(1)	(2)	(3)	(4)	(5)
(0)	(1)	(2)	(3)	(4)	(5)
(3)	(4)	(5)	(0)	(1)	(2)
(0)	(1)	(2)	(3)	(4)	(5)

www.dbraulibrary.org.in

(B)

<0>	<3>	<0>	<0>	<3>	<0>
<1>	<4>	<1>	<1>	<4>	<1>
<2>	<5>	<2>	<2>	<5>	<2>
<3>	<0>	<3>	<3>	<0>	<3>
<4>	<1>	<4>	<4>	<1>	<4>
<5>	<2>	<5>	<5>	<2>	<5>

and the corresponding square of double symbols is

(C)

(00)	(13)	(20)	(30)	(43)	(50)
(31)	(44)	(51)	(01)	(14)	(21)
(02)	(15)	(22)	(32)	(45)	(52)
(03)	(10)	(23)	(33)	(40)	(53)
(34)	(41)	(54)	(04)	(11)	(24)
(05)	(12)	(25)	(35)	(42)	(55).

It is magic in diagonals but not in rows and columns. Now we transform square (*A*) by placing columns 4, 5, 6 in the reverse order, 6, 5, 4; square (*B*) is similarly transformed by placing rows 4, 5, 6 in the reverse order, 6, 5, 4. The transformed squares are

(A')

(0)	(1)	(2)	(5)	(4)	(3)
(3)	(4)	(5)	(2)	(1)	(0)
(0)	(1)	(2)	(5)	(4)	(3)
(0)	(1)	(2)	(5)	(4)	(3)
(3)	(4)	(5)	(2)	(1)	(0)
(0)	(1)	(2)	(5)	(4)	(3)

(B')

<0>	<3>	<0>	<0>	<3>	<0>
<1>	<4>	<1>	<1>	<4>	<1>
<2>	<5>	<2>	<2>	<5>	<2>
<5>	<2>	<5>	<5>	<2>	<5>
<4>	<1>	<4>	<4>	<1>	<4>
<3>	<0>	<3>	<3>	<0>	<3>

Notice that both of their diagonals consist of the numbers (0), (1), (2), (3), (4), (5), and <0>, <1>, <2>, <3>, <4>, <5>. The square (*C*) undergoes the change which amounts to placing columns 4, 5, 6 and rows 4, 5, 6 in the reverse order, 6, 5, 4. The transformed square is

(C')

(00)	(13)	(20)	(50)	(43)	(30)
(31)	(44)	(51)	(21)	(14)	(01)
(02)	(15)	(22)	(52)	(45)	(32)
(05)	(12)	(25)	(55)	(42)	(35)
(34)	(41)	(54)	(24)	(11)	(04)
(03)	(10)	(23)	(53)	(40)	(33)

It contains the same 36 double symbols as (C) and remains magic in both diagonals. Notice that the series of second components in the first row

$$0 \ 3 \ 0 | 0 \ 3 \ 0$$

and the first components in the first column

$$0 \ 3 \ 0 | 0 \ 3 \ 0$$

are symmetrical about their middle. This is a very important fact which allows a further transformation of (C'), as follows: in the two middle columns in the first row exchange 2 and 5; in columns 2 and 5 of the first row exchange 1 and 4. Exchange also 2 and 5, 1 and 4, in the first column. Such exchanges do not alter symbols of the first row and column in their totality and do not affect the diagonals. The resulting square (C'')

(C'')

(00)	(43)	(30)	(20)	(13)	(30)
(34)	(44)	(51)	(21)	(14)	(01)
(05)	(15)	(22)	(52)	(45)	(32)
(02)	(12)	(25)	(55)	(42)	(35)
(31)	(41)	(54)	(24)	(11)	(04)
(03)	(10)	(23)	(53)	(40)	(33)

is now magic in its diagonals and all rows and columns *except* rows 1, 6, and columns 1, 6. In fact, take for example the second column. The first components of its symbols are

$$4, 4, 1, 1, 4, 1;$$

that is, it contains 4 and 1 each three times, while the second components are six different numbers:

$$3, 4, 5, 2, 1, 0.$$

By the choice of symbols, therefore, the second column is magic and, for the same reason, that is also true of columns

3, 4, 5. Take again, say, the third row. The second components of its symbols are

5, 5, 2, 2, 5, 2,

so that 5 and 2 each occurs three times, while the first components are

0, 1, 2, 5, 4, 3.

Consequently the third row, and similarly other rows except 1 and 6, are magic.

In the square (C'') now we take only the two middle rows and columns as shown:

		(50)	(20)		
		(51)	(21)		
(05)	(15)	(22)	(52)	(45)	(32)
(02)	(12)	(25)	(55)	(42)	(35)
		(54)	(24)		
		(23)	(53)		

Then we exchange 0 and 3 in the third line and column. This gives

		(53)	(20)		
		(51)	(21)		
(35)	(15)	(22)	(52)	(45)	(02)
				↓	↓
(02)	(12)	(25)	(55)	(42)	(35)
		(54)	(24)		
		↑	↑		
		(20)	(53),		
		↑	↑		

but here we get four pairs of identical symbols (02), (20), (35), (53), which troublesome circumstance disappears after two double exchanges of 2 and 5 as indicated in the diagram. The resulting middle rows and columns, when completed by other symbols left untouched, finally produce a square

(00)	(43)	(53)	(20)	(13)	(30)
(34)	(44)	(51)	(21)	(14)	(01)
(35)	(15)	(22)	(52)	(42)	(05)
(02)	(12)	(25)	(55)	(45)	(32)
(31)	(41)	(24)	(54)	(11)	(04)
(03)	(10)	(50)	(23)	(40)	(33)

which is magic in all rows, columns, and diagonals. This method, though explained for a particular example, is general, as anyone can convince himself after a careful examination of the whole procedure.

To produce actually a magic square of 36 cells, let us take for example

$$\begin{array}{llll}
 (0) = 0, & (3) = 5; & \langle 0 \rangle = 1, & \langle 3 \rangle = 6 \\
 (1) = 1, & (4) = 4; & \langle 1 \rangle = 2, & \langle 4 \rangle = 5. \\
 (2) = 2, & (5) = 3; & \langle 2 \rangle = 3, & \langle 5 \rangle = 4.
 \end{array}$$

Then, evaluating numerically the double symbols, we get the following magic square:

1	30	24	13	12	31
35	29	20	14	11	2
34	10	15	21	27	4
3	9	16	22	28	33
32	26	17	23	8	5
6	7	19	18	25	36

CHAPTER VII

CONGRUENCES WITH ONE UNKNOWN. LAGRANGE'S THEOREM AND ITS APPLICATIONS

1. Congruences in General. Let

$$f(x) = p_0x^n + p_1x^{n-1} + \dots + p_n$$

be a polynomial with integer coefficients and m an integer considered as a modulus. To solve a numerical congruence

$$p_0x^n + p_1x^{n-1} + \dots + p_n \equiv 0 \pmod{m}$$

one is required to find all integers which, when substituted for x , satisfy this congruence. Such integers are called the roots of the congruence.

Since

$$f(a') \equiv f(a) \pmod{m}$$

when

$$a' \equiv a \pmod{m},$$

it is clear that the congruence, being satisfied by one number, will be satisfied by all numbers of the class to which it belongs modulo m . The class of numbers modulo m is completely characterized by one of its members; consequently, for a complete solution of the congruence, it suffices to exhibit roots belonging to different classes; that is, roots distinct modulo m . When speaking of the number of roots we, therefore, always mean the number of distinct roots. Theoretically all the distinct solutions of a congruence

$$f(x) \equiv 0 \pmod{m}$$

can be found by substituting for x members of a complete system of residues, for instance, the numbers $0, 1, 2, \dots, m - 1$, and ascertaining which of the numbers

$$f(0), f(1), \dots, f(m - 1)$$

are divisible by m . If none of these numbers is divisible by m , then the congruence is impossible and has no roots. When the modulus is small, this procedure may be used in practice.

Congruences, like equations, are classified according to their degree. The congruence

$$p_0x^n + p_1x^{n-1} + \dots + p_n \equiv 0 \pmod{m}$$

is of degree n if p_0 is not divisible by m ; otherwise it is equivalent to a congruence of a lower degree. Thus

$$3x^3 - 6x^2 + 5x - 3 \equiv 0 \pmod{7}$$

is a congruence of the third degree, while

$$6x^3 - 3x^2 + 7x - 1 \equiv 0 \pmod{6}$$

is equivalent to the following second-degree congruence:

$$-3x^2 + 7x - 1 \equiv 0 \pmod{6}.$$

Example 1. Consider the congruence

$$f(x) = x(x + 1)(2x + 1) \equiv 0 \pmod{6}.$$

By trial we find

$$f(0) = 0, \quad f(1) = 6, \quad f(2) = 30, \quad f(3) = 84, \quad f(4) = 180, \\ f(5) = 330;$$

and since all these numbers are divisible by 6, we conclude that the proposed congruence has six solutions:

$$x \equiv 0, \quad x \equiv 1, \quad x \equiv 2, \quad x \equiv 3, \quad x \equiv 4, \quad x \equiv 5 \pmod{6}.$$

In other words, all integers satisfy this congruence, and

$$\frac{x(x+1)(2x+1)}{6}$$

is an integer for all integral x .

Example 2. Let us try to find solutions, if any, of the congruence

$$f(x) = 3x^2 - 6x^2 + 5x - 3 \equiv 0 \pmod{7}.$$

By substituting $x = 0, \pm 1, \pm 2, \pm 3$, which form a complete system of residues mod 7, we find

$$\begin{aligned} f(0) &= -3, & f(1) &= -1, & f(2) &= 7, & f(3) &= 39 \\ f(-1) &= -17, & f(-2) &= -61, & f(-3) &= -153. \end{aligned}$$

Hence the congruence has one root

$$x \equiv 2 \pmod{7}.$$

Example 3. To solve the congruence

$$f(x) = x^4 - 2 \equiv 0 \pmod{13}$$

we substitute $x = 0, \pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \pm 6$. Since none of the numbers

$$\begin{aligned} f(0) &\equiv -2, & f(\pm 1) &\equiv -1, & f(\pm 2) &\equiv +1, & f(\pm 3) &\equiv 1 \\ f(\pm 4) &\equiv 7, & f(\pm 5) &\equiv -1, & f(\pm 6) &\equiv 7 \pmod{13} \end{aligned}$$

is divisible by 13, the congruence is impossible.

Exercises

1. Solve the congruence

$$x^2 - 3 \equiv 0 \pmod{13}.$$

Ans. Impossible.

2. Solve the congruence

$$2x^2 - 3x + 9 \equiv 0 \pmod{11}.$$

Ans. $x \equiv 2, 5 \pmod{11}$.

3. Solve the congruence

$$x^4 + 2x^2 + 4 \equiv 0 \pmod{7}.$$

Ans. $x \equiv \pm 1, \pm 2 \pmod{7}$.

2. Congruences of the First Degree. It is natural to start with congruences of the first degree. Such congruences can always be taken in the form

$$ax \equiv b \pmod{m},$$

and we can distinguish two cases according as a and m are relatively prime or not. If a and m are relatively prime, then the numbers

$$0, a, 2a, \dots, (m-1)a$$

form a complete system of residues modulo m . Consequently one and only one of them is of the same class as b . If this number is ax_0 , then x_0 is the unique solution of the proposed congruence mod m and all other roots of the same are congruent $x_0 \pmod{m}$.

If a and m are not relatively prime, let d be their g.c.d. Then the proposed congruence is impossible if b is not divisible by d ; otherwise it is entirely equivalent to the congruence

$$\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}},$$

in which a/d and m/d are relatively prime numbers. Hence this congruence has a unique solution $x_0 \pmod{m/d}$; that is, all its roots as well as the roots of the congruence

$$ax \equiv b \pmod{m}$$

are

$$x = x_0 + \frac{m}{d}t$$

where t is an arbitrary integer. Taking $t = 0, 1, 2, \dots, d-1$, we get exactly d distinct modulo m roots

$$x_0, x_0 + \frac{m}{d}, x_0 + 2\frac{m}{d}, \dots, x_0 + (d-1)\frac{m}{d};$$

for two values of t congruent modulo d lead to two values of x congruent mod m , while the exhibited d numbers belong to different classes mod m . We conclude, therefore, that the congruence of the first degree

$$ax \equiv b \pmod{m}$$

is possible if and only if $d = (a, m)$ divides b , and in this case it has exactly d distinct solutions mod m .

3. Methods for Solving Congruences of the First Degree.

A congruence of the first degree is equivalent to the indeterminate equation

$$ax - my = b.$$

The method of solving such equations was explained in Secs. 5 and 6, Chap. III. The reduction of the congruence to the indeterminate equation affords in practice the most expeditious method of solution, especially if a and m are large numbers. There are two other methods, however, based on entirely different principles. We can suppose that a and m are relatively prime numbers, and also we can take $b = 1$. For, if x_0 is a solution of the congruence

$$ax_0 \equiv 1 \pmod{m},$$

then bx_0 or any residue of it will be a solution of the congruence

$$ax \equiv b \pmod{m}.$$

Now, since a and m are relatively prime, by Euler's theorem

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

or

$$aa^{\varphi(m)-1} \equiv 1 \pmod{m},$$

so that

$$a^{\varphi(m)-1}$$

or any residue of this number can be taken for x_0 .

Example. Solve the congruence

$$35x \equiv 14 \pmod{182}.$$

First we ascertain whether this congruence is possible. To this end we find $d = (35, 182) = 7$ and, since 14 is divisible by 7, the congruence has seven solutions. To find them, we must solve the congruence

$$5x \equiv 2 \pmod{26}.$$

One root of the congruence is

$$2 \cdot 5^{e(26)-1} = 2 \cdot 5^{11}$$

or any of its residues mod 26. Now

$$11 = 8 + 2 + 1$$

and

$$5^1 \equiv 5, \quad 5^2 \equiv -1, \quad 5^4 \equiv 1, \quad 5^8 \equiv 1 \pmod{26};$$

$$5^{11} \equiv 5 \cdot -1 \cdot 1 \equiv -5 \pmod{26}$$

$$2 \cdot 5^{11} \equiv -10 \pmod{26},$$

so that one root of the congruence

$$5x \equiv 2 \pmod{26}$$

is $x_0 = -10$. Consequently the seven roots of the congruence

$$35x \equiv 14 \pmod{182}$$

are

$$-10, 16, 42, 68, -88, -62, -36,$$

or, if we prefer positive numbers,

$$172, 16, 42, 68, 94, 120, 146.$$

The second of the two above-mentioned methods is based upon the following considerations. Numbers $a, 2a, 3a, \dots, (m-1)a$ when divided by m leave quotients q_1, q_2, \dots, q_{m-1} and remainders r_1, r_2, \dots, r_{m-1} which, save for order, coincide with $1, 2, \dots, m-1$. Thus for $i = 1, 2, \dots, m-1$ we have

$$ia = mq_i + r_i$$

and, squaring both sides,

$$i^2 a^2 = r_i^2 + 2mq_i r_i + q_i^2 m^2$$

or

$$i^2 a^2 \equiv r_i^2 + 2mq_i r_i \pmod{m^2}.$$

On the other hand,

$$\begin{aligned} r_i q_i &\equiv i a q_i \pmod{m} \\ m r_i q_i &\equiv m i a q_i \pmod{m^2}, \end{aligned}$$

and so

$$i^2 a^2 \equiv r_i^2 + 2m a i q_i \pmod{m^2}.$$

Summing these congruences for $i = 1, 2, \dots, m-1$ and remembering that r_1, r_2, \dots, r_{m-1} coincide in their totality with $1, 2, \dots, m-1$, we get

$$\frac{m(m-1)(2m-1)}{6} a^2 \equiv \frac{m(m-1)(2m-1)}{6} + 2ma \sum_{i=1}^{m-1} i q_i \pmod{m^2},$$

whence

$$m(m-1)(2m-1)a^2 \equiv m(m-1)(2m-1) + 12ma \sum_{i=1}^{m-1} i q_i \pmod{m^2},$$

or, dividing both sides and the modulus by m ,

$$(m-1)(2m-1)a^2 \equiv (m-1)(2m-1) + 12a \sum_{i=1}^{m-1} i q_i \pmod{m},$$

or else

$$a \left(a - 12 \sum_{i=1}^{m-1} i q_i \right) \equiv 1 \pmod{m}.$$

This shows that

$$x \equiv a - 12 \sum_{i=1}^{m-1} iq_i \pmod{m}$$

satisfies the congruence

$$ax \equiv 1 \pmod{m}.$$

Since

$$q_i = \left[\frac{ia}{m} \right],$$

we have a more explicit expression for x

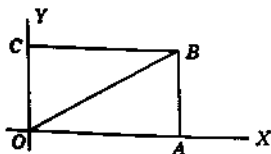
$$x \equiv a - 12 \sum_{i=1}^{m-1} i \left[\frac{ia}{m} \right] \pmod{m}.$$

The sum on the right-hand side can be transformed into a far more convenient expression, as we shall show in the next section. www.dbraultlibrary.org.in

4. Continuation. The simplest way to transform the sum

$$\sum_{i=1}^{m-1} i \left[\frac{ai}{m} \right]$$

is based on geometrical considerations. Consider the rectangle $OACB$ with $OA = m$, $OC = a$, and take its horizontal and vertical sides for coordinate axes as shown in the diagram.



Points with integral coordinates are called "lattice points." Attribute to a lattice point (i, j) the weight i and seek the

combined weight of all the lattice points in the triangle OAB excluding sides OA and AB . These lattice points are located on the lines $x = 1, x = 2, \dots, x = m - 1$. To find out how many lattice points are located on the line $x = i$, we notice that the equation of OB is

$$y = \frac{a}{m}x.$$

Consequently on $x = i$ there are as many lattice points as there are integers $1, 2, 3, \dots$ not exceeding ai/m or

$$\left[\frac{ai}{m} \right]$$

lattice points each of weight i . The weight due to all lattice points on the line $x = i$ being

$$i \left[\frac{ai}{m} \right]$$

the combined weight of all lattice points in the triangle OAB is

$$\sum_{i=1}^{m-1} i \left[\frac{ai}{m} \right].$$

Now we can compute the same weight in another manner, considering that all lattice points under consideration are located on the lines $y = 1, 2, \dots, a - 1$ to the right of OB . On $y = h$, including OC but excluding AB , there are m lattice points of weights

$$0, 1, 2, \dots, m - 1.$$

On $y = h$, including OC but to the left of OB , there are

$$\left[\frac{mh}{a} \right] + 1$$

lattice points of weights

$$0, 1, 2, \dots, \left[\frac{mh}{a} \right].$$

Consequently, the sum of weights of the lattice points on $y = h$ within OAB is

$$0 + 1 + 2 + \dots + (m-1) - \left(0 + 1 + 2 + \dots + \left[\frac{mh}{a} \right] \right) = \frac{m(m-1)}{2} - \frac{1}{2} \left[\frac{mh}{a} \right] \left(\left[\frac{mh}{a} \right] + 1 \right),$$

and the sum of weights of all lattice points in OAB is

$$\frac{(a-1)m(m-1)}{2} - \frac{1}{2} \sum_{h=1}^{a-1} \left[\frac{mh}{a} \right]^2 - \frac{1}{2} \sum_{h=1}^{a-1} \left[\frac{mh}{a} \right].$$

Now

$$\begin{aligned} \sum_{h=1}^{a-1} \left[\frac{mh}{a} \right] &= \sum_{h=1}^{a-1} \left[\frac{m(a-h)}{a} \right] = \sum_{h=1}^{a-1} \left[m - \frac{mh}{a} \right] \\ &= (a-1)(m-1) - \sum_{h=1}^{a-1} \left[\frac{mh}{a} \right], \end{aligned}$$

whence

$$\sum_{h=1}^{a-1} \left[\frac{mh}{a} \right] = \frac{(a-1)(m-1)}{2};$$

consequently the above expression for the weight of all lattice points in OAB simplifies to

$$\frac{(a-1)(m-1)(2m-1)}{4} - \frac{1}{2} \sum_{h=1}^{a-1} \left[\frac{mh}{a} \right]^2.$$

But another expression for the same weight is

$$\sum_{i=1}^{m-1} i \left[\frac{ai}{m} \right],$$

and thus we arrive at the desired transformation

$$\sum_{i=1}^{m-1} i \left[\frac{ai}{m} \right] = \frac{(a-1)(m-1)(2m-1)}{4} - \frac{1}{2} \sum_{h=1}^{a-1} \left[\frac{mh}{a} \right]^2.$$

Multiplying both sides by 12 and dropping multiples of m , we get

$$12 \sum_{i=1}^{m-1} i \left[\frac{ai}{m} \right] \equiv 3a - 3 - 6 \sum_{h=1}^{a-1} \left[\frac{mh}{a} \right]^2 \pmod{m}.$$

But the solution of the congruence

$$ax \equiv 1 \pmod{m}$$

as given in Sec. 3 was

$$x \equiv a - 12 \sum_{i=1}^{m-1} i \left[\frac{ai}{m} \right] \pmod{m},$$

and it can now be put into the more convenient form

$$x \equiv 3 - 2a + 6 \sum_{h=1}^{a-1} \left[\frac{mh}{a} \right]^2 \pmod{m}.$$

For small values of a , even if m is large, this congruence can be conveniently used for solving congruences of the first degree.

Example. Solve the congruence

$$5x \equiv 1 \pmod{69}.$$

Here we have $a = 5$, $m = 69$; correspondingly

$$\left[\frac{mh}{a} \right] \equiv 13, 27, 41, 55 \pmod{69}$$

$$\left[\frac{mh}{a} \right]^2 \equiv 31, 39, 25, -11 \pmod{69}$$

and

$$\sum_{h=1}^{a-1} \left[\frac{mh}{a} \right]^2 \equiv 15 \pmod{69},$$

whence

$$x \equiv 3 - 10 + 90 \equiv 14 \pmod{69}.$$

This interesting solution is taken from a little-known paper by Voronoi, to which we shall have occasion to refer later.

G. Voronoi (1866-1908), a very prominent Russian mathematician, published but few papers, but all were of fundamental importance. They deal with the generalization of continued fractions, asymptotic evaluation of arithmetical functions, and the reduction theory of quadratic forms in several variables.

Exercises and Problems

1. Solve the congruence $513x \equiv -17 \pmod{1,163}$.

$$\text{Ans. } x \equiv 968 \pmod{1,163}.$$

2. Solve the congruence $66x \equiv 121 \pmod{737}$.

$$\text{Ans. } x \equiv 13, 80, 147, 214, 281, 348, 415, 482, 549, 616, 683 \pmod{737}.$$

3. Solve the congruence $(n+1)^2x \equiv 1 \pmod{(2n+1)^3}$.

$$\text{Ans. } x \equiv 4 - 4(2n+1)(2n+3) + 4(2n+1)^2(2n+3)^2 \pmod{(2n+1)^3}.$$

4. An ancient problem, still enjoying wide popularity, requires one to divide equally wine contained in an 8-gal. vessel by means of two empty vessels of 5 and 3 gal. capacity. It can be generalized as follows. Of three vessels A , B , C , whose capacities are $a > b > c$, the first is full of wine and the two others are empty. Supposing that b and c are relatively prime numbers and a even, divide the wine into equal parts, using vessels A , B , C and no other measure. Show that the problem always can be solved if $a \leq 2b + 2c$ and $a \geq b + c - 2$.

5. **An Important System of Congruences.** Very often it is necessary to find integers which belong to preassigned classes

This necessary condition is at the same time sufficient. To prove this, we shall use the method of induction. Consider first two congruences

$$x \equiv \alpha \pmod{a}, \quad x \equiv \beta \pmod{b}.$$

The first is satisfied by

$$x = \alpha + at,$$

and the second will be satisfied if the integer t is so chosen that

$$at \equiv \beta - \alpha \pmod{b}.$$

Since, by hypothesis, $\beta - \alpha$ is divisible by (a, b) , this congruence is possible and the statement is proved for two congruences. If there are three congruences

$$x \equiv \alpha \pmod{a}, \quad x \equiv \beta \pmod{b}, \quad x \equiv \gamma \pmod{c},$$

the first two can be satisfied in the most general way by

$$x = x_0 + vt,$$

where x_0 is a particular solution and v denotes the l.c.m. of a and b . To satisfy the third congruence, t must satisfy the congruence

$$vt \equiv \gamma - x_0 \pmod{c},$$

and we must show that this is possible; that is, that the g.c.d. of v and c divides $\gamma - x_0$. To this end let

$$a = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \cdots p_s^{\alpha_s}$$

$$b = p_1^{\beta_1} p_2^{\beta_2} p_3^{\beta_3} \cdots p_s^{\beta_s}$$

$$c = p_1^{\gamma_1} p_2^{\gamma_2} p_3^{\gamma_3} \cdots p_s^{\gamma_s}$$

be prime factorizations of a , b , c . Let ω_1 be the greater of the numbers α_1, β_1 ; ω_2 the greater of the numbers α_2, β_2 ; and so on. Then

$$v = p_1^{\omega_1} p_2^{\omega_2} \cdots p_s^{\omega_s}$$

and

$$(v, c) = p_1^{\tau_1} p_2^{\tau_2} \cdots p_s^{\tau_s}$$

if τ_1 is the smaller of the two numbers ω_1, γ_1 ; τ_2 the smaller of the two numbers ω_2, γ_2 ; and so on. It suffices to show that $\gamma - x_0$ is divisible by $p_1^{\tau_1}, p_2^{\tau_2}, \dots, p_s^{\tau_s}$ separately. To prove this we notice that one at least of the congruences

$$\alpha - x_0 \equiv 0 \pmod{p_1^{\omega_1}}, \quad \beta - x_0 \equiv 0 \pmod{p_1^{\omega_1}}$$

is true. Let it be the second one and $\beta_1 = \omega_1$. On the other hand (b, c) is divisible exactly by $p_1^{\tau_1}$, and by hypothesis

$$\beta - \gamma \equiv 0 \pmod{(b, c)}.$$

Even more

$$\beta - \gamma \equiv 0 \pmod{p_1^{\tau_1}}$$

and, since

$$\beta - x_0 \equiv 0 \pmod{p_1^{\beta_1}}$$

and $\omega_1 \geq \tau_1$, we shall have

$$\gamma - x_0 \equiv 0 \pmod{p_1^{\tau_1}}.$$

In the same way we prove that $\gamma - x_0$ is divisible by $p_2^{\tau_2}, p_3^{\tau_3}, \dots$. Thus the statement is proved in the case of three congruences.

Supposing now as being proved that the conditions

$$\begin{array}{lll} \alpha - \beta \equiv 0 \pmod{(a, b)}, & \dots, & \alpha - \kappa \equiv 0 \pmod{(a, k)} \\ \beta - \gamma \equiv 0 \pmod{(b, c)}, & \dots, & \beta - \kappa \equiv 0 \pmod{(b, k)} \\ \dots & \dots & \dots \\ & & \iota - \kappa \equiv 0 \pmod{(i, k)}, \end{array}$$

are sufficient for the solvability of n congruences

$$\begin{array}{llll} x \equiv \alpha \pmod{a}, & x \equiv \beta \pmod{b}, & \dots, & \\ & x \equiv \iota \pmod{i}, & x \equiv \kappa \pmod{k}, & \end{array}$$

we shall prove that the additional conditions

$$\alpha - \lambda \equiv 0 \pmod{(a, l)}, \quad \beta - \lambda \equiv 0 \pmod{(b, l)}, \quad \dots, \\ \kappa - \lambda \equiv 0 \pmod{(k, l)}$$

assure the possibility of $n + 1$ congruences

$$x \equiv \alpha \pmod{a}, \quad x \equiv \beta \pmod{b}, \quad \dots, \quad x \equiv \lambda \pmod{l}.$$

The most general solution of n congruences is

$$x = x_0 + \nu t,$$

where x_0 is some particular solution and ν the l.c.m. of a, b, c, \dots, k . It suffices to show that the congruence

$$\nu t \equiv \lambda - x_0 \pmod{l}$$

is solvable. To this end let the prime p_1 enter in a, b, \dots, k, l in powers $p_1^{\alpha_1}, p_1^{\beta_1}, \dots, p_1^{\kappa_1}, p_1^{\lambda_1}$ and let ω_1 be the greatest of the exponents $\alpha_1, \beta_1, \dots, \kappa_1$, and τ_1 the smaller of the two numbers λ_1 and ω_1 . Then ν contains p_1 in the power $p_1^{\omega_1}$ and (ν, l) contains p_1 in the power $p_1^{\tau_1}$. Of the congruences

$$\alpha - x_0 \equiv 0 \pmod{p_1^{\omega_1}}, \quad \beta - x_0 \equiv 0 \pmod{p_1^{\omega_1}}, \\ \dots, \quad \kappa - x_0 \equiv 0 \pmod{p_1^{\omega_1}}$$

at least one is true. Let it be the second, and $\beta_1 = \omega_1$. (On the other hand, by the hypothesis

$$\beta - \lambda \equiv 0 \pmod{p_1^{\tau_1}},$$

which combined with

$$\beta - x_0 \equiv 0 \pmod{p_1^{\omega_1}},$$

because $\tau_1 \leq \omega_1$, leads to

$$\lambda - x_0 \equiv 0 \pmod{p_1^{\tau_1}},$$

and this suffices to show that $\lambda - x_0$ is divisible by the g.c.d. of l and ν . The congruence

$$\nu t \equiv \lambda - x_0 \pmod{l}$$

being possible, the proof of the statement is achieved, while the nature of the proof at the same time indicates a method for solving simultaneous congruences.

Example. Solve the congruences

$$x \equiv 4 \pmod{24}, \quad x \equiv 4 \pmod{36}, \quad x \equiv 52 \pmod{56}.$$

We have $(24, 36) = 12$; $(24, 56) = 8$; $(36, 56) = 4$, and since these numbers divide, respectively,

$$4 - 4 = 0; \quad 52 - 4 = 48; \quad 52 - 4 = 48,$$

the proposed system is solvable. To satisfy the first two congruences, we seek t from

$$24t \equiv 0 \pmod{36} \quad \text{or} \quad 2t \equiv 0 \pmod{3}.$$

Take $t = 0$, and then $x_1 = 4$ satisfies the first two congruences. To satisfy the third, we seek t from

$$4 + 72t \equiv 52 \pmod{56}$$

or

$$9t \equiv 6 \pmod{7},$$

and we can take $t = 3$. Then $4 + 72 \cdot 3 = 220$ satisfies all three congruences, and the most general solution will be

$$x \equiv 220 \pmod{504}.$$

6. Case of Moduli Relatively Prime in Pairs. If the moduli a, b, c, \dots, l are relatively prime in pairs, the system of simultaneous congruences

$$x \equiv \alpha \pmod{a}, \quad x \equiv \beta \pmod{b}, \quad \dots, \quad x \equiv \lambda \pmod{l}$$

is always solvable. This follows immediately from the general criterion of Sec. 5, but can also be established independently by actually exhibiting the solution in a very convenient form. Let us first consider the special case

$$x \equiv 1 \pmod{a}, \quad x \equiv 0 \pmod{b}, \quad x \equiv 0 \pmod{c}, \\ \dots, \quad x \equiv 0 \pmod{l}.$$

We disregard the first congruence, and the general solution of the others is

$$x \equiv bc \cdots l t = \frac{m}{a} t,$$

where $m = abc \cdots l$ and t is an arbitrary integer. To satisfy the first congruence, t must be determined by

$$\frac{m}{a} t \equiv 1 \pmod{a}.$$

Since $bc \cdots l$ is prime to a , this congruence is solvable. Let A denote some solution of it; then $x = A \frac{m}{a} \alpha$ satisfies the congruences:

$$x \equiv \alpha \pmod{a}, \quad x \equiv 0 \pmod{b}, \quad \dots, \quad x \equiv 0 \pmod{\lambda}.$$

Similarly, if B, C, \dots, L are determined by the congruences $\frac{m}{b} B \equiv 1 \pmod{b}, \frac{m}{c} C \equiv 1 \pmod{c}, \dots, \frac{m}{l} L \equiv 1 \pmod{l}$, the numbers

$$B \frac{m}{b} \beta, \quad C \frac{m}{c} \gamma, \quad \dots, \quad L \frac{m}{l} \lambda$$

will satisfy the systems of congruences

$$\begin{array}{lll} x \equiv 0 \pmod{a}, & x \equiv \beta \pmod{b}, & x \equiv 0 \pmod{c}, \\ & \dots, & x \equiv 0 \pmod{l} \\ x \equiv 0 \pmod{a}, & x \equiv 0 \pmod{b}, & x \equiv \gamma \pmod{c}, \\ & \dots, & x \equiv 0 \pmod{l} \\ \dots & \dots & \dots \\ x \equiv 0 \pmod{a}, & x \equiv 0 \pmod{b}, & x \equiv 0 \pmod{c}, \\ & \dots, & x \equiv \lambda \pmod{l}. \end{array}$$

It is clear, then, that

$$A \frac{m}{a} \alpha + B \frac{m}{b} \beta + \dots + L \frac{m}{l} \lambda$$

satisfies all the congruences

$$x \equiv \alpha \pmod{a}, x \equiv \beta \pmod{b}, \dots, x \equiv \lambda \pmod{l}$$

and the most general solution is

$$x \equiv A \frac{m}{a} \alpha + B \frac{m}{b} \beta + \dots + L \frac{m}{l} \lambda \pmod{abc \dots l}.$$

This method of solution is especially convenient when we have to solve several systems of congruences for various $\alpha, \beta, \dots, \lambda$ because A, B, C, \dots, L are determined once and for all. It seems that some similar method was known to the ancient Chinese; hence the method of this section is often called "Chinese method."

Example Solve the system of congruences

$$x \equiv 1 \pmod{2}, x \equiv 3 \pmod{5}, x \equiv 4 \pmod{7}, x \equiv 6 \pmod{11}.$$

To determine A, B, C, D we have to solve the congruences

$$\begin{aligned} 35 \cdot 11A &\equiv 1 \pmod{2}, & 14 \cdot 11B &\equiv 1 \pmod{5}, \\ 19 \cdot 11C &\equiv 1 \pmod{7}, & 10 \cdot 7D &\equiv 1 \pmod{11} \end{aligned}$$

or

$$\begin{aligned} A &\equiv 1 \pmod{2}, & B &\equiv -1 \pmod{5}, & 5C &\equiv 1 \pmod{7}, \\ & & 4D &\equiv 1 \pmod{11}. \end{aligned}$$

We can take $A = 1, B = -1, C = 3, D = 3$; then

$$x \equiv 385 - 462 + 1320 + 1260 \equiv 2503 \equiv 193 \pmod{770}.$$

Exercises

1. Solve the simultaneous congruences

(a) $x \equiv 3 \pmod{4}, x \equiv 6 \pmod{15}, x \equiv 7 \pmod{36}, x \equiv 70 \pmod{48}$;

(b) $x \equiv 2 \pmod{4}, x \equiv 6 \pmod{15}, x \equiv 30 \pmod{36}, x \equiv 42 \pmod{48}$.

Ans. (a) Impossible system; (b) $x \equiv 426 \pmod{720}$.

2. Solve the simultaneous congruences

$$x \equiv 1 \pmod{7}, \quad x \equiv 6 \pmod{22}, \quad x \equiv 11 \pmod{13}$$

by the Chinese method.

Ans. $x \equiv 50 \pmod{2,002}$.

7. Congruences of Higher Degree: Composite Moduli.

Let m be a composite number factored into factors a, b, c, \dots, l relatively prime in pairs and

$$f(x) \equiv 0 \pmod{m} \quad (A)$$

a congruence modulo m . This congruence is equivalent to the system of simultaneous congruences

$$f(x) \equiv 0 \pmod{a}, f(x) \equiv 0 \pmod{b}, \dots, f(x) \equiv 0 \pmod{l}$$

which we shall call (B). Consequently any root of the proposed congruence mod m must be congruent to some root α of

$$f(x) \equiv 0 \pmod{a},$$

mod a , to some root β of

$$f(x) \equiv 0 \pmod{b},$$

mod b , and so on. Conversely, designating by $\alpha, \beta, \dots, \lambda$ arbitrarily chosen roots of the congruences (B) and determining x by the simultaneous congruences

$$x \equiv \alpha \pmod{a}, x \equiv \beta \pmod{b}, \dots, x \equiv \lambda \pmod{l} \quad (C)$$

x will be a root of the congruence (A). Thus, to have all roots of (A), it suffices to attribute to $\alpha, \beta, \dots, \lambda$ all possible values and for each chosen system $\alpha, \beta, \dots, \lambda$ solve for x the congruences (C); all roots of (A) thus obtained will be distinct mod $abc \cdots l = m$. Hence, if $N(m)$ denotes the number of distinct roots of (A) and similar notation is used for the other congruences, then

$$N(m) = N(a)N(b) \cdots N(l).$$

Example. Find all the roots of the congruence

$$x^2 + 19x^2 - x + 23 \equiv 0 \pmod{42}.$$

The congruence

$$x^3 + 19x^2 - x + 23 \equiv 0 \pmod{2}$$

has one root, $\alpha = 1$. Congruence

$$x^3 + 19x^2 - x + 23 \equiv 0 \pmod{3}$$

has two roots, $\beta = \pm 1$. Congruence

$$x^3 + 19x^2 - x + 23 \equiv 0 \pmod{7}$$

has three roots, $\gamma = \pm 1, 2$. Consequently the proposed congruence has six distinct roots. To find them we must solve the simultaneous congruences

$$x \equiv \alpha \pmod{2}, \quad x \equiv \beta \pmod{3}, \quad x \equiv \gamma \pmod{7}$$

for six systems α, β, γ :

α	β	γ
1	1	1
1	1	-1
1	1	2
1	-1	1
1	-1	-1
1	-1	2

By the Chinese method we find

$$x \equiv 21\alpha - 14\beta - 6\gamma \pmod{42},$$

whence the six roots of the proposed congruence are

$$\begin{aligned} x &\equiv 21 - 14 - 6 \equiv 1 \pmod{42} \\ x &\equiv 21 - 14 + 6 \equiv 13 \pmod{42} \\ x &\equiv 21 - 14 - 12 \equiv 37 \pmod{42} \\ x &\equiv 21 + 14 - 6 \equiv 29 \pmod{42} \\ x &\equiv 21 + 14 + 6 \equiv 41 \pmod{42} \\ x &\equiv 21 + 14 - 12 \equiv 23 \pmod{42}. \end{aligned}$$

8. Congruences of Higher Degree: Moduli Powers of Primes. By the preceding section, solution of congruences for composite moduli depends on the solution of similar congruences for moduli which are powers of primes. Let

$$f(x) \equiv 0 \pmod{p^a} \tag{A}$$

be a congruence whose modulus is a power of a prime p . Every root of this congruence modulo p^{a-1} is congruent to some root β of the congruence

$$f(x) \equiv 0 \pmod{p^{a-1}}, \quad (B)$$

which root is in turn congruent modulo p to some root α of the congruence

$$f(x) \equiv 0 \pmod{p} \quad (C)$$

with a prime modulus p . To find all roots of (A) congruent to $\beta \pmod{p^{a-1}}$ we seek them in the form

$$x = p^{a-1}t + \beta.$$

By Taylor's theorem

$$f(\beta + p^{a-1}t) = f(\beta) + p^{a-1}tf'(\beta) + p^{2a-2}t^2 \frac{f''(\beta)}{1 \cdot 2} + \dots$$

In this expansion all terms beginning with the third are divisible by p^a , for already $2a-2 \geq a$ if $a > 1$ and

$$\frac{f''(\beta)}{1 \cdot 2}, \quad \frac{f'''(\beta)}{1 \cdot 2 \cdot 3}, \quad \dots$$

clearly are integers. Hence

$$f(\beta + p^{a-1}t) \equiv f(\beta) + p^{a-1}tf'(\beta) \pmod{p^a},$$

and thus t must be determined from the congruence

$$f(\beta) + p^{a-1}tf'(\beta) \equiv 0 \pmod{p^a},$$

which is equivalent to

$$tf'(\beta) + \frac{f(\beta)}{p^{a-1}} \equiv 0 \pmod{p}$$

or

$$tf'(\alpha) + \frac{f(\beta)}{p^{a-1}} \equiv 0 \pmod{p}, \quad (D)$$

since $f'(\beta) \equiv f'(\alpha) \pmod{p}$.

Now we must distinguish two cases: (1) $f'(\alpha)$ nondivisible by p , and (2) $f'(\alpha)$ divisible by p . In the first case congruence (D) has a unique solution mod p ; in the second case it is either impossible or has p solutions. Consequently, to each root of the congruence (B) corresponds either one root of (A), or p roots, or none.

The procedure for solving (A), according to these explanations, consists in the following steps. First, congruence (C) with prime modulus must be solved. Then we seek roots of the congruence

$$f(x) \equiv 0 \pmod{p^2} \quad (E)$$

corresponding to each root of (C). After that we seek roots of

$$f(x) \equiv 0 \pmod{p^3}$$

corresponding to all roots of (E), and so on. By this process to each root α of (C) will correspond a unique root of (A) if $f'(\alpha)$ is not divisible by p . In the contrary case, (A) has either no roots corresponding to α or several of them.

NOTE: It can be shown that the congruences $f(\alpha) \equiv 0$, $f'(\alpha) \equiv 0 \pmod{p}$ can hold only for primes dividing the discriminant of the equation $f(x) = 0$. The number of such primes is therefore limited, provided $f(x) = 0$ has no multiple root.

Example 1. Solve the congruence

$$x^2 - 2x + 2 \equiv 0 \pmod{27}.$$

Modulo 3 this congruence has the unique solution -1 . We have $f(-1) = 3$, $f'(-1) = 1$. The congruence

$$t + 1 \equiv 0 \pmod{3}$$

has a unique solution mod 3, and we can take $t = -1$. Then $x = -3 - 1 = -4$ is the only root of the congruence

$$x^2 - 2x + 2 \equiv 0 \pmod{9}.$$

Again, $f(-4) = -54$, $f'(-4) \equiv f'(-1) \equiv 1 \pmod{3}$, and we have to seek t from the congruence

$$t - 6 \equiv 0 \pmod{3},$$

whence $t \equiv 0 \pmod{3}$, and we can take $t = 0$. Thus $x \equiv -4 \pmod{27}$ is the only root of the proposed congruence.

Example 2. Solve the congruence

$$x^3 - 2x + 6 \equiv 0 \pmod{125}.$$

Modulo 5 this congruence has two solutions, 1 and 2. If we take first $\alpha = 1$, then $f(1) = 5$, $f'(1) = 1$. The auxiliary congruence

$$t + 1 \equiv 0 \pmod{5}$$

has one root only, and we can take $t = -1$. Then $x = 1 - 5 \cdot 1 = -4$ is the unique root of

$$x^3 - 2x + 6 \equiv 0 \pmod{25}$$

congruent 1 mod 5. Again $f(-4) = -50$, $f'(-4) = 46 \equiv 1 \pmod{5}$. The auxiliary congruence to determine t is

$$t - 2 \equiv 0 \pmod{5}.$$

Taking $t = 2$, then $x = 25 \cdot 2 - 4 = 46$ is the only root of the proposed congruence congruent 1 mod 5. Now we start with $\alpha = 2$; then $f(2) = 10$, $f'(2) = 10$. The auxiliary congruence

$$10t + 2 \equiv 0 \pmod{5}$$

is impossible. Hence

$$x^3 - 2x + 6 \equiv 0 \pmod{25}$$

has no roots congruent 2 mod 5; thus the proposed congruence has no solution $\equiv 2 \pmod{5}$. It follows that there is a unique root, $x \equiv 46 \pmod{125}$.

Exercises and Problems

- Find all distinct solutions of the congruence $x^2 \equiv 46 \pmod{105}$.
Ans. $x \equiv \pm 61, \pm 26, \pm 19, \pm 16$.
- Find all distinct solutions of the congruence $x^6 - 11x^4 + 36x^2 - 36 \equiv 0 \pmod{135}$.
Ans. Impossible.
- Solve the congruence $x^3 - 3x + 27 \equiv 0 \pmod{1125}$.
Ans. $x \equiv 648, 273, -102 \pmod{1125}$.
- How many solutions has the congruence $x^2 \equiv 1 \pmod{m}$? *Ans.* Let $\sigma = 1$ or 2, according as m is divisible only by 4 or by 8; in all other

cases $\sigma = 0$. Also let ν be the number of distinct odd prime factors of m . The requested number is $2^{\sigma+\nu}$.

5. Prove the following generalization of Wilson's theorem: The product of positive integers relatively prime to m and less than m is $\equiv -1 \pmod{m}$ if m is 2, 4, power of an odd prime, or the double of such a power; in all other cases it is $\equiv 1 \pmod{m}$.

9. Congruences with a Prime Modulus: Lagrange's Theorem. As we have seen, the solution of congruences in the last instance depends on that of congruences with prime moduli. Congruences with prime moduli possess many remarkable properties and, on that account, deserve special consideration. Here we shall consider only one of these properties, expressed in a very simple and yet important theorem discovered by Lagrange in 1768. Consider a congruence for the prime modulus p

$$f(x) = p_0x^n + p_1x^{n-1} + \dots + p_n \equiv 0 \pmod{p}$$

and suppose that p_0 is not divisible by p , so that the congruence is of degree n . Lagrange's theorem states that it cannot have more than n distinct roots.

This property is certainly true for congruences of the first degree which have exactly one root. Supposing now that congruences of degree $n - 1$ with prime modulus do not have more roots than their degree, we shall prove that the same holds for congruences of degree n , and that will be sufficient to convince ourselves of the truth of Lagrange's theorem in general.

Let a be a root of

$$f(x) \equiv 0 \pmod{p}$$

so that $f(a)$ is divisible by p . The difference $f(x) - f(a)$ is divisible algebraically by $x - a$, and the quotient is a polynomial of degree $n - 1$ with integer coefficients the first of which is p_0 . Thus, we have identically,

$$f(x) = (x - a)f_1(x) + f(a).$$

Now let b be any other root of

$$f(x) \equiv 0 \pmod{p}$$

different from a . Then, by the preceding identity,

$$f(b) = (b - a)f_1(b) + f(a),$$

and, since $f(a)$ and $f(b)$ are both divisible by p ,

$$(b - a)f_1(b) \equiv 0 \pmod{p}$$

or

$$f_1(b) \equiv 0 \pmod{p},$$

because $b - a$ is not divisible by p . Thus, if the congruence

$$f(x) \equiv 0 \pmod{p}$$

had, besides a , at least n other roots, all these roots would be roots of

$$f_1(x) \equiv 0 \pmod{p},$$

which is impossible, because by hypothesis this congruence of degree $n - 1$ cannot have more than $n - 1$ roots.

As a corollary to Lagrange's theorem we have the following proposition:

If the congruence

$$p_0x^n + p_1x^{n-1} + \dots + p_n \equiv 0 \pmod{p}$$

is satisfied by more than n integers distinct modulo p , then necessarily all the coefficients p_0, p_1, \dots, p_n are divisible by p . For suppose that p_i is the first of the coefficients p_0, p_1, \dots, p_n nondivisible by p ; then the congruence

$$p_i x^{n-i} + \dots + p_n \equiv 0 \pmod{p}$$

of degree $n - i$ would have more than n roots, which is impossible by Lagrange's theorem.

10. Some Applications of Lagrange's Theorem. Consider the polynomial

$$f(x) = x^{p-1} - 1 - (x-1)(x-2) \cdots (x-p+1)$$

of degree $p-2$. By Fermat's theorem

$$x^{p-1} - 1 \equiv 0 \pmod{p}$$

for $x = 1, 2, \dots, p-1$. Also the product

$$(x-1)(x-2) \cdots (x-p+1)$$

vanishes for the same values of x . Consequently the congruence

$$f(x) \equiv 0 \pmod{p}$$

is satisfied by $p-1$ values of x distinct modulo p , and this can be only if all the coefficients of $f(x)$ are divisible by p , so that

$$f(x) = p\varphi(x)$$

where $\varphi(x)$ is a polynomial with integer coefficients. Thus, identically in x

$$x^{p-1} - 1 = (x-1)(x-2) \cdots (x-p+1) + p\varphi(x).$$

Taking here $x = p$, we get

$$p^{p-1} - 1 = 1 \cdot 2 \cdot 3 \cdots (p-1) + p\varphi(p);$$

that is,

$$1 \cdot 2 \cdot 3 \cdots (p-1) \equiv -1 \pmod{p}.$$

Thus we have another proof of Wilson's theorem.

For another application let a be an arbitrary integer non-divisible by p . Then, since

$$0, a, 2a, \dots, (p-1)a$$

is a complete system of residues mod p , we have

$$S_n(p) = 0^n + 1^n + \cdots + (p-1)^n \equiv a^n S_n(p) \pmod{p}$$

or

$$(a^n - 1)S_n(p) \equiv 0 \pmod{p}.$$

If n is not divisible by $p - 1$ and, when divided by $p - 1$, leaves the remainder $r < p - 1$, then by Fermat's theorem

$$a^n \equiv a^r \pmod{p},$$

and so

$$(a^r - 1)S_n(p) \equiv 0 \pmod{p}.$$

The congruence

$$x^r - 1 \equiv 0 \pmod{p}$$

has not more than $r < p - 1$ roots, whence it follows that among the numbers $1, 2, \dots, p - 1$ there is at least one number a for which $a^r - 1$ is not divisible by p , but then

$$S_n(p) \equiv 0 \pmod{p},$$

provided n is not divisible by $p - 1$. This result has been proved already in Sec. 11, Chap. VI, but by a less simple and general method.

11. Condition for a Congruence to Have Number of Roots Equal to Its Degree. Every congruence

$$p_0x^n + p_1x^{n-1} + \dots + p_n \equiv 0 \pmod{p}$$

of degree n for the prime modulus p can be reduced to the form

$$x^n + r_1x^{n-1} + \dots + r_n \equiv 0 \pmod{p}.$$

To do this, determine m by the condition

$$p_0m \equiv 1 \pmod{p}$$

and multiply both sides of the proposed congruence by m . The resulting congruence

$$p_0mx^n + p_1mx^{n-1} + \dots + mp_n \equiv 0 \pmod{p}$$

is equivalent to the congruence of the requested form. Every congruence

$$f(x) = x^n + r_1x^{n-1} + \dots + r_n \equiv 0 \pmod{p}$$

can be replaced by an equivalent congruence of degree $< p$. Divide $f(x)$ by $x^p - x$ and call the quotient and the remainder, respectively, $\varphi(x)$ and $F(x)$. Then from the identity

$$f(x) = (x^p - x)\varphi(x) + F(x)$$

and Fermat's theorem it follows that every root of $f(x) \equiv 0 \pmod{p}$ is a root of $F(x) \equiv 0 \pmod{p}$, and vice versa; but the last congruence is of degree $< p$ if not all of its coefficients are divisible by p , in which case it is satisfied by all integers.

Now let the degree of the congruence

$$f(x) = x^n + r_1x^{n-1} + \dots + r_n \equiv 0 \pmod{p}$$

be $< p$. Divide $x^p - x$ by $f(x)$ and call the quotient $f_1(x)$ and the remainder $r(x)$, so that

$$x^p - x = f(x)f_1(x) + r(x).$$

If $f(x) \equiv 0 \pmod{p}$ has exactly n roots, then the congruence $r(x) \equiv 0 \pmod{p}$ will be satisfied by n integers distinct mod p . As the degree of $r(x)$ is $n - 1$ or less, this can be only if all the coefficients of $r(x)$ are divisible by p , so that

$$r(x) = ps(x)$$

where the coefficients of $s(x)$ are integers. Conversely, if this condition is satisfied, the congruence

$$f(x) \equiv 0 \pmod{p}$$

will have exactly n roots. Since for every integer $0, 1, 2, \dots, p - 1$ both $x^p - x$ and $r(x)$ are divisible by p , the congruence

$$f(x)f_1(x) \equiv 0 \pmod{p}$$

will have p solutions. Of these, let s numbers satisfy the congruence $f(x) \equiv 0 \pmod{p}$; then the other $p - s$ will satisfy the congruence $f_1(x) \equiv 0 \pmod{p}$ of degree $p - n$. By Lagrange's theorem

$$s \leq n$$

and

$$p - s \leq p - n;$$

that is, $s \geq n$. Both conditions on s and n can hold only when $s = n$, and so the congruence

$$f(x) \equiv 0 \pmod{p}$$

has exactly n roots.

12. An Application. A number a is called a "residue of the e th power of the prime p " if the congruence

$$x^e \equiv a \pmod{p}$$

is possible; otherwise a is called a "nonresidue of the e th power." For $e = 2, 3, 4$ we can thus speak of quadratic, cubic, biquadratic residues or nonresidues. The number $a \equiv 0 \pmod{p}$ is a trivial residue and will be excluded from further considerations. As we shall see later, the consideration of residues of the e th power presents interest only when $p - 1$ is divisible by e . Assuming this, we may ask the question: Under what conditions is the congruence

$$x^e \equiv a \pmod{p}$$

possible? Let $p - 1 = ef$; then we may write

$$x^{p-1} - 1 = x^{ef} - a^f + a^f - 1.$$

On the other hand

$$x^{ef} - a^f = (x^e - a)(x^{e(f-1)} + ax^{e(f-2)} + \dots + a^{f-1})$$

and

$$x^p - x = (x^e - a)Q(x) + (a^f - 1)x, \quad (A)$$

where

$$Q(x) = x(x^{e(f-1)} + ax^{e(f-2)} + \dots + a^{f-1}).$$

Now if there is a number α such that $\alpha^e - a \equiv 0 \pmod{p}$, then from (A) and Fermat's theorem it follows that

$$\alpha^f \equiv 1 \pmod{p}.$$

Conversely, if this condition is fulfilled, by the criterion of the preceding section the congruence

$$x^e - a \equiv 0 \pmod{p}$$

will have exactly e solutions. Thus we reach the conclusion: a , nondivisible by p , is a residue of the e th power if and only if

$$a^{\frac{p-1}{e}} \equiv 1 \pmod{p}.$$

This condition being fulfilled, the congruence

$$x^e \equiv a \pmod{p}$$

has exactly e solutions.

If p is an odd prime and a is nondivisible by p , then, by Fermat's theorem,

$$a^{p-1} - 1 = (a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) \equiv 0 \pmod{p}.$$

Hence either

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

or

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p},$$

and both congruences cannot hold simultaneously. Consequently, a is a quadratic residue or nonresidue of p according as

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

or

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

This theorem was discovered by Euler and is known as "Euler's criterion."

The identity

$$x^p - x = x(x^{f-1} - 1)(x^{f(e-1)} + x^{f(e-2)} + \dots + 1)$$

again, by the criterion of Sec. 11, shows that the congruence

$$x^f - 1 \equiv 0 \pmod{p}$$

has exactly f solutions provided f is a divisor of $p - 1$. Hence we conclude that, for $p = ef + 1$, there are exactly $f = (p - 1)/e$ residues of the e th power among the numbers

$1, 2, 3, \dots, p - 1$, and $\frac{(e - 1)}{e}(p - 1)$ nonresidues.

Thus for an odd p there are $(p - 1)/2$ quadratic residues and $(p - 1)/2$ quadratic nonresidues among the numbers $1, 2, \dots, p - 1$. For $p = 3f + 1$ there are $(p - 1)/3$ cubic residues and $2(p - 1)/3$ cubic nonresidues in the series $1, 2, \dots, p - 1$. For $p = 4f + 1$ there are $(p - 1)/4$ biquadratic residues and $3(p - 1)/4$ biquadratic nonresidues in the series $1, 2, \dots, p - 1$.

Exercises and Problems

1. Let $S_n(x_1, x_2, \dots, x_p)$ be a homogeneous symmetric function of the indeterminates x_1, x_2, \dots, x_p of dimension n . If p is a prime and n is not divisible by $p - 1$, then $S_n(1, 2, 3, \dots, p) \equiv 0 \pmod{p}$.

2. Prove that for a prime $p \equiv 1 \pmod{4}$ the congruence $x^2 + 1 \equiv 0 \pmod{p}$ is solvable and has two distinct roots.

3. Prove that for a prime $p \equiv 1 \pmod{8}$ the congruence $x^4 + 1 \equiv 0 \pmod{p}$ is solvable and has four roots. From this result deduce that both congruences $x^2 - 2 \equiv 0$ and $x^2 + 2 \equiv 0 \pmod{p}$ are solvable.

4. Prove that for a prime $p \equiv 1 \pmod{3}$ the congruences $x^2 + x + 1 \equiv 0$ and $x^2 + 3 \equiv 0 \pmod{p}$ are solvable.

5. Let p be a prime, b some quadratic nonresidue of p , and

$$F(x) = \frac{(x + \sqrt{b})^{p+1} - (x - \sqrt{b})^{p+1}}{2\sqrt{b}}$$

a polynomial in x with integer coefficients. Show that the congruence $F(x) \equiv 0 \pmod{p}$ has p roots.

6. With the notations of the preceding problem, and denoting by e a divisor of $p + 1$, show that the congruence

$$\frac{(x + \sqrt{b})^e - (x - \sqrt{b})^e}{2\sqrt{b}} \equiv 0 \pmod{p}$$

has exactly $e - 1$ roots.

7. If $p = ef + 1$ is a prime and N denotes the number of solutions of the congruence $x^e \equiv a \pmod{p}$, then

$$N \equiv \sum_{x=0}^{p-1} (1 - (x^e - a)^{e-1}) \pmod{p}.$$

Hence, by using the properties of $S_n(p) = 1^n + 2^n + \dots + (p-1)^n$, deduce that

$$\begin{aligned} N &= e && \text{if } a^f - 1 \equiv 0 \pmod{p}; \\ N &= 0, && \text{otherwise.} \end{aligned}$$

Downloaded from www.dbraulibrary.org.in

APPENDIX

CALENDAR PROBLEMS

1. **Relation between Dates and Days of the Week.** It is familiar to everyone that, in the universally adopted Gregorian calendar, the common year consists of 365 days and each leap year of 366 days. Leap years are the years for which the number is divisible by 4, except the centurial years, which are leap years only if divisible by 400. Thus, the first centurial leap year after the reformation of the calendar, which occurred in 1582, was 1600, but 1700, 1800, 1900 were common years; the next centurial leap year will be 2000, and so on. It is easy to determine the number of leap years between 1600 exclusive and a given year N inclusive. The number of all years for which the number is divisible by 4 in the assumed interval is the same as the number of integers x such that

$$400 < x \leq \frac{N}{4};$$

that is,

$$\left[\frac{N}{4} \right] - 400.$$

From this we must exclude the number of centurial years not divisible by 400. The number of all centurial years between 1600 exclusive and N is

$$\left[\frac{N}{100} \right] - 16,$$

and among them there are

$$\left[\frac{N}{400} \right] - 4$$

divisible by 400. Consequently the number of centurial years which are not leap years is

$$\left[\frac{N}{100} \right] - \left[\frac{N}{400} \right] - 12$$

and the requested number of all leap years between 1600 exclusive and N inclusive is thus

$$T = \left[\frac{N}{4} \right] - \left[\frac{N}{100} \right] + \left[\frac{N}{400} \right] - 388.$$

This expression can be put into more convenient form by putting

$$N = 100C + D$$

where C is the number of centuries and $D < 100$. Then

$$\left[\frac{N}{4} \right] = 25C + \left[\frac{D}{4} \right]; \quad \left[\frac{N}{100} \right] = C; \quad \left[\frac{N}{400} \right] = \left[\frac{C}{4} \right]$$

and

$$T = \left[\frac{D}{4} \right] - C + \left[\frac{C}{4} \right] + 25C - 388.$$

Since in a leap year an additional day is added at the end of February, it is convenient to proceed as if the years begin in March. Then March, April, May, . . . will be counted as the first, second, third, . . . months of the year N , while January and February of the same year will be considered as the eleventh and twelfth months of the year $N - 1$. It will be also convenient to denote days of the week beginning with Sunday by 0, 1, 2, . . . , 6. Now suppose that the

first of March of the year 1600 had the number a . Since the next following year 1601 was a common year, 365 days elapsed between March 1, 1600, and March 1, 1601. But 365 days consist of 52 full weeks and 1 day; hence March 1, 1601, had the number $a + 1$ or this number diminished by 7. Again, since the years 1602 and 1603 were common years, March 1, 1602, and March 1, 1603, had the numbers $a + 2$ and $a + 3$ or these numbers diminished by a proper multiple of 7. Between March 1, 1603, and March 1, 1604, since 1604 was a leap year, 366 days or 52 weeks and 2 days elapsed; hence the number of March 1, 1604, was $a + 5$ or the least positive residue of it modulo 7.

It is clear now that every common year passed augments the number of March 1 modulo 7 by one unit and every leap year by two units. Hence, to find the number of March 1 in the year N , we have to add to a the number of all years between 1600 exclusive and N inclusive and also the number of leap years in the same interval, and to reduce the sum to its least positive residue mod 7. Thus March 1 of the year N will have the number a' determined by the congruence

$$a' \equiv a + 100C + D - 1600 + \left\lfloor \frac{D}{4} \right\rfloor - C + \left\lfloor \frac{C}{4} \right\rfloor + 25C - 388 \pmod{7}$$

or

$$a' \equiv a + D + \left\lfloor \frac{D}{4} \right\rfloor + \left\lfloor \frac{C}{4} \right\rfloor - 2C \pmod{7}.$$

For the year 1938, March 1 was on Tuesday, so $a' = 2$; again for the same year

$$D = 38, \quad C = 19; \quad D + \left\lfloor \frac{D}{4} \right\rfloor + \left\lfloor \frac{C}{4} \right\rfloor - 2C \equiv 6 \pmod{7},$$

whence

$$2 \equiv a + 6 \pmod{7}, \quad a = 3.$$

That is, March 1, 1600, was Wednesday and the preceding expression for a' becomes

$$a' \equiv 3 + D + \left[\frac{D}{4} \right] + \left[\frac{C}{4} \right] - 2C \pmod{7}.$$

This congruence determines the day of the week on which March 1 falls in every year after the Gregorian reform.

To determine the weekday corresponding to the first of all other months of the year, we notice that

Apr. 1	has a number 3 units greater than Mar. 1.
May 1	has a number 2 units greater than Apr. 1.
June 1	has a number 3 units greater than May 1.
July 1	has a number 2 units greater than June 1.
Aug. 1	has a number 3 units greater than July 1.
Sept. 1	has a number 3 units greater than Aug. 1.
Oct. 1	has a number 2 units greater than Sept. 1.
Nov. 1	has a number 3 units greater than Oct. 1.
Dec. 1	has a number 2 units greater than Nov. 1.
Jan. 1	has a number 3 units greater than Dec. 1.
Feb. 1	has a number 3 units greater than Jan. 1.

The expression

$$[2.6m - 0.2]$$

takes the same increments when m runs through the numbers 1, 2, . . . 12, from which it is easy to see that the number of the day of the week corresponding to the first of the month whose number is m is the least positive residue of the expression

$$1 + [2.6m - 0.2] + D + \left[\frac{D}{4} \right] + \left[\frac{C}{4} \right] - 2C$$

modulo 7. Finally, the number of the day of the week corresponding to the k th day of the m th month is determined by the congruence

$$f \equiv k + [2.6m - 0.2] + D + \left[\frac{D}{4} \right] + \left[\frac{C}{4} \right] - 2C \pmod{7}.$$

This useful rule was proposed by Rev. Zeller. It must not be forgotten that January and February of a given year are considered here as the eleventh and twelfth months of the preceding year.

Example 1. What day of the week was August 1, 1914? Here we have

$$C = 19, \quad D = 14; \quad D + \left[\frac{D}{4} \right] + \left[\frac{C}{4} \right] - 2C \equiv 4 \pmod{7}$$

$$m = 6; \quad [2.6 \times 6 - 0.2] \equiv 1, \quad k \equiv 1 \pmod{7}.$$

Consequently

$$f \equiv 2 + 4 \equiv 6 \pmod{7}$$

or $f = 6$. Therefore August 1, 1914, was Saturday.

Example 2. February 29, 1952, will occur on what day of the week? Here

$$C = 19, \quad D = 51; \quad D + \left[\frac{D}{4} \right] + \left[\frac{C}{4} \right] - 2C \equiv 1 \pmod{7}$$

$$m = 12; \quad [2.6 \times 12 - 0.2] \equiv 3, \quad k \equiv 1 \pmod{7}$$

$$f \equiv 5 \pmod{7}.$$

Hence February 29, 1952, will be on Friday.

Zeller's rule can be presented in a different form by introducing the remainders a and b which the number of the year $N = 100C + D$ leaves when divided by 4 and 7. For D we have the two congruences

$$D \equiv a \pmod{4}, \quad D \equiv b - 2C \pmod{7}.$$

Solving them by the Chinese method, we get the general expression for D :

$$D = 21a + 8b - 16C + 28l,$$

whence

$$\left[\frac{D}{4} \right] = 5a + 2b - 4C + 7l$$

and

$$\left[\frac{D}{4} \right] + D \equiv -2a - 4b + C \pmod{7}.$$

Zeller's congruence becomes, then,

$$f \equiv k + [2.6m - 0.2] - 2a - 4b + \left[\frac{C}{4} \right] - C \pmod{7}$$

and can be used for solving problems of the following types.

Example 3. On what days do Sundays occur in March? For Sundays $f = 0$ and for March $m = 1$, $[2.6 - 0.2] = 2$, so that

$$k \equiv 2a + 4b + C - \left[\frac{C}{4} \right] + 5 \pmod{7}.$$

Take, for example, $N = 1938$; then $a = 2$, $b = 6$, $C = 19$ and

$$k \equiv 6 \pmod{7};$$

that is, in 1938 Sundays fell on March 6, 13, 20, 27.

Example 4. In what years of the present century will November 18 fall on Sunday? In this case $C = 19$, $k = 18$, $m = 9$ and the congruence

$$a + 2b \equiv -1 \pmod{7}$$

must be satisfied. It gives

$$b \equiv 3 + 3a \pmod{7}$$

and

$$D \equiv 17a \pmod{28}.$$

Corresponding to $a = 0, 1, 2, 3$ we have

$$D = 0, 28, 56, 84$$

$$D = 17, 45, 73$$

$$D = 6, 34, 62, 90$$

$$D = 23, 51, 79.$$

The present century began in 1901, and $D = 0$ must be excluded. The following years, therefore, answer the requirement:

1906, 1917, 1923, 1928, 1934, 1945, 1951, 1956, 1962, 1973, 1979, 1984,
1990.

2. Remarks on the Church Calendar. Zeller's congruence virtually solves all problems concerning the ordinary civil calendar. But Christian churches have other calendar problems concerning the fixing of dates of movable feasts which all depend on the date of Easter. By the decision of the council of Nicea in 325 A.D., the date of Easter was fixed by the following rule: Easter must be celebrated on the Sunday immediately following the first full moon which occurs on or after March 21. Thus the problem of determining the date of Easter is complicated by the necessity of reconciling two entirely different calendars: solar and lunar. A very good adaptation of both calendars is based on a cycle discovered by Meton, a Greek who lived in the fifth century B.C. This is called the Metonic cycle, though this cycle was known to the Babylonians and Chinese long before the time of Meton. The duration of the tropical solar year is very nearly 365.2422 days, or 365 days, 5 hr., 48 min., and 46 sec., while the duration of lunation or the synodic month is very nearly 29.530588 days or 29 days, 12 hrs., 44 min., and 2.8 sec. Now the duration of 19 tropical solar years is

$$19 \cdot 365.2422 = 6,939.6018 \text{ days, or } 6,939 \text{ days, } 14 \text{ hr., } 27 \text{ min.}$$

On the other hand, the duration of 235 lunations is

$$235 \cdot 29.530588 = 6,939.6882, \text{ or } 6,939 \text{ days, } 16 \text{ hr., } 31 \text{ min.}$$

Thus 19 solar years are almost equal to 235 lunations; hence, after 19 years the same phases of the moon again fall on the same days of the year, or very nearly so.

For practical purposes of calendar reckoning true durations of solar years and lunations cannot be used. Instead, the length of the year in the Julian calendar, then used in Rome and adopted by the old church, was $365\frac{1}{4}$ days and the mean length of lunation was adjusted in accordance with the Metonic

cycle. Years beginning with the year immediately preceding our era were divided into cycles of 19 years, and each of the cycles consisted of 235 lunar months of 29 and 30 days distributed identically in all cycles, with the provision that the lunar month comprising February 29 in leap years was lengthened by one day. All these 235 lunar months were combined into 19 lunar years: 12 years of 354 days consisting of 6 months of 29 and 6 months of 30 days, 6 embolismic years of 384 days with one additional month of 30 days, and one embolismic year of 383 days, the last in the cycle, ending with a month of 29 days. Altogether the total length of 235 months in a cycle, disregarding augmentation caused by leap years, was

$$19 \cdot 354 + 6 \cdot 30 + 29 = 6,935 \text{ days.}$$

Now if leap year happens on the first, second, or third year of the cycle, there will be five leap years; there will be only four leap years if the first leap year falls on the fourth year of the cycle. In the first three cases the cycle contains 6,940 days, and in the last case only 6,939 days. The mean duration of the cycle is therefore $6,939\frac{3}{4}$ days, agreeing exactly with 19 Julian years.

A place which any year occupies in the respective cycle is called the "golden number" of the year. Thus, golden numbers of the years occupying the first, second, third, etc., places in the cycle are 1, 2, 3, Since one of the cycles began in the year 0 of our era, it is clear that the golden number of the year N is the remainder c , obtained in the division of N by 19, augmented by 1.

The epact of a year is the age of the (calendar) moon on March 1 of that year, the age being 0 for the new moon. It must be noticed that with the ancients the day of the new moon did not coincide with the astronomical new moon but was the first day on which the thin crescent became visible.

Hence the full moon followed 13 days after the new moon. Now in the first year of the cycle, according to the old church calendar, the epact is 8. Since the first lunar year of the cycle contains 354 days, which is 11 days less than 365 days, the epact of the second year will be $8 + 11 = 19$; again, the second lunar year contains 354 days, which augments the epact by 11, so that the epact of the third year will be $19 + 11 = 30$, or 0. And, in general, the months of 29 and 30 days are so arranged within the cycle that, passing from year to year, the epact is always augmented by 11; however, as soon as it becomes 30 or more it is reduced by subtracting a proper multiple of 30 to obtain a number less than 30. Hence, in the old church calendar the epact E is completely characterized by the congruence

$$E \equiv 8 + 11c \pmod{30},$$

with the same meaning of c as before. When the epact is E , the first new moon in March occurs always on the $31 - E$ day of March, and the next new moon, with the arrangement of the calendar as it is, always 30 days later.

This adaptation of both solar and lunar calendars was simple and satisfactory enough to serve for a considerable number of years to come. But at the time of the reformation of the calendar it was felt necessary to improve it in regard to both the length of the solar year and the phases of the moon, which then actually occurred four days earlier than the calendar indicated. To attain the first purpose, and to preserve at the same time the simplicity of intercalations of leap years, a very sensible arrangement was made to retain as leap years only those centurial years whose number is divisible by 400. This change necessitated the change in epacts referred to as the "solar equation." By virtue of the solar equation all epacts are diminished by 1 in century years such as 1700, 1800, 1900, etc., which are not leap years.

But there was introduced another change of epacts because of the fact that 235 lunations are not exactly equal to 19 Gregorian years. This fact causes new moons to arrive one day earlier than indicated by the Metonic cycle in about 310 years and necessitates another correction of epacts known as the "lunar equation." By virtue of the lunar equation all epacts are augmented by 1 seven times at the end of every 300 years after the year 1800, and once at the end of 400 years closing the first period of 2,500 years, after which the same process is repeated over again periodically. Thus epacts in the reformed calendar are not constant but vary from century to century.

As to the arrangement of the lunisolar reformed calendar, it would be too long to explain here in detail. Referring those who desire more information on this point to the excellent article on the calendar in the "Encyclopaedia Britannica" (all newer editions including the thirteenth, but not the fourteenth, edition), here we shall give only an excerpt of the important table known as the perpetual calendar.

Days.....	1 2 3 4 5	6 7 8 9 10	11 12 13 14 15
March.....	0 29 28 27 26	25' 25 24 23 22 21	20 19 18 17 16
April.....	25' 25 29 28 27 26 24	23 22 21 20 19	18 17 16 15 14

Days.....	16 17 18 19 20	21 22 23 24 25	26 27 28 29 30	31
March.....	15 14 13 12 11	10 9 8 7 6	5 4 3 2 1	0 Epacts
April.....	13 12 11 10 9	8 7 6 5 4	3 2 1 0 29	Epacts

This table, for each epact from 0 to 29, gives the corresponding day of the new moon in March and April. Notice that epact

25 appears in two forms: 25 and 25'. The first form corresponds to years whose golden number is ≤ 11 , and the second to those with golden numbers > 11 . Notice also that the new moon next to the first one in March, if it falls on March 1, 2, 3, 4, 5, 6, 7, follows 30 days later, with two exceptions corresponding to epacts 24 and 25', where the interval between two consecutive new moons is 29 days.

3. The Date of Easter. The preceding explanations, though brief and incomplete, are necessary to make understandable the rules proposed by Gauss for determining the date of Easter. To derive these rules, the first necessary step is to give a general formula for the Gregorian epact. As we have seen, all epacts are diminished by 1 in century years which are not leap years. In the same way the expression

$$\left[\frac{C}{4} \right] - C$$

www.dbraudlibrary.org.in

is diminished where C is the number of centuries in the year. Again epacts are increased by 1 seven times in intervals of 300 years and one time in 400 years. The same increases are shown by the expression

$$\left[\frac{8C + 13}{25} \right],$$

as one can see from the following table:

$C = 18$	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42
$\left[\frac{8C + 13}{25} \right] = 6$			7			8			9			10			11			12			13			

Hence it is easy to see that the Gregorian epact is defined by the congruence

$$E \equiv \alpha + \left[\frac{C}{4} \right] - C + \left[\frac{8C + 13}{25} \right] + 11c \pmod{30},$$

where α is a constant and c , as before, is the remainder left when the number of the year N is divided by 19. Now for the year 1900 the Gregorian calendar gives $E = 29$. Since $c = 0$, $C = 19$, for this year we have

$$29 \equiv \alpha + 4 - 19 + 6 \equiv \alpha - 9 \pmod{30},$$

whence $\alpha = 8$; and so in general

$$E \equiv 8 + \left[\frac{C}{4} \right] - C + \left[\frac{8C + 13}{25} \right] + 11c \pmod{30}.$$

According to the above table the Paschal new moon in March occurs on the $31 - E$ day of March or, considering April as the extension of March, on the $(31 - E) + 30$ day of March, disregarding for the present the two exceptions pointed out before. In general, therefore, Paschal new moons in March occur on dates F satisfying the congruence

$$F \equiv 23 + C - \left[\frac{C}{4} \right] - \left[\frac{8C + 13}{25} \right] - 11c \equiv 23 + C - \left[\frac{C}{4} \right] - \left[\frac{8C + 13}{25} \right] + 19c \pmod{30},$$

and dates $G = F + 13$ of the full moon satisfy the congruence

$$G \equiv 6 + C - \left[\frac{C}{4} \right] - \left[\frac{8C + 13}{25} \right] + 19c \pmod{30}.$$

To find the date of the first full moon occurring on or after March 21, we must find that solution of this congruence for which $G - 21$ is as small as possible and nonnegative. Now

$$G - 21 \equiv 15 + C - \left[\frac{C}{4} \right] - \left[\frac{8C + 13}{25} \right] + 19c \pmod{30},$$

and consequently $G - 21$ is the remainder in the division of

$$19c + M; \quad M = 15 + C - \left[\frac{C}{4} \right] - \left[\frac{8C + 13}{25} \right]$$

by 30, which remainder we shall denote by d . Finally

$$G = 21 + d$$

and the next following date is March $22 + d$. Now we must seek the date of the first Sunday in March falling on March $22 + d$ or after. Dates of Sundays in March satisfy the congruence (Sec. 1, Example 3)

$$k \equiv 2a + 4b + C - \left[\frac{C}{4} \right] + 5 \pmod{7}$$

or

$$k - 22 - d \equiv 2a + 4b + 6d + C - \left[\frac{C}{4} \right] + 4 \pmod{7}.$$

Consequently $k - 22 - d$ is the remainder in the division of

$$2a + 4b + 6d + L; \quad L = 4 + C - \left[\frac{C}{4} \right]$$

by 7, which remainder we shall denote by e . Finally

$$k = 22 + d + e$$

is the date of Easter in March, considering April as an extension of March. The date of Easter in April will be

$$d + e - 9$$

in case $22 + d + e > 31$.

We must consider now changes that are caused by the two exceptions mentioned at the end of Sec. 2. The first exception corresponds to epect 24. In this case, as follows from the congruence for E ,

$$19c + M \equiv 29 \pmod{30},$$

and so $d = 29$. The date of the first full moon on or after March 21 instead of being $21 + d$ will be $21 + d - 1$. To determine e we must therefore change d into $d - 1$, which changes e into $e + 1$ if $e < 6$, and into 0 if $e = 6$. The date of Easter remains $22 + d + e$ unless $e = 6$, in which case this date will be March $21 + 29 = 50$, or April 19.

The second exception occurs when $E = 25$ and, at the same time, $c \geq 11$. Then

$$19c + M \equiv 28 \pmod{30},$$

so that $d = 28$. Unless at the same time $e = 6$, nothing is changed in the final rule. But if $e = 6$, then Easter must be celebrated on March $21 + 28 = 49$, or April 18, instead of April 25. If we take $c = 11, 12, 13, 14, 15, 16, 17, 18$, corresponding values of M will be

$$M \equiv 2, 5, 10, 13, 16, 21, 24, 29.$$

Thus finally we have the following rule proposed by Gauss to find the date of Easter:

Divide the number of the year N by 4, 7, 19 and call the resulting remainders a, b, c . Divide

$$19c + M$$

by 30 and call the remainder d . Divide

$$2a + 4b + 6d + L$$

by 7 and call the remainder e . Then the date of Easter is

$$\text{March } (22 + d + e) \quad \text{or} \quad \text{April } (d + e - 9),$$

with the following two exceptions: (1) if $d = 29$, $e = 6$, Easter must be celebrated one week earlier on April 19; (2) if $d = 28$, $e = 6$, and $M = 2, 5, 10, 13, 16, 21, 24, 29$, Easter must be celebrated one week earlier on April 18. As to M and L , their expressions are

$$M = 15 + C - \left[\frac{C}{4} \right] - \left[\frac{8C + 13}{25} \right]$$

$$L = 4 + C - \left[\frac{C}{4} \right].$$

Similar rules apply for the Greek orthodox or Old Style calendar; only then $M = 15$, $L = 6$, and no exceptions occur.

Example 1. Find the date of Easter in 1940. Throughout the present century $M = 24$, $L = 5$; moreover, $a = 0$, $b = 1$, $c = 2$. Hence $19c + M = 62$, and $d = 2$; $2a + 4b + 6d + 5 = 21$, and $e = 0$. Easter in 1940 must be celebrated on March 24.

Example 2. In what years of the present century is Easter celebrated on April 1? We must have $d = 10 - e$ and

$$19c + 24 \equiv 10 - e \pmod{30}$$

$$2a + 4b + 6(10 - e) + 5 \equiv e \pmod{7}$$

or

$$19c \equiv 16 - e \pmod{30}$$

$$4b \equiv 2a - 2 \pmod{7}$$

whence

$$c \equiv 4 + 11e \pmod{30}, \quad b \equiv 3a + 3 \pmod{7}.$$

From the possible values $e = 0, 1, 2, 3, 4, 5, 6$, only those must be retained to which $c < 19$ corresponds. Such values of e are

$$e = 0, 1, 3, 4, 6,$$

and correspondingly

$$c = 4, 15, 7, 18, 10.$$

To find N we must solve the system of congruences

$$N \equiv a \pmod{4}, \quad N \equiv 3a + 3 \pmod{7}, \quad N \equiv c \pmod{19}.$$

By the Chinese rule

$$N \equiv -95a - 56c - 228 \pmod{532}.$$

Corresponding to five values of c and four values of a , we get 20 values of $N \pmod{532}$:

80,	276,	360,	444,	528
181,	265,	349,	433,	517
86,	170,	254,	338,	422
75,	159,	243,	327,	523.

Of these only 327, 338, 349, 360 must be retained, since others do not correspond to years of the present century. The requested years are found to be

1923, 1934, 1945, 1956.

Example 3. For what years of the present century does the general rule suffer exceptions? Exceptions take place when $d = 29$, $e = 6$, or $d = 28$, $e = 6$, since $M = 24$. If at first $d = 29$, $e = 6$, we have

$$19c \equiv 5 \pmod{30}, \quad 2b \equiv 1 - a \pmod{7},$$

whence $c \equiv 5$ and

$$b \equiv 4 - 4a \pmod{7}.$$

Correspondingly

$$N \equiv a \pmod{4}, \quad N \equiv 4 - 4a \pmod{7}, \quad N \equiv 5 \pmod{19}$$

and

$$N \equiv 437a - 52 \pmod{532}.$$

For $a = 0, 1, 2, 3$,

$$N \equiv 480, 385, 290, 195 \pmod{532}.$$

Only $N \equiv 385$ can be used; the corresponding year is 1934. If $d = 28$, $e = 6$,

$$19c \equiv 4 \pmod{30}, \quad 4b + 2a \equiv 1 \pmod{7},$$

whence $c \equiv 16$ and

$$b \equiv 2 - 4a \pmod{7}.$$

Correspondingly

$$N \equiv 437a + 16 \pmod{532},$$

and for $a = 0, 1, 2, 3$

$$N \equiv 16, 453, 358, 263 \pmod{532}.$$

Only $N \equiv 358$ can be used; to this the year 1954 corresponds. Thus the only years in the present century for which the rule suffers exceptions are 1954 and 1981.

CHAPTER VIII

RESIDUES OF POWERS

1. Exponent of a Modulo m . Let a be any number relatively prime to m taken as a modulus. In the series of powers of a

$$1, a, a^2, a^3, \dots \quad (A)$$

all terms are relatively prime to m and hence are congruent to terms of a reduced system of residues modulo m . Since any reduced system of residues contains $\varphi(m)$ terms, whereas series (A) is infinite, there must be two terms in (A), say a^k and a^l , congruent modulo m . We can suppose $l > k$; then, dividing both sides of the congruence

$$a^l \equiv a^k \pmod{m}$$

by a^k , which is relatively prime to m , we have

$$a^{l-k} \equiv 1 \pmod{m}.$$

Hence there are positive exponents s for which

$$a^s \equiv 1 \pmod{m}.$$

Let h be the smallest of such exponents; it is called "the exponent to which a belongs mod m ," or simply "exponent of a modulo m ." By its very definition h is characterized by two properties: first,

$$a^h \equiv 1 \pmod{m};$$

and second, no power of a with positive exponent $< h$ is congruent to 1 mod m .

If s is any positive exponent for which

$$a^s \equiv 1 \pmod{m},$$

then

$$s \equiv 0 \pmod{h}.$$

In fact, suppose that s , when divided by h , leaves the remainder r , so that we can write

$$s = hq + r; \quad 0 \leq r < h.$$

Then

$$a^s = (a^h)^q a^r$$

and, since $a^h \equiv 1 \pmod{m}$,

$$a^s \equiv a^r \equiv 1 \pmod{m}.$$

But this cannot hold unless $r = 0$, so that s is divisible by h .

Numbers

$$1, a, a^2, \dots, a^{h-1} \tag{B}$$

are all different modulo m , since the congruence

$$a^s \equiv a^r \pmod{m},$$

provided $s > r$, implies

$$a^{s-r} \equiv 1 \pmod{m},$$

and this is impossible if $s < h$, since then the positive number $s - r < h$ cannot be divisible by h . Numbers

$$a^h, a^{h+1}, \dots, a^{2h-1}$$

are congruent mod m to the terms $1, a, a^2, \dots, a^{h-1}$ of the series (B). Again,

$$a^{2h}, a^{2h+1}, \dots, a^{3h-1}$$

are congruent to terms of the series (B), and so on. That is to say, the series $1, a, a^2, \dots$ is periodic modulo m with the

period 1, a, a^2, \dots, a^{h-1} . In other words, if ρ_k is the remainder in the division of a^k by m , then the series

$$\rho_0, \rho_1, \rho_2, \dots$$

is periodic with a period of h terms

$$\rho_0, \rho_1, \dots, \rho_{h-1}$$

repeating itself indefinitely.

2. Practical Rule for the Formation of Periods. Congruent numbers evidently have the same periods of remainders. We can suppose, therefore, from the beginning that $a < m$. Then it is very easy to find step by step the remainders r_1, r_2, \dots, r_{m-1} obtained in the division of the numbers $a, 2a, \dots, (m-1)a$ by m . Evidently $r_1 = a$, next $r_2 = r_1 + a$ or $r_2 = r_1 + a - m$ according as $r_1 + a < m$ or $r_1 + a \geq m$; again $r_3 = r_2 + a$ or $r_3 = r_2 + a - m$ according as $r_2 + a < m$ or $r_2 + a \geq m$, and so on. Write the numbers 1, 2, $\dots, m-1$ and r_1, r_2, \dots, r_{m-1} in two lines, as shown here,

$$\begin{array}{c} 1, 2, 3, \dots, m-1 \\ r_1, r_2, r_3, \dots, r_{m-1} \end{array}$$

and add a third line of numbers in the following manner: In the first column place that number ρ_1 of the second line which stands below 1 in the first line; in the second column place that number ρ_2 of the second line which stands below ρ_1 in the first line; in the third column place that number ρ_3 which stands below ρ_2 in the first line, and continue in the same way until some number ρ_h in the third line is 1. Then

$$\rho_1, \rho_2, \dots, \rho_h$$

is the required period of remainders and h is the exponent of a modulo m . In fact $\rho_1 = r_1 \equiv a$, $\rho_2 = r_{\rho_1} \equiv \rho_1 a \equiv a^2$, $\rho_3 = r_{\rho_2} \equiv \rho_2 a \equiv a^3$ and so on, all congruences taken modulo m .

Example 1. Let us find the period of remainders for $a = 7$, $m = 15$. The whole procedure is summarized in the three following lines

1	2	3	4	5	6	7	8	9	10	11	12	13	14
7	14	6	13	5	12	4	11	3	10	2	9	1	8
7	4	13	1.										

Hence

$$7 \equiv 7, \quad 7^2 \equiv 4, \quad 7^3 \equiv 13, \quad 7^4 \equiv 1 \pmod{15},$$

so that $7 \pmod{15}$ belongs to the exponent 4 and the period of the remainders is

$$1, 7, 4, 13.$$

Example 2. Let $a = 2$, $m = 27$. In this case we have

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
2	4	8	10	12	14	16	18	20	22	24	26	1	3	5	7	9	11	13	15	17	19	21	23	25	26
2	4	8	16	5	10	20	13	26	25	23	19	11	22	17	7	14	1								

that is, $2 \pmod{27}$ belongs to the exponent 18, and the period of the remainders is

$$1, 2, 4, 8, 16, 5, 10, 20, 13, 26, 25, 23, 19, 11, 22, 17, 7, 14.$$

3. Properties of Exponents Modulo m . 1. The exponent h to which a number a relatively prime to m belongs mod m is a divisor of $\varphi(m)$. By Euler's theorem

$$a^{\varphi(m)} \equiv 1 \pmod{m};$$

hence by Sec. 1

$$\varphi(m) \equiv 0 \pmod{h}.$$

The same property can be proved independently of Euler's theorem, as Euler himself has shown. If the period

$$1, a, a^2, \dots, a^{h-1} \quad (A)$$

represents the reduced system of residues mod m , then $h = \varphi(m)$ and the statement is proved. If not, then there is a number b relatively prime to m and not congruent to any of the numbers (A). All numbers

$$b, ba, ba^2, \dots, ba^{h-1} \quad (B)$$

are relatively prime to m , different mod m among themselves and different mod m from the numbers (A). In fact the congruence

$$ba^s \equiv ba^r \pmod{m}$$

is equivalent to

$$a^s \equiv a^r \pmod{m},$$

and this congruence is impossible for two different numbers r, s taken from the series $0, 1, 2, \dots, h-1$. On the other hand,

$$ba^s \equiv a^r \equiv a^{r+h} \pmod{m}$$

implies

$$b \equiv a^{r-s+h} \pmod{m},$$

contrary to the definition of b . Thus (A) and (B) together contain $2h$ numbers different mod m and prime to m . If these $2h$ numbers form a reduced system of residues mod m , then $2h = \varphi(m)$, and the statement is proved. If not, then there is a number c prime to m and not congruent mod m to any of the numbers (A) and (B). In this case the series

$$c, ca, ca^2, \dots, ca^{h-1} \tag{C}$$

contains numbers prime to m , different mod m among themselves and different from the numbers (A) and (B). That the numbers (C) are different mod m among themselves and from the numbers (A) follows from a proof analogous to that for the numbers (B). To show that the numbers (C) differ from the numbers (B), it suffices to notice that the congruence

$$ca^s \equiv ba^r \equiv ba^{r+h} \pmod{m}$$

implies

$$c \equiv ba^{r-s+h} \pmod{m}$$

contrary to the fact that c is not congruent to any of the numbers (B). Series (A), (B), and (C) contain $3h$ numbers prime to m and different mod m . If these $3h$ numbers form

a reduced system of residues mod m , then $3h = \varphi(m)$, and the statement is proved. Continuing in the same way, we conclude that the number of members in a reduced system of residues is a multiple of h ; that is, $\varphi(m) = hf$.

From this property Euler's theorem follows immediately. For, raising both sides of the congruence

$$a^h \equiv 1 \pmod{m}$$

to the power f , we get

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

This was the way in which Euler himself proved his theorem, except for the use of congruence notation.

2. Let a belong to the exponent $h \pmod{m}$. To what exponent does a^s then belong? To answer this question let us seek all the exponents x for which

$$(a^s)^x \equiv 1 \pmod{m}$$

This congruence is fulfilled if and only if

$$sx \equiv 0 \pmod{h}.$$

Now let d be the g.c.d. of s and h ; then this congruence is entirely equivalent to

$$\frac{s}{d}x \equiv 0 \pmod{\frac{h}{d}}$$

or, since s/d and h/d are relatively prime, to

$$x \equiv 0 \pmod{\frac{h}{d}}.$$

That is, the required exponents are

$$x = \frac{h}{d}t, \quad t = 0, 1, 2, \dots$$

and the smallest positive one of them is

$$x = \frac{h}{d}$$

Consequently a^s belongs to the exponent h/d if $d = (s, h)$. In particular a^s belongs to the exponent h if and only if s is relatively prime to h .

3. Let a and b belong respectively to the exponents h and k , which are relatively prime. To what exponent does their product ab belong? Let us seek exponents x such that

$$(ab)^x \equiv a^x b^x \equiv 1 \pmod{m}.$$

Raising both members of this congruence to the powers h and k and noticing that

$$a^{hx} \equiv 1, \quad b^{kx} \equiv 1 \pmod{m},$$

we get

$$b^{hx} \equiv 1 \pmod{m},$$

whence

$$hx \equiv 0 \pmod{k}, \quad kx \equiv 0 \pmod{h}$$

or, since h and k are relatively prime by hypothesis,

$$x \equiv 0 \pmod{k}, \quad x \equiv 0 \pmod{h}$$

whence

$$x = kht,$$

where t is an integer. Conversely, for such exponents x

$$(ab)^x \equiv 1 \pmod{m}.$$

Since the smallest positive value of x corresponds to $t = 1$, it is clear that ab modulo m belongs to the exponent hk . More generally, if the numbers a, b, c, \dots, l belong to the exponents $\alpha, \beta, \gamma, \dots, \lambda$ modulo m and the latter numbers are relatively prime in pairs, then $abc \dots l$ belongs to the exponent $\alpha\beta\gamma \dots \lambda$.

Exercises and Problems

- Determine the exponents to which the numbers 3, 7, 13 belong for the moduli 17, 29, 61, respectively. *Ans.* 16, 7, 3.
- Determine the period of the remainders for $a = 11$, $m = 102$.
- Prove that odd prime divisors of the numbers $x^2 + 1$ are of the form $4n + 1$.
- Prove that odd prime divisors of the numbers $x^4 + 1$ are of the form $8n + 1$.
- Prove that odd prime divisors of the numbers $x^2 + x + 1$ are of the form $6n + 1$.
- Prove that there are infinitely many primes of each of the forms $4n + 1$, $6n + 1$, $8n + 1$.
- If p is a prime > 2 , then prime divisors of

$$a^{p-1} + a^{p-2} + \dots + a + 1$$

are either p or primes of the form $2px + 1$. Prove that there are infinitely many primes of the form $2px + 1$.

- If the number $2^{2^n} + 1$ is not prime, its prime divisors are of the form

$$2^{2^n+1}w + 1$$

4. Primitive Roots for Prime Moduli. From now on we shall confine ourselves to prime moduli. The exponent to which any number nondivisible by a prime p belongs modulo p must be a divisor of $p - 1$. If d is an arbitrarily selected divisor of $p - 1$, are there numbers belonging to the exponent d modulo p ? We shall see presently that there are exactly $\varphi(d)$ incongruent numbers of this kind. At present let us denote by $\psi(d)$ the number of integers in the series 1, 2, 3, . . . , $p - 1$ belonging to a chosen exponent d , a divisor of $p - 1$. If there are no numbers belonging to the exponent d , then $\psi(d) = 0$. Suppose that a belongs to the exponent d . Then the congruence

$$x^d \equiv 1 \pmod{p} \tag{A}$$

of degree d is satisfied by d incongruent numbers

$$1, a, a^2, \dots, a^{d-1}. \tag{B}$$

By Lagrange's theorem the numbers (B) are the only roots of the congruence (A). On the other hand, any number belonging to the exponent d must satisfy (A). Consequently, numbers belonging to the exponent d must be sought among the numbers (B). By Sec. 3, powers of a belong to the exponent d if and only if the exponents of these powers are numbers relatively prime to d . It follows, then, that in the series (B) there are exactly $\varphi(d)$ numbers belonging to the exponent d . Thus, if there is one number belonging to d , then there are exactly $\varphi(d)$ such numbers; in other words, either $\psi(d) = 0$ or $\psi(d) = \varphi(d)$, so that in any event $\psi(d) \leq \varphi(d)$. Now the numbers 1, 2, 3, . . . , $p - 1$ belong to various divisors d, d', d'', \dots of $p - 1$, as exponents, hence

$$\psi(d) + \psi(d') + \psi(d'') + \dots = p - 1.$$

But we have also

$$\varphi(d) + \varphi(d') + \varphi(d'') + \dots = p - 1;$$

whence, by subtraction,

$$[\varphi(d) - \psi(d)] + [\varphi(d') - \psi(d')] + [\varphi(d'') - \psi(d'')] + \dots = 0.$$

But all the differences in the brackets are nonnegative integers, and their sum can equal 0 only if they are all equal to 0; hence

$$\psi(d) = \varphi(d), \quad \psi(d') = \varphi(d'), \quad \psi(d'') = \varphi(d''), \dots$$

for all divisors d, d', d'', \dots of $p - 1$.

Thus to any selected divisor d of $p - 1$ belong exactly $\varphi(d)$ different numbers modulo p . In particular there are $\varphi(p - 1)$ different numbers modulo p belonging to the exponent $p - 1$. Any number which for a prime modulus p belongs to the exponent $p - 1$ is called, following Euler, a

“primitive root” (*radix primitiva*) of p . If g is a primitive root of p , then powers of g

$$1, g, g^2, \dots, g^{p-2}$$

represent a reduced system of residues mod p . The importance of primitive roots lies exactly in this possibility of representing a reduced system of residues for a prime modulus. How easily several of the previously established theorems can be derived from the consideration of primitive roots one can see from the following examples.

Since $1, 2, 3, \dots, p-1$ and $1, g, g^2, \dots, g^{p-2}$ are two reduced systems of residues mod p , we have

$$1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-1) \equiv g^{1+2+\dots+(p-2)} \equiv g^{\frac{(p-2)(p-1)}{2}} \pmod{p}.$$

Now for $p > 2$

$$g^{p-1} - 1 \equiv (g^{\frac{p-1}{2}} + 1)(g^{\frac{p-1}{2}} - 1) \equiv 0 \pmod{p},$$

but

$$g^{\frac{p-1}{2}} - 1$$

cannot be divisible by p , since g belongs to the exponent $p-1$; consequently

$$g^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

and

$$g^{\frac{(p-2)(p-1)}{2}} \equiv -1 \pmod{p}$$

for an odd prime p . As a result, we get another and very simple proof of Wilson's theorem

$$1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-1) \equiv -1 \pmod{p}$$

for an odd prime p , and for $p = 2$ it is evident.

For another application consider the sum

$$S_n(p) = 1^n + 2^n + \cdots + (p-1)^n.$$

We have again

$$S_n(p) \equiv 1 + g^n + g^{2n} + \cdots + g^{(p-2)n} \pmod{p}.$$

Now, if n is not divisible by $p-1$, $g^n - 1$ is not divisible by p . In this case

$$1 + g^n + g^{2n} + \cdots + g^{(p-2)n} = \frac{g^{n(p-1)} - 1}{g^n - 1}$$

is clearly divisible by p , and so

$$S_n(p) \equiv 0 \pmod{p}.$$

But if n is divisible by $p-1$, then

$$g^n \equiv g^{2n} \equiv \cdots \equiv g^{(p-2)n} \equiv g^n \pmod{p}$$

and

$$S_n(p) \equiv p-1 \equiv -1 \pmod{p}.$$

5. Method for Finding Primitive Roots. Though the existence of primitive roots for prime moduli has been proved, the proof does not suggest any practical method for finding the primitive roots in a given case. No direct method for this purpose is known which does not require tedious trials when the modulus is somewhat large. Perhaps the best is based upon the following considerations. Let

$$p-1 = a^{\alpha} b^{\beta} c^{\gamma} \cdots l^{\lambda}$$

be a prime factorization of $p-1$. Suppose we can find in some way numbers P, Q, R, \dots, W belonging modulo p to the exponents $a^{\alpha}, b^{\beta}, c^{\gamma}, \dots, l^{\lambda}$, respectively. Since these exponents are relatively prime in pairs,

$$PQR \cdots W,$$

or any residue of it modulo p , will belong, by Sec. 3, to the exponent $a^\alpha b^\beta c^\gamma \cdots l^k = p - 1$ and be therefore a primitive root. The whole question is one of finding such numbers P, Q, R, \dots, W . Now if A is any nonresidue of the power $a \pmod p$, we can take

$$P \equiv A^{\frac{p-1}{a^\alpha}} \pmod p.$$

In fact

$$\left(A^{\frac{p-1}{a^\alpha}}\right)^{a^\alpha} \equiv A^{p-1} \equiv 1 \pmod p;$$

consequently the exponent h to which

$$A^{\frac{p-1}{a^\alpha}}$$

belongs modulo p is a divisor of a^α . Hence $h = a^k$ where $k \leq \alpha$, and it is necessary to prove that k cannot be less than α . Supposing $k < \alpha$, it is clear that $a^{\alpha-1}$ will be divisible by a^k , but then

$$\left(A^{\frac{p-1}{a^\alpha}}\right)^{a^{\alpha-1}} \equiv A^{\frac{p-1}{a}} \equiv 1 \pmod p,$$

which is impossible by Sec. 12, Chap. VII, since A is a nonresidue of the power a . Thus $k = \alpha$, and the statement is proved. Similarly if B, C, \dots, L are nonresidues of the powers b, c, \dots, l , we can take

$$Q \equiv B^{\frac{p-1}{b^\beta}}, \quad R \equiv C^{\frac{p-1}{c^\gamma}}, \quad \dots, \quad W \equiv L^{\frac{p-1}{l^k}} \pmod p.$$

As to the nonresidues A, B, C, \dots of the powers a, b, c, \dots , they can be found by trials, and it is important to show that the number of trials will not be too great for moderate values of p . To this end we shall prove that, e being any divisor of $p - 1$, either -1 is a nonresidue of the power e or there is a positive nonresidue less than \sqrt{p} . The proof is based upon the following lemma:

For some positive $r < \sqrt{p}$, a residue of $Nr \pmod{p}$, where N is any given integer, numerically will be less than \sqrt{p} . To prove the lemma, denote by t an integer such that

$$t^2 < p < (t + 1)^2$$

and consider $(t + 1)^2$ integers

$$Nx - y,$$

where x and y run independently through the values $0, 1, 2, \dots, t$. Since the number of such integers is greater than p , among them there must be at least two which are congruent modulo p . Let two such integers be

$$Nx' - y', \quad Nx'' - y'',$$

so that, setting $x'' - x' = r$, $y'' - y' = s$, we have

$$Nr \equiv s \pmod{p}$$

Both r and s are numerically $\leq t < \sqrt{p}$, and r is different from 0. For if r were 0, s would be divisible by p and, since s is numerically less than p , s would be 0 too. But both equalities $r = 0$, $s = 0$ are impossible, since the two pairs x'', y'' and x', y' are supposed to be different. Thus r is different from 0, and we can suppose it to be positive and $< \sqrt{p}$. At the same time the residue s of Nr is numerically less than \sqrt{p} , and thus the lemma is proved. Notice that nowhere in this proof was p supposed to be prime; the proof supposes only that it is not a square.

To apply this lemma, we suppose that p is a prime and N is some nonresidue of the power $e \pmod{p}$. We also suppose that -1 is a residue of the power e . By the lemma there is a positive number $r < \sqrt{p}$ such that

$$Nr \equiv s \pmod{p}$$

and s is numerically less than \sqrt{p} . Now if r is a nonresidue, the statement is proved. But if r is a residue, then, since

$$(Nr)^{\frac{p-1}{e}} \equiv N^{\frac{p-1}{e}} \pmod{p},$$

Nr and s are nonresidues. If s is a positive number, then there is a positive nonresidue $< \sqrt{p}$. If s is negative and, by hypothesis, -1 is a residue, then $-s$ will be a positive nonresidue $< \sqrt{p}$. Thus in all cases either -1 is a nonresidue of the power e or there is a positive nonresidue $< \sqrt{p}$.

Thus in seeking the nonresidues of the powers a, b, c, \dots we may try numbers $< \sqrt{p}$, and thus the number of trials will be considerably reduced. When one primitive root g is found, the others will be powers of g with exponents relatively prime to $p-1$ or any residues of such powers.

Example 1. Find the least positive primitive root of $p = 43$. Since

$$p-1 = 2 \cdot 3 \cdot 7,$$

we may seek first some nonresidues of the powers 2, 3, 7. We find at once that -1 is a quadratic nonresidue, so that we can take $A = -1$. But -1 is necessarily a residue for any odd power, so that to find a cubic nonresidue we must seek it among the positive numbers $< \sqrt{43}$ and, as can easily be seen, only among the primes 2, 3, 5. Now

$$2^{14} \equiv 1 \pmod{43}, \quad 3^{14} \equiv -7 \pmod{43};$$

hence we can take $B = 3$. Again,

$$2^6 \equiv 21 \pmod{43},$$

so that $C = 2$ is a nonresidue of the seventh power. One primitive root is therefore

$$g \equiv (-1)^{21} \cdot 3^{14} \cdot 2^6 \equiv 7 \cdot 21 \equiv 18 \pmod{43}.$$

To find the least positive primitive root, we form the period of remainders of 18 (mod 43) as explained in Sec. 2:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
18	36	11	29	4	22	40	15	33	8	26	1	19	37	12	30	5	23	41	16	34
<u>18</u>	<u>23</u>	<u>27</u>	<u>13</u>	<u>19</u>	<u>41</u>	<u>7</u>	<u>40</u>	<u>32</u>	<u>17</u>	<u>5</u>	<u>4</u>	<u>29</u>	<u>6</u>	<u>22</u>	<u>9</u>	<u>33</u>	<u>35</u>	<u>28</u>	<u>31</u>	<u>42</u>
22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42
9	27	2	20	38	13	31	6	24	42	17	35	10	28	3	21	39	14	32	7	25
25	<u>20</u>	<u>16</u>	<u>30</u>	<u>24</u>	<u>2</u>	<u>36</u>	<u>3</u>	<u>11</u>	<u>26</u>	<u>38</u>	<u>39</u>	<u>14</u>	<u>37</u>	<u>21</u>	<u>34</u>	<u>10</u>	<u>8</u>	<u>15</u>	<u>12</u>	<u>1</u>

The underlined 12 numbers are primitive roots; the least of them is 3.

Example 2. Find a primitive root of $p = 127$. Here

$$p - 1 = 2 \cdot 3^2 \cdot 7.$$

Again we can take $A = -1$ since -1 is a quadratic nonresidue of 127. To find a cubic nonresidue, we try the primes 2, 3, 5, 7, ... and find

$$2^{42} \equiv 1 \pmod{127}, \quad 3^{42} \equiv -20 \pmod{127},$$

and correspondingly we can take $B = 3$. Again

$$2^{18} \equiv 16 \pmod{127};$$

so $C = 2$. Finally

$$g \equiv (-1)^{63} \cdot 3^{14} \cdot 2^{18} \equiv 29 \pmod{127}$$

is one of the primitive roots.

Exercises and Problems

1. Find the least primitive roots for $p = 47, 79, 97$. *Ans.* 5, 3, 5.
2. Find a primitive root for $p = 157, 587$. *Ans.* 6, -4.
3. If e is a divisor of $p - 1$, the congruence $x^e \equiv 1 \pmod{p}$ has exactly e roots. A root of this congruence which belongs to an exponent $< e$ satisfies at least one of the congruences

$$x^{e/a} \equiv 1, \quad x^{e/b} \equiv 1, \quad x^{e/c} \equiv 1, \quad \dots \pmod{p},$$

a, b, c, \dots being different prime divisors of e .

4. Referring to the preceding problem, prove that $\varphi(e)$ distinct integers mod p belong to the exponent e .
5. Prove that the product of all primitive roots is congruent to 1 mod p if $p > 3$.
6. Show that the sum of all primitive roots is $\equiv 0$ if $p - 1$ is divisible by a square > 1 ; and that, otherwise, it is $\equiv \pm 1 \pmod{p}$. How would one determine the sign \pm ?

7. A primitive root for a composite modulus m would be a number G whose powers

$$1, G, G^2, \dots, G^{\varphi(m)-1}$$

form a reduced system of residues mod m . Prove that primitive roots exist only if $m = p^n$ or $m = 2p^n$ where p is an odd prime or $m = 4$. **HINT:** Let g be a primitive root mod p , and let $g^{p-1} - 1$ be nondivisible by p^2 ; then $G = g$; otherwise $G = g + p$ is a primitive root mod p^n . Also, for every odd number a ,

$$a^{2^n-2} \equiv 1 \pmod{2^n}.$$

6. Indices. Since

$$1, g, g^2, \dots, g^{p-2},$$

for a primitive root g mod p , is a reduced system of residues, every number a nondivisible by p is congruent mod p to a power of g :

$$a \equiv g^r \pmod{p}.$$

The exponent r of this power is called the "index of a " and is denoted by "ind a ," so that

$$a \equiv g^{\text{ind } a} \pmod{p}.$$

The relation between a number and its index is very similar to the relation between a number and its logarithm. For a given a its index belongs to a definite class of numbers mod $p - 1$; in fact the congruence

$$g^{\nu'} \equiv g^{\nu} \pmod{p}$$

is possible only if $\nu' \equiv \nu \pmod{p - 1}$. Of course, the same number can have various indices according to the choice of the primitive root g ; but once this choice is made, the indices become determined modulo $p - 1$.

Between the index of a product aa' and the indices of the factors a and a' , the following fundamental relation holds:

$$\text{ind } (aa') \equiv \text{ind } a + \text{ind } a' \pmod{p - 1}.$$

To prove this, it suffices to observe that by definition

$$a \equiv g^{\text{ind } a}, \quad a' \equiv g^{\text{ind } a'} \pmod{p},$$

whence

$$aa' \equiv g^{\text{ind } a + \text{ind } a'} \pmod{p}.$$

Since, on the other hand,

$$aa' \equiv g^{\text{ind } (aa')} \pmod{p},$$

we must have

$$\text{ind } (aa') \equiv \text{ind } a + \text{ind } a' \pmod{p-1}.$$

This congruence can be immediately extended to any number of factors

$$\text{ind } (aa'a'' \cdots) \equiv \text{ind } a + \text{ind } a' + \text{ind } a'' + \cdots$$

and in particular

$$\text{ind } (a^n) \equiv n \text{ind } a \pmod{p-1}.$$

7. Application of Indices to the Solution of Congruences.

Consider the binomial congruence

$$x^n \equiv a \pmod{p}, \tag{A}$$

where a is a number nondivisible by a prime p . Taking the indices of both numbers, we have

$$n \text{ind } x \equiv \text{ind } a \pmod{p-1}, \tag{B}$$

which is a congruence of the first degree to determine the unknown index of x . If this congruence has no solution for $\text{ind } x$, the proposed congruence (A) is impossible. Let d be the greatest common divisor of n and $p-1$; then the congruence (B) is possible if and only if

$$\text{ind } a \equiv 0 \pmod{d},$$

which is entirely equivalent to

$$\frac{p-1}{d} \text{ind } a \equiv 0 \pmod{p-1}$$

or

$$a^{\frac{p-1}{d}} \equiv 1 \pmod{p}, \quad (C)$$

since numbers with indices congruent to $0 \pmod{p-1}$ are congruent to $1 \pmod{p}$. Congruence (C) is thus the necessary and sufficient condition for the possibility of congruence (A). This condition being satisfied, congruence (B) gives d distinct values for $\text{ind } x \pmod{p-1}$, to which correspond d distinct roots modulo p of the congruence (A).

Thus the congruence

$$x^n \equiv a \pmod{p}$$

is possible only if

$$a^{\frac{p-1}{d}} \equiv 1 \pmod{p},$$

and, if this condition is fulfilled, it has exactly d solutions, which can be found by solving a certain congruence of degree d . Congruence (B) can be written thus:

$$\frac{n}{d} \text{ ind } x \equiv \frac{\text{ind } a}{d} \pmod{\frac{p-1}{d}}. \quad (D)$$

Moreover,

$$\frac{p-1}{d} \text{ ind } x \equiv 0 \pmod{\frac{p-1}{d}}. \quad (E)$$

Since n/d and $(p-1)/d$ are relatively prime numbers, two positive integers u and v can be found by solving the indeterminate equation

$$\frac{n}{d} u - \frac{p-1}{d} v = 1.$$

Multiplying both members of (D) by u and subtracting (E) multiplied by v , we have

$$\text{ind } x \equiv u \frac{\text{ind } a}{d} \pmod{\frac{p-1}{d}}$$

or

$$d \text{ ind } x \equiv u \text{ ind } a \pmod{p-1},$$

whence

$$x^d \equiv a^u \pmod{p},$$

and this is the congruence of degree d , giving all d solutions of the proposed congruence when the latter is possible.

Example. Consider the congruence

$$x^{15} \equiv 2 \pmod{43}.$$

Since $(15, 42) = 3$, we must see whether the condition

$$2^{14} \equiv 1 \pmod{43}$$

is satisfied or not. Since it is satisfied, the proposed congruence has three roots which satisfy a congruence of the third degree. To find this congruence we solve for u and v the equation

$$15u - 42v = 3$$

and we find $u = 3$, $v = 1$. Consequently three roots of the proposed congruence satisfy the congruence

$$x^3 \equiv 8 \pmod{43}.$$

A number a for which the congruence

$$x^n \equiv a \pmod{p}$$

is possible is a residue of the n th power. If n divides $p - 1$, the condition for a being a residue of the n th power is

$$a^{\frac{p-1}{n}} \equiv 1 \pmod{p},$$

which was found in a different way in Sec. 12, Chap. VII. If n does not divide $p - 1$, but the g.c.d. of $p - 1$ and n is d , then the condition for a being a residue of the n th power is

$$a^{\frac{p-1}{d}} \equiv 1 \pmod{p}.$$

That is, all the residues of the n th power are residues of a smaller power d . Consequently the theory of residues of the n th power presents interest only when n is a divisor of $p - 1$. Thus there is no special theory of cubic residues for prime moduli of the form $p = 3n + 2$; in this case all numbers are cubic residues. Also for primes $p = 4n + 3$ the theory of biquadratic residues coincides with the theory of quadratic residues.

8. Tables of Indices and Primitive Roots. At the end of this book one can find tables which for all primes not exceeding 100 permit one to find the index of any given number and, conversely, a number corresponding to a given index. The largest collection of tables of indices for all primes $< 1,000$, the "Canon arithmeticus," computed under the direction of Jacobi, was published in 1839. There are extensive tables of primitive roots. One such table, giving the smallest primitive roots for all primes $< 6,200$, can be found in the book "Anfangsgründe der Zahlentheorie," by G. Wertheim.

When we have a table of indices, the solution of binomial congruences does not require anything but the solution of congruences of the first degree. For instance, if we want to find three roots of the congruence

$$x^3 \equiv 8 \pmod{43},$$

we replace this congruence by the congruence of the first degree:

$$3 \text{ ind } x \equiv 3 \text{ ind } 2 \pmod{42}.$$

or

$$\text{ind } x \equiv \text{ind } 2 \pmod{14}.$$

Now in Example 1, Sec. 5, we have a table of indices for $p = 43$ corresponding to the primitive root 18. From this table we find $\text{ind } 2 = 27$; hence

$$\text{ind } x \equiv 27, 41, 13 \pmod{42}.$$

To indices 13, 27, 41 correspond, respectively, 29, 2, 12, so that the roots of the congruence

$$x^3 \equiv 8 \pmod{43},$$

which are the same as the roots of the congruence

$$x^{15} \equiv 2 \pmod{43},$$

are

$$x \equiv 2, 12, 29 \pmod{43}.$$

Exercises and Problems

1. By means of the table of indices, solve the following congruences:
 (a) $x^2 \equiv 46 \pmod{97}$; (b) $x^7 \equiv 5 \pmod{71}$; (c) $x^8 \equiv 2 \pmod{89}$.
 Ans. (a) 20, 21, 56; (b) 10, 15, 16, 24, 36, 54, 58; (c) $\pm 9, \pm 19, \pm 23, \pm 39$.

2. Solve the congruences

$$(a) x^{40} \equiv 55 \pmod{73}; \quad (b) x^{13} \equiv -3 \pmod{67}.$$

$$\text{Ans. (a) } \pm 13; \pm 14, \pm 16, \pm 67; \quad (b) \pm 5, \pm 11, \pm 51.$$

3. Denote by $(\text{ind } a)_g$ the index of a when a primitive root g is chosen as the basis of the system of indices. Show that in two systems with bases g and γ , indices of the same number are connected by the congruence

$$(\text{ind } a)_\gamma \equiv (\text{ind } a)_g (\text{ind } g)_\gamma \pmod{p-1}.$$

4. The index of a number a belonging to the exponent e is a multiple of $(p-1)/e$. Show that a primitive root can be so chosen that the index of a will be equal to $(p-1)/e$.

5. Among the roots of the congruence

$$x^d \equiv a \pmod{p}$$

there are

$$\frac{\phi(p-1)}{\phi\left(\frac{p-1}{d}\right)}$$

primitive roots if a belongs to the exponent $\frac{p-1}{d} \pmod{p}$.

6. If a prime p is of the form $6n+5$, the least positive residues of the numbers

$$1^3, 2^3, 3^3, \dots, (p-1)^3$$

coincide in their totality with $1, 2, 3, \dots, p-1$. For primes of the form $6n+1$, each of these residues repeats itself exactly three times.

7. Show that the sum of the cubic residues in the series $1, 2, 3, \dots, p-1$ is $p(p-1)/2$ if $p \equiv 5 \pmod{6}$ and $p(p-1)/6$ if $p \equiv 1 \pmod{6}$.

8. By counting lattice points in the area bounded by the lines $y^3 = px$, $y = 1$, $y = p-1$ (including boundary lines) in two different ways, establish for an odd prime $p > 3$ the identity

$$[\sqrt[3]{p}] + [\sqrt[3]{2p}] + [\sqrt[3]{3p}] + \dots + [\sqrt[3]{(p-1)^2p}] = \frac{1}{3}(p-1)(3p^2 - 7p + 6).$$

9. Find a number written in the scale of seven, with less than 40 digits, such that if the digit "3" is moved from its extreme right to its extreme left, the result (still in the scale of seven) is $\frac{2}{5}$ of the original number.

Ans. $1\frac{1}{2}_7(7^{22} - 1)$.

APPENDIX

ON CARD SHUFFLING

1. A simple, though not easily practicable, way of shuffling cards consists in dividing a pack of $2n$ cards into equal halves and placing the cards of the first (upper) half between consecutive cards of the second half, the last card of the first half occupying the position at the bottom of the pack after shuffling. Thus if eight cards from the top down are denoted by

1 2 3 4 5 6 7 8

the position of the cards after shuffling will be

5 1 6 2 7 3 8 4.

The problem with which we shall deal here consists in finding the position of any given card after any number of shufflings. Let the cards in the original order from the top down be

1, 2, 3, . . . , n | $n + 1, n + 2, . . . , 2n$.

After shuffling, cards 1, 2, 3, . . . , n occupy the second, fourth, sixth, . . . , $2n$ th places, whereas cards $n + 1, n + 2, . . . , 2n$ occupy the first, third, . . . , $(2n - 1)$ th places. Let some card occupy place x_1 before shuffling and place x_2 after shuffling. Then, by our previous remarks,

$$x_2 = 2x_1$$

if $x_1 \leq n$ and

$$x_2 = 2x_1 - 2n - 1$$

if $x_1 > n$. In both cases we have the congruence

$$x_2 \equiv 2x_1 \pmod{2n + 1}$$

which, because $x_2 < 2n + 1$, determines x_2 completely and can replace the two expressions for x_2 which have a different form according to the value of x_1 . If the shufflings are repeated in exactly the same manner and the places occupied by the chosen card after the second, third, . . . shufflings are x_3, x_4, \dots , then in the same manner we have

$$x_3 \equiv 2x_2, \quad x_4 \equiv 2x_3, \quad \dots, \quad x_{k+1} \equiv 2x_k \pmod{2n+1},$$

whence, by successive substitutions,

$$x_{k+1} \equiv 2^k x_1 \pmod{2n+1}.$$

This congruence solves the problem of finding the position of any chosen card after any number of shufflings.

Suppose now that after k shufflings the first card returns to its original place. Then $x_{k+1} = x_1 = 1$ and

$$2^k \equiv 1 \pmod{2n+1},$$

which shows that for any x_1 www.dbraulibrary.org.in

$$x_{k+1} \equiv x_1 \pmod{2n+1};$$

that is, $x_{k+1} = x_1$, or all cards return to their original positions as soon as the first one does so. The smallest number of shufflings restoring all cards to their original positions is, therefore, the exponent to which 2 belongs mod $2n + 1$. Now for an ordinary pack of 52 cards, 2 belongs to the exponent $52 \pmod{53}$, and so 52 shufflings are required to restore the order of the cards.

2. Another interesting but less common way of shuffling cards consists in taking the top card in the right hand and placing other cards alternately above and below it. Thus cards 1, 2, 3, 4, 5, 6, 7, 8 in the original position are placed after shuffling in the order 8, 6, 4, 2, 1, 3, 5, 7. In general, cards

$$1, 2, 3, \dots, 2n$$

in the original position are placed in the order

$$2n, 2n - 2, \dots, 4, 2, 1, 3, 5, \dots, 2n - 1.$$

Let the original position of some card be x_1 , and let x_2 be its position after shuffling. Then if x_1 is even, it occupies the place $x_1/2$ from the beginning of the series $2, 4, \dots, 2n$ and $n - x_1/2 + 1$ from the end, so that

$$x_2 = n - \frac{x_1}{2} + 1.$$

If x_1 is odd, it occupies the place $\frac{x_1 + 1}{2}$ from the beginning of the series $1, 3, 5, \dots, 2n - 1$; consequently

$$x_2 = n + \frac{x_1 + 1}{2}.$$

The formulas for x_2 look quite different for an even and an odd x_1 . Yet they both can be expressed in one formula of slightly more complicated structure:

$$x_2 = n - (-1)^{x_1} \frac{x_1}{2} + \frac{1}{2} + \frac{1 + (-1)^{x_1}}{4},$$

and this in turn can be replaced by

$$2(2x_2 - 1) = (-1)^{x_1 - 1}(2x_1 - 1) + 4n + 1$$

or by a congruence

$$2(2x_2 - 1) \equiv (-1)^{x_1 - 1}(2x_1 - 1) \pmod{4n + 1},$$

which determines $2x_2 - 1$ completely as the least positive residue of $(-1)^{x_1 - 1}(2x_1 - 1)$ modulo $4n + 1$. Places occupied by the same card after the second, third, \dots shufflings will be denoted by x_3, x_4, \dots . Putting for brevity

$$2x_i - 1 = v_i,$$

we shall have the congruences

$$2v_2 \equiv (-1)^{\frac{v_1-1}{2}} v_1$$

$$2v_3 \equiv (-1)^{\frac{v_2-1}{2}} v_2$$

$$\dots \dots \dots$$

$$2v_{k+1} \equiv (-1)^{\frac{v_k-1}{2}} v_k; \quad (\text{mod } 4n + 1)$$

whence, after eliminating v_2, v_3, \dots, v_k ,

$$2^k v_{k+1} \equiv (-1)^{\epsilon_k} v_1 \pmod{4n + 1},$$

where

$$\epsilon_k = \frac{v_1 - 1}{2} + \frac{v_2 - 1}{2} + \dots + \frac{v_k - 1}{2}.$$

Now, if after k shufflings the first card is restored to its original position, $v_{k+1} = v_1 = 1$ and

$$2^k \equiv \pm 1 \pmod{4n + 1}.$$

At the same time all the cards will return to their initial positions, for then

$$v_{k+1} \equiv \pm v_1 \pmod{4n + 1}.$$

The sign $-$ cannot hold in this congruence; otherwise the even number $v_1 + v_{k+1}$ would be divisible by $4n + 1$ and so would be $\frac{1}{2}(v_1 + v_{k+1})$. But this is impossible, since both v_1 and v_{k+1} are less than $4n$. So in the preceding congruence the sign $+$ must hold, but then $v_{k+1} = v_1$ and $x_{k+1} = x_1$ for any card. Thus the smallest number of shufflings restoring all cards to their original order is the smallest exponent k , such that

$$2^k \equiv \pm 1 \pmod{4n + 1}$$

without specifying the sign \pm .

For an ordinary pack $2n = 52$, $4n + 1 = 105$, and mod 105

$$\begin{array}{llll} 2^1 \equiv 2 & 2^2 \equiv 4 & 2^3 \equiv 8 & 2^4 \equiv 16 \\ 2^5 \equiv 32 & 2^6 \equiv 64 & 2^7 \equiv 23 & 2^8 \equiv 46 \\ 2^9 \equiv -13 & 2^{10} \equiv -26 & 2^{11} \equiv 53 & 2^{12} \equiv 1. \end{array}$$

Thus 12 shufflings by this method suffice to restore the original order of the cards.

CHAPTER IX

ARITHMETICAL PROPERTIES OF BERNOULLIAN NUMBERS

1. Origin of Bernoullian Numbers. The following formulas, well known since remote times,

$$1 + 2 + 3 + \dots + (x-1) = \frac{x^2}{2} - \frac{x}{2}$$

$$1^2 + 2^2 + 3^2 + \dots + (x-1)^2 = \frac{x^3}{3} - \frac{x^2}{2} + \frac{x}{6}$$

$$1^3 + 2^3 + 3^3 + \dots + (x-1)^3 = \frac{x^4}{4} - \frac{x^3}{2} + \frac{x^2}{4}$$

express the sums

$$S_n(x) = 1^n + 2^n + \dots + (x-1)^n$$

for $n = 1, 2, 3$, as polynomials in x of the respective degrees 2, 3, 4 with rational coefficients. Jacob Bernoulli (1654-1705), the eldest member of the family of Bernoullis, famous in the history of mathematics, made the important discovery that for any positive integer n the sum $S_n(x)$ coincides, when x is an integer, with the polynomial

$$\frac{x^{n+1}}{n+1} - \frac{x^n}{2} + B_1 \frac{n x^{n-1}}{1} - B_2 \frac{n(n-1)(n-2) x^{n-3}}{1 \cdot 2 \cdot 3} + \dots,$$

the last term of which is

$$(-1)^{n/2-1} B_{n/2} x \quad \text{or} \quad (-1)^{(n-3)/2} n B_{(n-1)/2} \frac{x^2}{2},$$

according as n is even or odd, and B_1, B_2, B_3, \dots are the rational numbers

$$B_1 = \frac{1}{6}, B_2 = \frac{1}{30}, B_3 = \frac{1}{42}, B_4 = \frac{1}{30}, B_5 = \frac{5}{66}, \dots,$$

determined one by one in a recurrent manner. These numbers, in honor of their discoverer, are called Bernoullian numbers. They play an important part in analysis and possess remarkable arithmetical properties, the principal of which we shall consider in this chapter.

2. Definition of Bernoullian Numbers by a Symbolic Formula. The Bernoullian numbers are introduced in the easiest and shortest way by means of a symbolic method of Blissard and Lucas. If a sequence of numbers b_1, b_2, \dots, b_n satisfies a linear relation

$$c_0 b_n + c_1 b_{n-1} + \dots + c_{n-1} b_1 + c_n = 0,$$

we agree to write this relation symbolically thus:

$$f(b) = c_0 b^n + c_1 b^{n-1} + \dots + c_{n-1} b + c_n = 0$$

on the condition that one replaces any power b^k by b_k .

It is evident that the two symbolic relations

$$\begin{aligned} f(b) &= c_0 b^n + c_1 b^{n-1} + \dots + c_n = 0 \\ \varphi(b) &= d_0 b^n + d_1 b^{n-1} + \dots + d_n = 0 \end{aligned}$$

imply

$$f(b) \pm \varphi(b) = 0.$$

For, passing to the nonsymbolic form, the last relation becomes

$$(c_0 \pm d_0) b_n + (c_1 \pm d_1) b_{n-1} + \dots + c_n \pm d_n = 0,$$

and it is a consequence of the two relations

$$\begin{aligned} c_0 b_n + c_1 b_{n-1} + \dots + c_n &= 0 \\ d_0 b_n + d_1 b_{n-1} + \dots + d_n &= 0 \end{aligned}$$

which are supposed to be satisfied.

If two polynomials $F(x, b)$ and $G(x, b)$ in indeterminates x, b are equal,

$$F(x, b) = G(x, b),$$

this relation will remain true after we replace each power b^k by b_k . To prove this, we observe that $F(x, b)$ and $G(x, b)$ can be arranged in powers of b as follows:

$$\begin{aligned}
 F(x, b) &= f_0(x)b^n + f_1(x)b^{n-1} + \dots + f_n(x) \\
 G(x, b) &= g_0(x)b^n + g_1(x)b^{n-1} + \dots + g_n(x),
 \end{aligned}$$

and the equality

$$F(x, b) = G(x, b)$$

means that the coefficients of like powers of b are identical polynomials in x , so that

$$f_i(x) = g_i(x) \quad \text{for } i = 0, 1, 2, \dots, n.$$

But then it is evident that

$$f_0(x)b_n + f_1(x)b_{n-1} + \dots + f_n(x) = g_0(x)b_n + g_1(x)b_{n-1} + \dots + g_n(x)$$

regardless of the values b_1, b_2, \dots, b_n .

After these preliminary remarks we define the sequence of numbers b_1, b_2, b_3, \dots by the symbolic formula

$$(b + 1)^n - b^n = 0 \tag{A}$$

for $n > 1$. Taking $n = 2, 3, 4, \dots$, we have in nonsymbolic form

$$\begin{aligned}
 2b_1 + 1 &= 0 \\
 3b_2 + 3b_1 + 1 &= 0 \\
 4b_3 + 6b_2 + 4b_1 + 1 &= 0 \\
 \dots &\dots \dots
 \end{aligned}$$

whence

$$b_1 = -\frac{1}{2}, b_2 = \frac{1}{6}, b_3 = 0, b_4 = -\frac{1}{30}, b_5 = 0, \dots$$

Thus, the symbolic formula (A) for $n = 2, 3, 4, 5, \dots$ serves to define an infinite sequence of rational numbers $b_1, b_2, b_3, b_4, \dots$.

By Taylor's formula we have for any polynomial $f(x)$

$$f(x+b+1) - f(x+b) = f'(x) + \{(b+1)^2 - b^2\} \frac{f''(x)}{1 \cdot 2} \\ + \{(b+1)^3 - b^3\} \frac{f'''(x)}{1 \cdot 2 \cdot 3} + \dots$$

identically in the indeterminates x and b . If we replace here each power b^k by b_k and take into account the symbolic equation (A), we get the fundamental symbolic formula

$$f(x+b+1) - f(x+b) = f'(x). \quad (B)$$

This identity in x will, of course, remain true after the replacement of the indeterminate x by any number. In particular, taking $x = -1$ and $f(x) = x^n$, we obtain another symbolic formula

$$b^n - (b-1)^n = (-1)^{n-1}n$$

which, when added to (A) member by member, gives

$$(b+1)^n - (b-1)^n = (-1)^{n-1}n \quad \text{for } n > 1. \quad (C)$$

For even $n = 2k$, this amounts to

$$C_{2k}^1 b_{2k-1} + C_{2k}^3 b_{2k-3} + \dots + C_{2k}^{2k-1} b_1 = -k;$$

but $C_{2k}^{2k-1} b_1 = -k$, and so

$$C_{2k}^1 b_{2k-1} + C_{2k}^3 b_{2k-3} + \dots + C_{2k}^{2k-3} b_3 = 0$$

for $k > 1$. Taking $k = 2, 3, 4, \dots$, we have

$$4b_3 = 0$$

$$6b_5 + 20b_3 = 0$$

$$8b_7 + 56b_5 + 56b_3 = 0,$$

whence $b_3 = 0$, $b_5 = 0$, $b_7 = 0$ and, in general, $b_{2k-1} = 0$ for $k > 1$. As to the numbers

$$b_2 = \frac{1}{6}, \quad b_4 = -\frac{1}{30}, \quad b_6 = \frac{1}{42}, \quad \dots,$$

the induction shows that they alternate in sign. The general proof of this fact is not quite easy and will be given later. Assuming it to be true, the numbers

$$(-1)^{k-1}b_{2k}$$

for $k = 1, 2, 3, \dots$ are positive.

We define the Bernoullian number B_k by

$$B_k = (-1)^{k-1}b_{2k}.$$

Taking $n = 2k + 1$ in (C), we derive easily the following recurrence formula to determine B_1, B_2, B_3, \dots :

$$C_{2k+1}^2 B_1 - C_{2k+1}^4 B_2 + C_{2k+1}^6 B_3 - \dots + (-1)^{k-1} C_{2k+1}^{2k} B_k = k - \frac{1}{2},$$

whence, without much labor, one can form a small table of Bernoullian numbers:

www.dbraulibrary.org.in

$B_1 = \frac{1}{6}$	$B_6 = \frac{691}{2,730}$
$B_2 = \frac{1}{30}$	$B_7 = \frac{7}{6}$
$B_3 = \frac{1}{42}$	$B_8 = \frac{3,617}{510}$
$B_4 = \frac{1}{30}$	$B_9 = \frac{43,867}{798}$
$B_5 = \frac{5}{66}$	$B_{10} = \frac{174,611}{330}$

3. The General Expression for the Sum $S_n(N)$. Taking $x = 0, 1, 2, \dots, N - 1$ in (B) and adding the resulting symbolic relations, we get a remarkably simple symbolic expression of the sum

$$f'(0) + f'(1) + \dots + f'(N - 1) = f(N + b) - f(b)$$

good for any polynomial $f(x)$. In particular, for

$$f(x) = \frac{x^{n+1}}{n+1}$$

we have

$$S_n(N) = 1^n + 2^n + \cdots + (N-1)^n = \frac{(N+1)^{n+1} - 1^{n+1}}{n+1} \quad (D)$$

and for $n = 2k$, passing to the nonsymbolic form and introducing Bernoullian numbers,

$$S_{2k}(N) = \frac{N^{2k+1}}{2k+1} - \frac{N^{2k}}{2} + (-1)^{k-1} B_k N + (-1)^{k-2} C_{2k}^2 B_{k-1} \frac{N^3}{3} + (-1)^{k-3} C_{2k}^4 B_{k-2} \frac{N^5}{5} + \cdots + C_{2k}^{2k-2} B_1 \frac{N^{2k-1}}{2k-1} \quad (E)$$

For instance, for $k = 2, 3, 4$

$$S_4(N) = \frac{N^5}{5} - \frac{N^4}{2} + \frac{N^3}{3} - \frac{N}{30};$$

$$S_6(N) = \frac{N^7}{7} - \frac{N^6}{2} + \frac{N^5}{2} - \frac{N^3}{6} + \frac{N}{42};$$

$$S_8(N) = \frac{N^9}{9} - \frac{N^8}{2} + \frac{2N^7}{3} - \frac{7N^5}{15} + \frac{2N^3}{9} - \frac{N}{30}.$$

4. Proof That Bernoullian Numbers Are Positive. This proof is based on evaluating the sum of the n th powers of numbers contained in the following table

1	2	3	-----	N-1
2	4	6	-----	2(N-1)
3	6	9	-----	3(N-1)

N-1	2(N-1)	3(N-1)	-----	(N-1)(N-1)

in two different ways. Summing by rows, we find, as a result,

$$\begin{aligned} \Sigma &= 1^n + 2^n + \dots + (N-1)^n + 2^n(1^n + 2^n + \dots + (N-1)^n) \\ &\quad + (N-1)^n + \dots + (N-1)^n(1^n + 2^n + \dots + (N-1)^n) \\ &\quad + (N-1)^n = (1^n + 2^n + \dots + (N-1)^n)^2. \end{aligned}$$

On the other hand, numbers of the table can be arranged in $N-1$ right angles, as shown. Since the sum of the n th powers in the i th right angle is

$$2i^n(1^n + 2^n + \dots + (i-1)^n) + i^{2n},$$

another expression for Σ is

$$\Sigma = \sum_{i=1}^{N-1} [2i^n(1^n + 2^n + \dots + (i-1)^n) + i^{2n}],$$

and on equating both we get

$$\begin{aligned} \sum_{i=1}^{N-1} [2i^n(1^n + 2^n + \dots + (i-1)^n) + i^{2n}] &= (1^n + 2^n + \dots + (N-1)^n)^2. \quad (F) \end{aligned}$$

By (D)

$$1^n + 2^n + \dots + (i-1)^n = \frac{(i+b)^{n+1} - b^{n+1}}{n+1} = \phi_n(i)$$

or, in expanded form,

$$1^n + 2^n + \dots + (i-1)^n = \frac{i^{n+1}}{n+1} - \frac{i^n}{2} + \sum_{k=1}^{n-1} C_n^k b_{k+1} \cdot \frac{i^{n-k}}{k+1},$$

whence

$$\begin{aligned} 2i^n(1^n + 2^n + \dots + (i-1)^n) + i^{2n} &= \frac{2i^{2n+1}}{n+1} \\ &\quad + 2 \sum_{k=1}^{n-1} C_n^k b_{k+1} \cdot \frac{i^{2n-k}}{k+1}. \end{aligned}$$

Again, by (D)

$$\sum_{i=1}^{N-1} [2i^n(1^n + 2^n + \dots + (i-1)^n) + i^{2n}]$$

$$= \frac{2}{n+1} \phi_{2n+1}(N) + 2 \sum_{k=1}^{n-1} C_n^k b_{k+1} \frac{\phi_{2n-k}(N)}{k+1}$$

where

$$1^n + 2^n + \dots + (N-1)^n = \phi_n(N).$$

and so by (F)

$$\frac{2}{n+1} \phi_{2n+1}(N) + 2 \sum_{k=1}^{n-1} C_n^k b_{k+1} \frac{\phi_{2n-k}(N)}{k+1} = \phi_n(N)^2 \quad (G)$$

for every positive integer N . Considering N not as an integer but as an indeterminate, both members of (G) are polynomials in N . These polynomials, being equal for $N = 1, 2, 3, \dots$, must be identical, and coefficients of like powers of N in both members of (G) must be equal.

Let us compare coefficients of N^2 . In the left-hand side the coefficient of N^2 is

$$\frac{2n+1}{n+1} b_{2n} + \sum_{k=1}^{n-1} \frac{2n-k}{k+1} C_n^k b_{k+1} b_{2n-k-1}.$$

In the right-hand side it is b_n^2 , and consequently

$$\frac{2n+1}{n+1} b_{2n} + \sum_{k=1}^{n-1} \frac{2n-k}{k+1} C_n^k b_{k+1} b_{2n-k-1} = b_n^2$$

or, separating the term corresponding to $k = n-1$,

$$\frac{2n+1}{n+1} b_{2n} + \sum_{k=1}^{n-2} \frac{2n-k}{k+1} C_n^k b_{k+1} b_{2n-k-1} = -nb_n^2.$$

We can drop even values of k , since then $b_{k+1} = 0$; setting $k = 2s - 1$ and distinguishing cases of even and odd n , we have

$$\frac{2n+1}{n+1}b_{2n} + \sum_{s=1}^{(n-2)/2} \frac{2n-2s+1}{2s} C_n^{2s-1} b_{2s} b_{2n-2s} = -nb_n^2, \quad n \text{ even,}$$

and

$$\frac{2n+1}{n+1}b_{2n} + \sum_{s=1}^{(n-1)/2} \frac{2n-2s+1}{2s} C_n^{2s-1} b_{2s} b_{2n-2s} = 0, \quad n \text{ odd.}$$

Assuming now as established that $(-1)^{s-1}b_{2s} > 0$ for $s < n$, these two relations give $(-1)^{n-1}b_{2n} > 0$, and so it is shown that the Bernoullian numbers are positive.

5. Staudt's Theorem. In formula (E), Sec. 3, we choose N divisible by the denominators of the Bernoullian numbers B_1, B_2, \dots, B_{k-1} and also by $2, 3, \dots, 2k+1$. Then it is clear that the difference

$$\frac{S_{2k}(N)}{N} - (-1)^{k-1}B_k$$

is an integer. On the other hand, N is divisible by *all* primes a, b, c, \dots such that

$$\frac{2k}{a-1}, \frac{2k}{b-1}, \frac{2k}{c-1}, \dots$$

are integers and by the theorem proved in Sec. 11, Chap. VI,

$$\frac{S_{2k}(N)}{N} + \frac{1}{a} + \frac{1}{b} + \frac{1}{c} + \dots$$

is also an integer. Consequently

$$B_k = G + (-1)^k \left(\frac{1}{a} + \frac{1}{b} + \frac{1}{c} + \dots \right),$$

where G is an integer. This is the famous theorem of Staudt, which can be stated in words as follows:

The fractional part of Bernoulli's number B_k is equal to $(-1)^k$ multiplied by the sum of all fractions $1/p$ where p is a prime and $2k/(p-1)$ an integer. For example,

$$B_4 = -1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{5}; \quad B_6 = \frac{1}{6} + \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{17}.$$

Notice that 2 and 3 occur in the denominators of all Bernoullian numbers. Also these denominators contain only different primes.

6. An Auxiliary Congruence. To have formula (E) before us, we write it down again:

$$S_{2k}(N) = \frac{N^{2k+1}}{2k+1} - \frac{N^{2k}}{2} + (-1)^{k-1} B_k N + (-1)^{k-2} C_{2k}^{2k-2} B_{k-1} \frac{N^3}{3} \\ + \dots + (-1)^{k-2} C_{2k}^{2k-2} B_1 \frac{N^{2k-1}}{2k-1}. \quad (E)$$

Consider a term

$$C_{2k}^{2i} B_{k-i} \frac{N^{2i+1}}{2i+1} = N^2 C_{2k}^{2i} B_{k-i} \frac{N^{2i-1}}{2i+1}$$

with $i > 1$, and let p be a prime which divides N and possibly the denominator of B_{k-i} and $2i+1$. Let $2i+1 = p^a q$, q nondivisible by p and $a \geq 0$. Then the denominator of the fraction

$$B_{k-i} \frac{N^{2i-1}}{2i+1}$$

contains p in the degree $a+1$ at most, and p occurs in the numerator in the degree $2i-1 = p^a q - 2$ at least. Now

$$p^a q - 2 \geq a + 1 \quad \text{or} \quad p^a q \geq a + 3$$

in all cases. For if $a = 0$, then $q = 2i+1 > 3$. If $a > 0$ and $p \geq 5$, we have already

$$5^a > a + 3.$$

Likewise

$$3^a > a + 3.$$

if $a \geq 2$, and the conclusion is true for $p = 3$. Finally, if $a = 1$, $p = 3$, then $q \geq 5$, since $3q = 2i + 1 > 3$ and q is not divisible by 3; but $3 \cdot 5 = 15 > 4$. Thus the fraction

$$B_{k-1} \frac{N^{2i-1}}{2i+1},$$

when reduced to its simplest terms, has its denominator *relatively prime to N* provided $i > 1$. As to the fraction

$$B_{k-1} \frac{N}{3},$$

its denominator, in reduced form, cannot contain any prime which divides N except 3 in the first power and then only if N is divisible by 3 and not by 9. Finally, the fraction

$$\frac{N^{2k-2}}{2},$$

in reduced form, has as denominator either 1 or 2.

From this discussion it follows that under all circumstances the sum of all terms, excepting $(-1)^{k-1} B_k N$, in the right-hand side of (E), can be presented in the form

$$N^2 \frac{R}{\epsilon S},$$

where S is relatively prime to N and $\epsilon = 1, 2, 3$, or 6. Thus

$$S_{2k}(N) = (-1)^{k-1} B_k N + N^2 \frac{R}{\epsilon S}.$$

Now let us set

$$B_k = \frac{P_k}{Q_k},$$

with relatively prime P_k and Q_k , and let us multiply both members of the preceding equality by Q_k . Noticing that Q_k is divisible by 6, the result can be presented thus:

$$(-1)^{k-1} Q_k S_{2k}(N) = P_k N + N^2 \frac{T}{S},$$

where T and S are relatively prime numbers and S is prime to N . But, since

$$N^2 \frac{T}{S}$$

is an integer, S must be equal to 1, and so

$$(-1)^{k-1} Q_k S_{2k}(N) = P_k N + N^2 T$$

or

$$(-1)^{k-1} Q_k S_{2k}(N) \equiv P_k N \pmod{N^2},$$

a remarkable congruence holding for any integer N .

7. Another Auxiliary Congruence. Let a be any number prime to N , q_s and r_s the respective quotient and remainder in the division of sa by N , so that

$$sa = Nq_s + r_s; \quad q_s = \left[\frac{sa}{N} \right].$$

Raising both members of this equality to the power $2k$ and neglecting terms divisible by N^2 , we get a congruence

$$a^{2k} s^{2k} \equiv r_s^{2k} + 2kNq_s r_s^{2k-1} \pmod{N^2}$$

or, since $r_s \equiv sa \pmod{N}$,

$$a^{2k} s^{2k} \equiv r_s^{2k} + 2kNa^{2k-1} s^{2k-1} q_s \pmod{N^2}.$$

Taking here $s = 1, 2, \dots, N-1$ and remembering that r_1, r_2, \dots, r_{N-1} differ only in order from $1, 2, \dots, N-1$, we get, after summation,

$$(a^{2k} - 1)S_{2k}(N) \equiv 2kNa^{2k-1} \sum_{s=1}^{N-1} s^{2k-1} \left[\frac{sa}{N} \right] \pmod{N^2}.$$

This is the second auxiliary congruence which we need to establish a theorem, remarkable for its generality, discovered by G. Voronoi in 1889 while he was still a student.

8. Voronoi's Theorem and Its Applications. On comparing both auxiliary congruences, we get

$$N(a^{2k} - 1)P_k \equiv (-1)^{k-1}NQ_k 2ka^{2k-1} \sum_{s=1}^{N-1} s^{2k-1} \left[\frac{sa}{N} \right] \pmod{N^2}$$

or, dividing both sides and the modulus by N ,

$$(a^{2k} - 1)P_k \equiv (-1)^{k-1} 2ka^{2k-1} Q_k \sum_{s=1}^{N-1} s^{2k-1} \left[\frac{sa}{N} \right] \pmod{N}.$$

This congruence holding for an arbitrary modulus N , a being relatively prime to N , constitutes the theorem of Voronoi. Many interesting properties of Bernoullian numbers follow as easy corollaries from this theorem.

In the first place we shall prove the generalization of a property of the numerators of Bernoullian numbers observed by the famous astronomer J. C. Adams during the preparation of his valuable table of the 62 first Bernoullian numbers. Adams observed that, whenever a prime p dividing k does not enter into the denominator of Bernoulli's number B_k , it divides its numerator. Let p^ω be the highest power of p dividing k ; then, taking $N = p^\omega$ in Voronoi's congruence, we have

$$(a^{2k} - 1)P_k \equiv 0 \pmod{p^\omega},$$

provided a is not divisible by p . Now since p does not enter in Q_k , by Staudt's theorem, $2k$ is not divisible by $p - 1$. Then, if a is a primitive root of p , $a^{2k} - 1$ is not divisible by p and consequently P_k is divisible not only by p but by p^ω .

As another application we shall show that

$$\frac{a^{k+1}(a^{2k} - 1)B_k}{2k}$$

is an integer for any integer a . Let $2kQ_k = LM$ be a factorization in which M is relatively prime to a and all prime factors of L divide a . Taking $N = M$ in Voronoi's congruence, we have

$$(a^{2k} - 1)P_k \equiv 0 \pmod{M};$$

that is,

$$\frac{(a^{2k} - 1)P_k}{M}$$

is an integer. On the other hand, let p be any prime divisor of L which enters into k in the degree $\beta \geq 0$ and into $2Q_k$ in the degree 2 at most. Then p enters into L in the degree not higher than $\beta + 2$. Since p divides a , it enters into a^{k+1} at least in the degree p^β .

$$p^\beta + 1 \geq \beta + 2,$$

since already

$$2^\beta \geq \beta + 1$$

for $\beta \geq 0$. Thus

$$\frac{a^{k+1}}{L}$$

is an integer and consequently

$$\frac{a^{k+1}(a^{2k} - 1)P_k}{LM} = \frac{a^{k+1}(a^{2k} - 1)B_k}{2k}$$

is always an integer.

9. Fractions mod m . Kummer's Congruences. By a fraction $a/b \pmod{m}$, whose denominator is prime to m , we agree to understand the unique solution mod m of the congruence

$$bx \equiv a \pmod{m}.$$

From this definition the following properties of fractions mod m can be derived without any difficulty.

1. The congruence

$$\frac{a}{b} \equiv \frac{a'}{b'} \pmod{m}$$

is satisfied if and only if $ab' - a'b \equiv 0 \pmod{m}$. In particular

$$\frac{a}{b} \equiv \frac{a'}{b'} \pmod{m}$$

if $a' \equiv a, b' \equiv b \pmod{m}$. Thus, for example, $\frac{5}{3} \equiv \frac{1}{2} \pmod{7}$.

2. The fractions

$$\frac{a}{b} \pm \frac{c}{d}, \quad \frac{ac}{bd}$$

modulo m are equivalent to the fractions

$$\frac{ad \pm bc}{bd}, \quad \frac{ac}{bd}$$

whether in this or reduced form. Thus

$$\frac{2}{5} - \frac{1}{2} \equiv \frac{-1}{3} \pmod{7}, \quad \frac{6}{5} \cdot \frac{7}{12} \equiv \frac{7}{10} \equiv 4 \pmod{11}.$$

3. If

$$\frac{a}{b} \equiv \frac{a'}{b'}, \quad \frac{c}{d} \equiv \frac{c'}{d'} \pmod{m},$$

then

$$\frac{a}{b} \pm \frac{c}{d} \equiv \frac{a'}{b'} \pm \frac{c'}{d'}, \quad \frac{ac}{bd} \equiv \frac{a'c'}{b'd'} \pmod{m}.$$

4. Let $f(x)$ be a polynomial with rational coefficients whose denominators are prime to m , and let α and β be two congruent integers mod m , then

$$f(\alpha) \equiv f(\beta) \pmod{m}.$$

After these preliminary remarks, we turn to the derivation of the remarkable congruences involving Bernoullian numbers and discovered by Kummer.

E. E. Kummer (1810–1893) by his introduction of ideal divisors achieved perhaps the most significant advance in the theory of numbers since Gauss. His deep investigations of cyclotomic fields with splendid applications to higher reciprocity laws and Fermat's last theorem, of which we shall speak later, opened the way to the creation of the general theory of algebraic numbers by Kronecker, Dedekind, and Zolotareff. This was the most splendid achievement of mathematical science in the nineteenth century.

Let p be an odd prime, $\mu = (p - 1)/2$, and k nondivisible by μ . By Staudt's theorem the denominators of the Bernoullian numbers

$$B_{k+\sigma\mu}$$

are prime to p because

$$\frac{2k + \sigma\mu}{p - 1} = \frac{k}{\mu} + \sigma$$

is not an integer. Consequently, if $k + \sigma\mu$ happens to be divisible by p^g , by the generalized Adams theorem $B_{k+\sigma\mu}$ will be divisible by p^g and the fraction

$$\frac{B_{k+\sigma\mu}}{k + \sigma\mu},$$

reduced to simplest terms, will have a denominator prime to p .

When writing this fraction we shall always mean the equal fraction in simplest terms. Let p^g be the highest power of p by which one of the numbers

$$k, k + \mu, k + 2\mu, \dots, k + n\mu$$

is divisible, so that in none of these numbers p occurs in the power $> g$. Now denoting by a a number nondivisible by p and taking $N = p^{n+g}$ in Voronoi's congruence, we have

$$\begin{aligned}
 & (-1)^{k-1+\sigma\mu} (a^{2k+\sigma(p-1)} - 1) P_{k+\sigma\mu} \\
 & \equiv 2(k + \sigma\mu) Q_{k+\sigma\mu} a^{2k+\sigma(p-1)-1} \sum_{s=1}^{p^{n+\sigma}-1} s^{2k-1+\sigma(p-1)} \left[\frac{sa}{p^{n+\sigma}} \right] \pmod{p^{n+\sigma}},
 \end{aligned}$$

whence, for $\sigma = 0, 1, 2, \dots, n$,

$$\begin{aligned}
 & (-1)^{k-1+\sigma\mu} (a^{2k+\sigma(p-1)} - 1) \frac{B_{k+\sigma\mu}}{k + \sigma\mu} \\
 & \equiv 2a^{2k+\sigma(p-1)-1} \sum_{s=1}^{p^{n+\sigma}-1} s^{2k-1+\sigma(p-1)} \left[\frac{sa}{p^{n+\sigma}} \right] \pmod{p^n},
 \end{aligned}$$

the left-hand side being interpreted as a fraction mod p^n . This congruence can be further simplified by a suitable choice of a . We shall take

$$a \equiv \gamma^{p^{n-1}} \pmod{p^n},$$

denoting by γ a primitive root mod p ; then, by Euler's theorem,

$$a^{p-1} \equiv \gamma^{(p-1)p^{n-1}} \equiv 1 \pmod{p^n}$$

and

$$\begin{aligned}
 & (-1)^{k-1+\sigma\mu} (a^{2k} - 1) \frac{B_{k+\sigma\mu}}{k + \sigma\mu} \\
 & \equiv 2a^{2k-1} \sum_{s=1}^{p^{n+\sigma}-1} s^{2k-1+\sigma(p-1)} \left[\frac{sa}{p^{n+\sigma}} \right] \pmod{p^n}.
 \end{aligned}$$

Multiply these congruences by

$$(-1)^\sigma C_n^\sigma; \quad \sigma = 0, 1, 2, \dots, n$$

and add them member by member. In the right-hand side perform the first summation with regard to σ , which gives

$$\sum_{\sigma=0}^n (-1)^\sigma C_n^\sigma s^{\sigma(p-1)} = (1 - s^{p-1})^n,$$

so that the general term of the sum taken with regard to s is

$$k_s = s^{2k-1}(1 - s^{p-1})^n \left[\frac{sa}{p^{n+s}} \right].$$

Suppose now that

$$k \geq \frac{n+1}{2}.$$

Then if s is divisible by p ,

$$s^{2k-1} \equiv 0 \pmod{p^n},$$

and if s is nondivisible by p ,

$$(1 - s^{p-1})^n \equiv 0 \pmod{p^n}$$

by Fermat's theorem. Therefore, for all integers s

$$k_s \equiv 0 \pmod{p^n},$$

and consequently

$$(a^{2k} - 1) \sum_{s=0}^n (-1)^{s(\mu+1)} C_n^s \frac{B_{k+s\mu}}{k+s\mu} \equiv 0 \pmod{p^n}.$$

But $a^{2k} - 1$ is not divisible by p , a being a primitive root mod p , and so finally we obtain Kummer's general congruence

$$\sum_{s=0}^n (-1)^{s(\mu+1)} C_n^s \frac{B_{k+s\mu}}{k+s\mu} \equiv 0 \pmod{p^n},$$

valid if $k \geq (n+1)/2$ and $2k$ is nondivisible by $p-1$. For $n=1, 2, 3$ in particular, we have

$$\frac{B_k}{k} - (-1)^\mu \frac{B_{k+\mu}}{k+\mu} \equiv 0 \pmod{p}$$

$$\frac{B_k}{k} - 2(-1)^\mu \frac{B_{k+\mu}}{k+\mu} + \frac{B_{k+2\mu}}{k+2\mu} \equiv 0 \pmod{p^2}$$

$$\frac{B_k}{k} - 3(-1)^\mu \frac{B_{k+\mu}}{k+\mu} + 3 \frac{B_{k+2\mu}}{k+2\mu} - (-1)^\mu \frac{B_{k+3\mu}}{k+3\mu} \equiv 0 \pmod{p^3},$$

the last two congruences requiring $k \geq 2$. For example, let us take $p = 5$, $k = 3$. Then

$$\frac{B_3}{3} = \frac{1}{126} \equiv 1 \pmod{125}, \quad \frac{B_5}{5} = \frac{1}{66} \equiv \frac{1}{16} \pmod{25},$$

$$\frac{B_7}{7} \equiv \frac{1}{6} \pmod{25}$$

and

$$\frac{B_3}{3} - 2\frac{B_5}{5} + \frac{B_7}{7} \equiv 1 - \frac{1}{8} + \frac{1}{6} \equiv \frac{25}{24} \equiv 0 \pmod{25},$$

as it should be.

Exercises and Problems

1. If a and b are two relatively prime numbers, then

$$\frac{(a^{2k} - 1)(b^{2k} - 1)B_k}{2k}$$

is always an integer.

www.dbraulibrary.org.in

2. Prove that for an odd prime p

$$pB_{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}.$$

HINT: Use the auxiliary congruence in Sec. 6.

3. Show that for an odd prime p

$$1^{p-2} + 2^{p-2} + \dots + \left(\frac{p-1}{2}\right)^{p-2} \equiv (-1)^{\frac{p+1}{2}} (2^p - 2)B_{\frac{p-1}{2}} \pmod{p}.$$

HINT: Notice that

$$\frac{2^p - 2}{p} \equiv 1 - \frac{1}{2} + \frac{1}{3} - \dots - \frac{1}{p-1} \pmod{p}.$$

4. Integers

$$T_k = \frac{2^{2k}(2^{2k} - 1)B_k}{2k}$$

occur in the expansion

$$\tan x = T_1 \frac{x}{1!} + T_2 \frac{x^3}{3!} + T_3 \frac{x^5}{5!} + \dots$$

and are called "tangent coefficients." By an appropriate application of the Voronoi congruence, prove that

$$T_{k+\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} T_k \pmod{p}$$

for a prime p .

5. Taking $a = 3, 4, 6$ in Voronoi's congruence, prove that for a prime $p > 3$

$$\frac{1 - 3^{p-2k} - 4^{p-2k} + 6^{p-2k}}{4k} (-1)^k B_k \equiv \sum_{s=[p/6]+1}^{[p/4]} s^{2k-1} \pmod{p}$$

if $2k$ is nondivisible by $p-1$.

6. In a similar manner prove also that

$$\frac{1 - 2^{p-2k} - 3^{p-2k} + 4^{p-2k}}{4k} (-1)^k B_k \equiv \sum_{s=[p/4]+1}^{[p/3]} s^{2k-1} \pmod{p}$$

$$\frac{1 - 4^{p-2k} - 5^{p-2k} + 8^{p-2k}}{4k} (-1)^k B_k \equiv \sum_{s=[p/8]+1}^{[p/5]} s^{2k-1} + \sum_{s=[3p/8]+1}^{[2p/5]} s^{2k-1} \pmod{p}$$

under the same hypothesis concerning k .

7. Prove that

$$\sum_{s=1}^{p^2-1} s^{2\nu p-1} \left[\frac{2s}{p^2} \right] \equiv - \sum_{\rho=1}^{(p-1)/2} \rho^{2\nu p-1} \pmod{p^2}$$

if $\nu-1$ is not divisible by $\frac{1}{2}(p-1)$. Hence, and from Voronoi's congruence, deduce that in case 2ν is not divisible by $p-1$ and ν by p

$$(2^{2\nu p} - 1) \frac{(-1)^{\nu p-1} B_{\nu p}}{2\nu p} \equiv -2^{2\nu p-1} \sum_{\rho=1}^{(p-1)/2} \rho^{2\nu p-1} \pmod{p^2}.$$

8. The symbolic equation

$$(e + 1)^n + (e - 1)^n = 0$$

for $n \geq 1$ determines the sequence of integers

$$e_1 = 0, \quad e_2 = -1, \quad e_3 = 0, \quad e_4 = 5, \dots$$

In general $e_{2k-1} = 0$ and $(-1)^k e_{2k} = E_k$ are positive integers called Eulerian numbers or "secant coefficients" since they occur in the expansion

$$\sec x = 1 + E_1 \frac{x^2}{1 \cdot 2} + E_2 \frac{x^4}{1 \cdot 2 \cdot 3 \cdot 4} + \dots$$

Show that for any polynomial $f(x)$

$$f(x + e + 1) + f(x + e - 1) = 2f(x)$$

symbolically, and hence deduce that

$$f(1) - f(3) + f(5) - \dots + (-1)^{x-1} f(2x - 1) \\ = \frac{1}{2} \{ f(e) + (-1)^{x-1} f(e + 2x) \}.$$

9. For an odd x the following congruence holds.

$$1^{2n} - 3^{2n} + 5^{2n} - \dots + (2x - 1)^{2n} \equiv (-1)^n E_n \pmod{x^2}.$$

Hence deduce that for an odd prime p

$$(a) \quad E_{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} E_n \pmod{p}$$

$$(b) \quad E_{\frac{p-1}{2}} \equiv 0 \pmod{p} \quad \text{if} \quad p \equiv 1 \pmod{4}$$

$$(c) \quad E_{\frac{p-1}{2}} \equiv -2 \pmod{p} \quad \text{if} \quad p \equiv 3 \pmod{4}.$$

10. Show that symbolically

$$e^{2n} + (e + 2)^{2n} = 2,$$

and hence deduce the congruence

$$(-1)^n E_n \equiv 1 + 2^{i+1} \pmod{2^{i+2}}$$

if $n = 2^i m$ and m is odd.

CHAPTER X

QUADRATIC RESIDUES

1. Definition of Quadratic Residues. Though we have already had occasion to touch lightly upon the subject of quadratic residues in Sec. 12, Chap. VII, it is in this chapter that we propose to deal with it extensively, beginning with the very first elements and developing the whole theory *ab initio* without reference to previously established results.

A number a is said to be a quadratic residue of another number m if the congruence

$$x^2 \equiv a \pmod{m}$$

can be satisfied by some integer x . If this congruence is impossible, a is said to be a quadratic nonresidue of m . It is convenient sometimes to have an abbreviated expression to denote whether a is a quadratic residue or nonresidue of m , so, with Gauss, we shall designate the first alternative by aRm and the second by aNm , the letters R and N being the initials of the Latin words *Residuum* and *Nonresiduum*. The case of a prime modulus, as we shall see, is of paramount importance; hence, until further notice, the modulus will be supposed to be a prime number.

2. Prime Moduli. Zero is a trivial quadratic residue of any modulus and henceforth will be excluded from consideration. As congruent numbers are at the same time quadratic residues or nonresidues, we may confine ourselves, for a prime modulus p , to the numbers

$$1, 2, 3, \dots, p - 1.$$

For $p = 2$ there is only one quadratic residue; the number 1.

To find all the distinct quadratic residues for an odd prime modulus it suffices to consider the squares

$$1^2, 2^2, \dots, (p-1)^2,$$

reduce them to their least positive residues, and among these retain only the distinct ones. Since

$$(p-i)^2 \equiv i^2 \pmod{p},$$

it is clear that all quadratic residues will be found among the least positive residues of the numbers

$$1^2, 2^2, \dots, \left(\frac{p-1}{2}\right)^2$$

Now no two of these numbers are congruent modulo p , for the congruence

$$x'^2 \equiv x^2 \pmod{p}$$

implies either

$$x' - x \equiv 0 \pmod{p}$$

and then $x' = x$, since x' and x are both positive and $< p/2$, or

$$x' + x \equiv 0 \pmod{p}$$

which is impossible since $0 < x' + x \leq p-1$. Thus the least positive residues of the squares

$$1^2, 2^2, \dots, \left(\frac{p-1}{2}\right)^2$$

are all different. Hence there are exactly $\frac{p-1}{2}$ quadratic residues for an odd prime p and, consequently, exactly as many quadratic nonresidues.

Example. Let $p = 11$. To find all the quadratic residues of 11, reduce the squares

$$1^2 = 1, \quad 2^2 = 4, \quad 3^2 = 9, \quad 4^2 = 16, \quad 5^2 = 25$$

to their least positive residues mod 11. The resulting numbers, arranged in order of their magnitude,

1, 3, 4, 5, 9

are quadratic residues of 11, and

2, 6, 7, 8, 10

are quadratic nonresidues.

Here we give a table of the quadratic residues and non-residues of primes not exceeding 29:

$$p = 3 \begin{array}{l} R \ 1 \\ N \ 2 \end{array}$$

$$p = 5 \begin{array}{l} R \ 1, 4 \\ N \ 2, 3 \end{array}$$

$$p = 7 \begin{array}{l} R \ 1, 2, 4 \\ N \ 3, 5, 6 \end{array}$$

$$p = 11 \begin{array}{l} R \ 1, 3, 4, 5, 9 \\ N \ 2, 6, 7, 8, 10 \end{array}$$

$$p = 13 \begin{array}{l} R \ 1, 3, 4, 9, 10, 12 \\ N \ 2, 5, 6, 7, 8, 11 \end{array}$$

$$p = 17 \begin{array}{l} R \ 1, 2, 4, 8, 9, 13, 15, 16 \\ N \ 3, 5, 6, 7, 10, 11, 12, 14 \end{array}$$

$$p = 19 \begin{array}{l} R \ 1, 4, 5, 6, 7, 9, 11, 16, 17 \\ N \ 2, 3, 8, 10, 12, 13, 14, 15, 18 \end{array}$$

$$p = 23 \begin{array}{l} R \ 1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18 \\ N \ 5, 7, 10, 11, 14, 15, 17, 19, 20, 21, 22 \end{array}$$

$$p = 29 \begin{array}{l} R \ 1, 4, 5, 6, 7, 9, 13, 16, 20, 22, 23, 24, 25, 28 \\ N \ 2, 3, 8, 10, 11, 12, 14, 15, 17, 18, 19, 21, 26, 27 \end{array}$$

3. Quadratic Residuosity of a Product. The product of two quadratic residues is also a quadratic residue. For, if R and

R' are both quadratic residues, the congruences

$$x^2 \equiv R, \quad x'^2 \equiv R' \pmod{p}$$

are satisfied by some integers x and x' . But then the congruence

$$y^2 \equiv RR' \pmod{p}$$

is satisfied by $y \equiv xx'$ and so RR' is a quadratic residue.

The product of a residue R by a nonresidue N is a quadratic nonresidue. For suppose that RN is a residue; then the congruence

$$z^2 \equiv RN \pmod{p}$$

is satisfied by some integer z . Also

$$R \equiv x^2 \pmod{p}$$

for some integer x and

$$z^2 \equiv Nx^2 \pmod{p}.$$

Let y be determined by the congruence

$$xy \equiv 1 \pmod{p}.$$

On multiplying both sides of the preceding congruence by y^2 , we get

$$N \equiv (zy)^2 \pmod{p}$$

contrary to the hypothesis that N is a nonresidue. Consequently NR is a quadratic nonresidue.

If R, R', R'', \dots are all quadratic residues and N some quadratic nonresidue, then the $(p-1)/2$ numbers

$$NR, NR', NR'', \dots \quad (A)$$

are $(p-1)/2$ incongruent quadratic nonresidues. Since there are exactly $(p-1)/2$ quadratic nonresidues, each of them is congruent to one and only one of the numbers (A).

This remark enables us to prove in a very simple way that the product of two nonresidues N' and N'' is always a quadratic residue. For

$$N' \equiv NR', \quad N'' \equiv NR'' \pmod{p}$$

for some choice of residues R' and R'' . Then

$$N'N'' \equiv N^2(R'R'') \pmod{p};$$

but N^2 and $R'R''$ are residues, and so is their product; consequently $N'N''$ is a quadratic residue.

By virtue of these theorems the quadratic residuality of a number represented as a product of factors can be inferred from the quadratic residuality of its factors.

4. Euler's Criterion. It has been proved already that a number a is a quadratic residue or nonresidue of a prime p according as

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

or

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

This important theorem, known as Euler's criterion, can be proved independently as follows. To any number r in the series

$$1, 2, 3, \dots, p-1 \tag{A}$$

corresponds in the same series a unique number s such that

$$rs \equiv a \pmod{p}. \tag{B}$$

The numbers r and s are different if a is a quadratic non-residue. In this case all numbers (A) can be paired in $(p-1)/2$ pairs r, s satisfying congruence (B). Taking the product of all congruences (B), for all $(p-1)/2$ pairs, we

get in the left-hand side the product of all numbers $1, 2, \dots, p - 1$; hence

$$a^{\frac{p-1}{2}} \equiv 1 \cdot 2 \cdot 3 \cdots (p - 1) \pmod{p} \quad (C)$$

if $a \not\equiv p$. If $a \equiv p$, then the numbers r and s can be equal only if

$$r^2 \equiv a \pmod{p}.$$

This congruence is possible and has two roots; if one of them, taken in the series (A), is c , the other will be $p - c$. If we exclude, therefore, from the series (A) the two numbers c and $p - c$, the remaining $p - 3$ numbers can be combined in $(p - 3)/2$ pairs r, s satisfying the congruence (B). Taking the product of all these congruences, the left-hand side will be the product of all the numbers $1, 2, \dots, p - 1$, *excluding* c and $p - c$, while the right-hand side is $a^{\frac{p-3}{2}}$; consequently

$$1 \cdot 2 \cdot 3 \cdots (p - 1) \equiv a^{\frac{p-3}{2}} c(p - c) \pmod{p}.$$

But

$$c(p - c) \equiv -c^2 \equiv -a \pmod{p},$$

and so

$$a^{\frac{p-1}{2}} \equiv -1 \cdot 2 \cdot 3 \cdots (p - 1) \pmod{p} \quad (D)$$

if $a \not\equiv p$. Now $a = 1$ is a quadratic residue; it follows then from (D) that

$$1 \cdot 2 \cdot 3 \cdots (p - 1) \equiv -1 \pmod{p},$$

which is Wilson's theorem.

The congruences (C) and (D) can be presented thus:

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

if $a \not\equiv p$, and

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

if aRp , which is equivalent to Euler's criterion. Since every number nondivisible by p is either a residue or nonresidue of p , it follows that

$$a^{p-1} \equiv \left(\frac{p-1}{a^2} \right)^2 \equiv 1 \pmod{p}$$

for a nondivisible by p , which is Fermat's theorem. This proof of Euler's criterion is due to Dirichlet.

Peter Gustav Dirichlet (1805–1859), famous as the originator of analytic methods in number theory, was one of the great masters of this science in the nineteenth century. Indirectly by his work and directly as an excellent teacher, Dirichlet exercised a great influence on the development of the theory of numbers, especially in Germany. His lectures on number theory have been collected and published by Dedekind under the title: "Vorlesungen über Zahlentheorie" (fourth edition, 1894). This book is considered, and rightly so, one of the best textbooks on the theory of numbers ever published.

5. Legendre's Symbol. Legendre introduced into the theory of numbers a very useful symbol to express the "quadratic character" of numbers with regard to a prime modulus. If a is not divisible by a prime p , Legendre's symbol, or symbol of quadratic character,

$$\left(\frac{a}{p} \right)$$

denotes $+1$ if aRp and -1 if aNp . Since by Euler's criterion

$$a^{\frac{p-1}{2}} \equiv 1 \quad \text{or} \quad \equiv -1 \pmod{p}$$

according as aRp or aNp , Legendre's symbol is uniquely defined by the congruence

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p} \right) \pmod{p}.$$

From this definition the following simple properties of Legendre's symbol can be derived immediately:

1. $(a'/p) = (a/p)$ if $a' \equiv a \pmod{p}$.
2. $(aa'/p) = (a/p)(a'/p)$.
3. $(c^2/p) = 1$. In particular, $(1/p) = 1$.
4. $(-1/p) = (-1)^{\frac{p-1}{2}}$.

The second property is the condensed statement of the theorem in Sec. 3. Property 4 is an important theorem in itself. It amounts to the following statement: for primes of the form $p = 4n + 1$,

$$\left(\frac{-1}{p}\right) = +1$$

and for primes of the form $p = 4n + 3$,

$$\left(\frac{-1}{p}\right) = -1.$$

In other words -1 is a quadratic residue of primes $\equiv 1 \pmod{4}$ and a quadratic nonresidue of primes $\equiv 3 \pmod{4}$.

Adrien Marie Legendre (1752-1833), in the field of number theory, was an immediate successor to Euler and Lagrange. Legendre published the first treatise on number theory, "Essai sur la théorie des nombres," in 1798. In this he gives a full account of the work of Euler and Lagrange, completed by his own discoveries. Though far surpassed by the "Disquisitiones arithmeticae" of Gauss, Legendre's book enjoyed great popularity and was reprinted with improvements and additions twice: in 1808 and 1830. The last edition appeared in two volumes under the title "Théorie des nombres."

6. Fundamental Problems. The whole theory of quadratic residues reduces to two fundamental problems:

1. Is a given number a a quadratic residue or nonresidue of a given prime p ?
2. For what prime moduli p is a given number a a quadratic residue or nonresidue?

The first problem in principle is solved by Euler's criterion, though this solution is not practicable for large primes. The second problem is by far the more difficult. It took nearly half of a century of effort by men like Euler, Lagrange, and Legendre before the first complete solution was given by Gauss. And remarkably enough the principles on which the solution of the second fundamental problem depends shed a new light on the first, and they supply a really practical way of solving it.

7. Quadratic Character of -1 and 2 . For $a = -1$ the solution of the second fundamental problem follows immediately from Euler's criterion: -1 is a residue of primes of the form $4n + 1$ and a nonresidue of primes of the form $4n + 3$. For $a = 2$, Euler's criterion fails to supply any information about primes in regard to which 2 is a residue or nonresidue, though induction reveals the following simple rule:

2 is a residue of primes of the form $8n + 1$ or $8n + 7$;

2 is a nonresidue of primes of the form $8n + 3$ or $8n + 5$.

This was known already to Fermat but was not proved until a century later by Euler and Lagrange. Though the proposition was hard for the first pioneers to prove, we now possess many simple proofs. Perhaps the following one, due to Stieltjes, is the simplest.

Write down the numbers $1, 2, 3, \dots, p - 1$ in their natural order and place above each number the sign $+$ or $-$, according as it is a residue or nonresidue. When in the succession of signs thus obtained two consecutive signs are alike, we say that there is a permanence; and when they are different, we say that there is a variation. Thus, for example, for $p = 13$ we have

+	-	+	+	-	-	-	-	+	+	-	+
1,	2,	3,	4,	5,	6,	7,	8,	9,	10,	11,	12.

The series of signs presents six variations and five permanences. To determine the number of variations and permanences in general, we observe that the signs corresponding to two consecutive numbers a and $a + 1$ present a variation or permanence according as z , determined by the congruence

$$az \equiv a + 1 \pmod{p} \tag{A}$$

is a quadratic nonresidue or residue. For, by Sec. 3, if z is a nonresidue, az or $a + 1$ will be nonresidue or residue according as a is residue or nonresidue. Similarly, if z is a residue, az will be a residue or nonresidue according as a is residue or nonresidue. Now if a runs through the $p - 2$ numbers $1, 2, \dots, p - 2$, the solution z of the congruence (A) will run through $p - 2$ distinct mod p numbers. For the two congruences

$$z \equiv 1 + \frac{1}{a}, \quad z \equiv 1 + \frac{1}{a'} \pmod{p}$$

require

$$\frac{1}{a} - \frac{1}{a'} \equiv \frac{a' - a}{aa'} \equiv 0 \pmod{p}$$

or $a' - a \equiv 0$, which is possible only if $a' = a$. Since z assumes $p - 2$ incongruent values and $z \equiv 1$ does not occur among them, values of z corresponding to $a = 1, 2, \dots, p - 2$ will form some permutation of the numbers

$$2, 3, \dots, p - 1. \tag{B}$$

The series of signs will present, therefore, as many variations as there are nonresidues in the series (B); that is, $(p - 1)/2$, and as many permanences as there are residues in the same series; that is, $(p - 3)/2$, since 1, missing from (B), is a residue.

Thus the number of variations is $V = \frac{p - 1}{2}$. If $p = 4n + 1$, this number will be even and, since \dagger stands above 1,

the same sign stands above $p - 1$; that is, $p - 1$ or -1 is a residue. If $p = 4n + 3$, the number of variations will be odd, and consequently the sign placed above $p - 1$ is $-$, which means that $p - 1$ or -1 is a nonresidue. Thus, independently of Euler's criterion, it is proved again that

- -1 is a residue of primes of the form $4n + 1$;
- -1 is a nonresidue of primes of the form $4n + 3$.

The series

$$1, 2, 3, \dots, p - 1$$

can be divided into two halves,

$$1, 2, 3, \dots, \frac{p-1}{2}$$

$$\frac{p+1}{2}, \frac{p+3}{2}, \dots, p - 1,$$

and the numbers of the second half are, respectively, congruent mod p to

$$-\frac{p-1}{2}, -\frac{p-3}{2}, \dots, -2, -1.$$

The number of variations corresponding to the series

$$-1, -2, \dots, -\frac{p-1}{2}$$

is the same as that for the series

$$1, 2, \dots, \frac{p-1}{2}.$$

For, if of two numbers $a, a + 1$, one is a residue and the other a nonresidue, the same will be true of the numbers $-a, -a - 1$. Consequently the number of variations in both halves,

$$1, 2, \dots, \frac{p-1}{2}$$

$$\frac{p+1}{2}, \frac{p+3}{2}, \dots, p - 1,$$

is the same; call it Z . The number of variations in the series

$$1, 2, \dots, \frac{p-1}{2}, \frac{p+1}{2}, \dots, p-1$$

will be

$$2Z + \epsilon,$$

where $\epsilon = 0$ if corresponding to $(p-1)/2, (p+1)/2$ we have a permanence, and $\epsilon = 1$ if we have a variation. Equating it to $(p-1)/2$ we find

$$Z = \frac{p-1-2\epsilon}{4}.$$

In case $p \equiv 1 \pmod{4}$, both

$$\frac{p-1}{2} \quad \text{and} \quad \frac{p+1}{2} = p - \frac{p-1}{2}$$

are residues or nonresidues at the same time, since -1 is a residue and then $\epsilon = 0$. In case $p \equiv 3 \pmod{4}$, one of these numbers is a residue and the other a nonresidue, because in this case -1 is a nonresidue; consequently $\epsilon = 1$. Thus

$$Z = \frac{p-1}{4} \quad \text{if} \quad p \equiv 1 \pmod{4};$$

$$Z = \frac{p-3}{4} \quad \text{if} \quad p \equiv 3 \pmod{4}.$$

If $p = 8n + 1$, then Z is even; but Z is odd if $p = 8n + 5$. Correspondingly, the number of variations for the series

$$1, 2, \dots, \frac{p-1}{2}$$

is even and odd. That is,

$$\frac{p-1}{2}Rp \quad \text{if} \quad p = 8n + 1;$$

$$\frac{p-1}{2}Np \quad \text{if} \quad p = 8n + 5.$$

Because $p - 1 = 2(p - 1)/2$ in both cases is a residue, 2 will be a residue of primes of the form $8n + 1$ and a nonresidue of primes of the form $8n + 5$.

Passing to primes $\equiv 3 \pmod{4}$, we distinguish two forms mod 8: $p = 8n + 3$ and $p = 8n + 7$. Corresponding to these forms, Z is even and odd, and

$$\frac{p-1}{2}Rp \quad \text{if} \quad p = 8n + 3;$$

$$\frac{p-1}{2}Np \quad \text{if} \quad p = 8n + 7.$$

But now $p - 1 = 2(p - 1)/2$ is a nonresidue; correspondingly, 2 is a nonresidue of primes $p = 8n + 3$ and a residue of primes $p = 8n + 7$.

Theorems concerning the quadratic characters of -1 and 2 can be presented in a condensed form by using Legendre's symbol. Noticing that $(p-1)/2$ is even or odd according as $p \equiv 1$ or $p \equiv 3 \pmod{4}$, we have

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

Again, $(p^2 - 1)/8$ is even or odd according as $p \equiv \pm 1$ or $p \equiv \pm 3 \pmod{8}$; hence, for all primes

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

As to the quadratic character of -2 , it results from the formula

$$\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{2} + \frac{p^2-1}{8}}.$$

Distinguishing the four forms of $p \pmod{8}$: $p = 8n + 1$, $8n + 3$, $8n + 5$, $8n + 7$, we conclude that

-2 is a residue of primes $p = 8n + 1$ or $8n + 3$;

-2 is a nonresidue of primes $p = 8n + 5$ or $8n + 7$.

Exercises and Problems

1. If a and b are two numbers nondivisible by a prime p , then either all three congruences

$$x^2 \equiv a, \quad x^2 \equiv b, \quad x^2 \equiv ab \pmod{p}$$

are solvable or only one of them is.

2. Show that the congruence

$$x^6 + 7x^4 - 40x^2 - 100 \equiv 0 \pmod{p}$$

is solvable for any prime p .

3. Denote by (RR) , (RN) , (NR) , (NN) the number of sequences

residue—residue
residue—nonresidue
nonresidue—residue
nonresidue—nonresidue

in the series $1, 2, 3, \dots, p-1$. Show that

$$(RR) = \frac{p-4 - (-1)^{\frac{p-1}{2}}}{4}, \quad (NN) = \frac{p-2 + (-1)^{\frac{p-1}{2}}}{4};$$

$$(RN) = \frac{p - (-1)^{\frac{p-1}{2}}}{4}, \quad (NR) = \frac{p-2 + (-1)^{\frac{p-1}{2}}}{4}.$$

HINT:

$$\sum_{x=1}^{p-2} \left\{ \left(\frac{x}{p} \right) + \left(\frac{x+1}{p} \right) \right\} = 2(RR) - 2(NN), \quad \sum_{x=1}^{p-2} \left\{ \left(\frac{x}{p} \right) - \left(\frac{x+1}{p} \right) \right\} = 2(RN) - 2(NR).$$

4. Referring to the preceding problem, show that the congruence

$$x^2 + y^2 + 1 \equiv 0 \pmod{p}$$

can be satisfied by integers x, y for any prime p .

5. The sum of the quadratic residues for a prime $p \equiv 1 \pmod{4}$ is $\frac{1}{4}p(p-1)$. Hence deduce

$$[\sqrt{p}] + [\sqrt{2p}] + \dots + \left[\sqrt{\frac{p-1}{4}p} \right] = \frac{p^2 - 1}{12}.$$

6. It is true, though the proof requires analytical methods, that the sum of the quadratic residues in the series $1, 2, \dots, p-1$ for a prime $p \equiv 3 \pmod{4}$ is always less than the sum of the quadratic nonresidues. Taking this for granted, prove the inequality

$$[\sqrt{p}] + [\sqrt{2p}] + \dots + \left[\sqrt{\frac{p-3}{4}p} \right] < \frac{(p-1)(p-2)}{12}.$$

7. Let a and b denote indefinitely the quadratic residues and nonresidues of the prime p in the series $1, 2, \dots, p-1$. Show that for $p \equiv 3 \pmod{4}$

$$\left\{ 2 - \left(\frac{2}{p} \right) \right\} \frac{\sum b - \sum a}{p} = \sum_{\alpha=1}^{\frac{p-1}{2}} \left(\frac{\alpha}{p} \right).$$

HINT:

$$\sum b - \sum a = - \sum_{x=1}^{\frac{p-1}{2}} \left(\frac{x}{p} \right) x,$$

and α together with $p - 2\alpha$ exhaust all the numbers $1, 2, \dots, p-1$ for $\alpha = 1, 2, \dots, \frac{p-1}{2}$.

8. Show that there are infinitely many primes of each of the forms $8n+1, 8n+3, 8n+5, 8n+7$. HINT: $4P^2+1$, for an odd P , is divisible by some prime $\equiv 5 \pmod{8}$; $2P^2+1$ is divisible by some prime $\equiv 3 \pmod{8}$; $8Q^2-1$ for any Q is divisible by some prime $\equiv 7 \pmod{8}$. For primes of the form $8n+1$, see Problem 4, Sec. 3, Chap. VIII.

8. **Quadratic Reciprocity Law.** The general solution of the second fundamental problem in the theory of quadratic residues depends on a theorem of great simplicity and elegance which, despite its simple appearance, expresses a deep property of numbers. This theorem was discovered by Euler and published in 1783 in a complete form as a result of extensive induction. Euler states the theorem in a rather complicated form, as follows:

Denoting by s any prime number, let us divide the odd squares $1, 9, 25, 49, \dots, (s-2)^2$ by $4s$ and denote the

remainders, all of the form $4k + 1$, by a . Other numbers of the same form as the remainders, and less than $4s$, we shall indicate by A . Then,

For primes of the form	We have
$4ns + a$	s a residue, $-s$ a residue
$4ns - a$	s a residue, $-s$ a nonresidue
$4ns + A$	s a nonresidue, $-s$ a nonresidue
$4ns - A$	s a nonresidue, $-s$ a residue

To illustrate this theorem, let us take $s = 5$. Dividing the odd squares

$$1, 9$$

by 20, we have only the following remainders:

$$a = 1, 9.$$

Other numbers of the form $4k + 1$ less than 20 are
www.dbraultlibrary.org.in
 $A = 13, 17.$

Hence 5 is a quadratic residue of primes of the form

$$20n + 1, 20n - 1, 20n + 9, 20n - 9$$

and a quadratic nonresidue of primes of the form

$$20n + 13, 20n - 13, 20n + 17, 20n - 17,$$

these eight forms containing all the odd primes.

In 1785 Legendre rediscovered the same theorem and by means of his symbol put it in this elegant form: for any two odd primes p, q ,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

Because of the symmetry of this relation in regard to p and q , Legendre gave the name "reciprocity law" to this remarkable

theorem and was the first to prove at least a part of it. In proving other parts, Legendre assumed without proof the existence of certain auxiliary primes. He assumed, namely, that for any prime r of the form $8n + 1$ there is another prime of the form $4n + 3$ of which r is a quadratic nonresidue. This is true, but so far has been proved only by analytical methods which were unknown at the time of Legendre.

Without any knowledge of the previous work by Euler and Legendre, Gauss in 1795, at the age of eighteen, discovered, again by induction, the reciprocity law of Legendre. A whole year passed before Gauss could prove it completely. "It tortured me," says Gauss, "for the whole year and eluded the most strenuous efforts before, finally, I got the proof explained in the fourth section of the 'Disquisitiones arithmeticae'." The reciprocity law was presented by Gauss in the simplest imaginable form, which we shall adopt here.

RECIPROCITY LAW. *A prime p is a quadratic residue or nonresidue of another prime q according as $(-1)^{\frac{q-1}{2}}$ q is a residue or a nonresidue of p .*

Later Gauss found six more totally different proofs, and the subsequent development of number theory brought the number of different proofs to more than 50. All of them are based, however, on more or less the same principles as the seven Gaussian proofs. We shall give here the fifth proof of Gauss, perhaps the shortest and simplest of all. It is based on a remarkable transformation of Euler's criterion which is known as the "Lemma of Gauss."

9. The Lemma of Gauss. Consider the $\frac{1}{2}(p - 1)$ multiples

$$a, 2a, 3a, \dots, \frac{p-1}{2}a \quad (A)$$

of a number a nondivisible by a prime p . Some of the least positive residues mod p of these multiples are less than $\frac{1}{2}p$ and

some are greater than $\frac{1}{2}p$. Call the number of the latter μ ; then

$$\left(\frac{a}{p}\right) = (-1)^\mu.$$

To prove this assertion, let

$$\alpha_1, \alpha_2, \dots, \alpha_r \tag{B}$$

be those least positive residues of the numbers (A) which are $< \frac{1}{2}p$, while

$$p - \beta_1, p - \beta_2, \dots, p - \beta_\mu$$

are the least positive residues $> \frac{1}{2}p$, so that $\beta_1, \beta_2, \dots, \beta_\mu$ are all $< \frac{1}{2}p$. Clearly, series (B) consists of different numbers, and so does the series

$$\beta_1, \beta_2, \dots, \beta_\mu. \tag{C}$$

Moreover, none of the numbers (B) occurs in (C). For the equality $\alpha_r = \beta_s$ implies the congruences

$$ia \equiv \alpha_r, \quad ja \equiv -\alpha_r \pmod{p},$$

with i and j both positive and less than $\frac{1}{2}p$, from which an impossible congruence

$$(i + j)a \equiv 0 \pmod{p}$$

follows, because neither a nor $i + j < p$ is divisible by p .

The numbers (B) and (C) together make up $\mu + \nu = (p - 1)/2$ numbers all less than $\frac{1}{2}p$ and all different; hence

$$\alpha_1, \alpha_2, \dots, \alpha_r; \quad \beta_1, \beta_2, \dots, \beta_\mu$$

coincide with

$$1, 2, \dots, \frac{p-1}{2},$$

only taken in a different order. Now

$$a \cdot 2a \cdot 3a \cdots \frac{p-1}{2}a \equiv 1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2} a^{\frac{p-1}{2}}$$

$$\equiv \alpha_1 \alpha_2 \cdots \alpha_\nu (p - \beta_1)(p - \beta_2) \cdots (p - \beta_\mu) \pmod{p}$$

or

$$1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2} a^{\frac{p-1}{2}} \equiv (-1)^\mu \alpha_1 \alpha_2 \cdots \alpha_\nu \beta_1 \beta_2 \cdots \beta_\mu$$

$$\equiv (-1)^\mu \cdot 1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2} \pmod{p},$$

whence

$$a^{\frac{p-1}{2}} \equiv (-1)^\mu \pmod{p}.$$

On the other hand,

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p},$$

and so

$$\left(\frac{a}{p}\right) \equiv (-1)^\mu \pmod{p}.$$

But $\left(\frac{a}{p}\right)$ and $(-1)^\mu$ are units ± 1 , and units congruent for an odd modulus must be equal. Thus the lemma of Gauss, stating that

$$\left(\frac{a}{p}\right) = (-1)^\mu,$$

is proved.

10. Proof of the Reciprocity Law. Let p and q be two different odd primes. By Gauss's lemma,

$$\left(\frac{q}{p}\right) = (-1)^\mu, \quad \left(\frac{p}{q}\right) = (-1)^\nu,$$

where μ and ν are the numbers of those multiples of q and p in the series

$$q, 2q, 3q, \dots, \frac{p-1}{2}q \quad (A)$$

$$p, 2p, 3p, \dots, \frac{q-1}{2}p, \quad (B)$$

whose least positive residues are, respectively, greater than $\frac{1}{2}p$ and $\frac{1}{2}q$. To prove the reciprocity law in the form given to it by Legendre:

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}},$$

it suffices to show that

$$\mu + \nu \equiv \frac{p-1}{2} \cdot \frac{q-1}{2} \pmod{2}.$$

Now this property can be established not only for two distinct odd primes p, q but for two odd relatively prime p and q , both > 1 . This can be shown in a great many ways; the fifth Gaussian proof proceeds as follows.

The least positive residue of any number mod p either is 0 or belongs to one of the series

$$1, 2, 3, \dots, \frac{p-1}{2} \quad (f)$$

$$\frac{p+1}{2}, \frac{p+3}{2}, \dots, p-1. \quad (f')$$

Modulo q the least positive residue is either 0 or belongs to one of the series

$$1, 2, 3, \dots, \frac{q-1}{2} \quad (F)$$

$$\frac{q+1}{2}, \frac{q+3}{2}, \dots, q-1. \quad (F')$$

Correspondingly, the numbers

$$1, 2, 3, \dots, \frac{pq-1}{2}, \quad (C)$$

none of which is divisible by p and q simultaneously, can be distributed in eight classes as follows:

Class 1 contains numbers whose least positive residues mod p belong to (f) and mod q belong to (F) . Let their number be α .

Class 2 contains numbers whose least positive residues mod p belong to (f) and mod q to (F') . Let their number be β .

Class 3 contains numbers whose least positive residues mod p belong to (f') and mod q to (F) . Let their number be γ .

Class 4 contains numbers whose least positive residues mod p belong to (f') and mod q to (F') . Let their number be δ .

Class 5 contains multiples of q whose least positive residues mod p belong to (f') . All the multiples of q in the series (C) are

$$q, 2q, \dots, \frac{p-1}{2}q.$$

Consequently Class 5 contains μ numbers.

Class 6 contains multiples of q whose least positive residues mod p belong to (f) . Their number is $(p-1)/2 - \mu$.

Class 7 contains multiples of p whose least positive residues mod q belong to (F') . Since the multiples of p in the series (C) are

$$p, 2p, \dots, \frac{q-1}{2}p,$$

Class 7 contains ν numbers.

Class 8 contains multiples of p whose least positive residues mod q belong to (F) . Their number is $(q-1)/2 - \nu$.

Classes 2, 4, and 7 comprise all the numbers of series (C) whose least positive residues mod q belong to (F') . For a given residue ρ belonging to (F') , such numbers are

$$\rho, q + \rho, 2q + \rho, \dots, \frac{p-3}{2}q + \rho.$$

In fact, the inequality

$$tq + \rho \leq \frac{pq - 1}{2} = \frac{p - 1}{2}q + \frac{q - 1}{2}$$

or

$$tq \leq \frac{p - 3}{2}q + \left(q + \frac{q - 1}{2} - \rho \right)$$

holds for $t = \frac{p - 3}{2}$ and no longer holds for $t = \frac{p - 1}{2}$.

Hence with a given ρ we have $\frac{p - 1}{2}$ numbers, and since ρ can have $\frac{q - 1}{2}$ values, the number of numbers in Classes 2, 4, and 7 is

$$\frac{p - 1}{2} \cdot \frac{q - 1}{2}$$

On the other hand, this same number is $\beta + \delta + \nu$, and so

$$\beta + \delta + \nu = \frac{p - 1}{2} \cdot \frac{q - 1}{2} \quad (1)$$

In a similar way, by interchanging p and q ; that is, by enumerating the numbers in Classes 3, 4, and 5 in two ways, we find that

$$\gamma + \delta + \mu = \frac{p - 1}{2} \cdot \frac{q - 1}{2} \quad (2)$$

To each number a of the series (C) belonging to Class 3 in the series

$$\frac{pq + 1}{2}, \frac{pq + 3}{2}, \dots, pq - 1 \quad (D)$$

corresponds the number $pq - a$, whose least positive residues for the moduli p and q belong to (f) and (f') , respectively, and vice versa. Therefore in the Class 3 there are exactly as many numbers as there are numbers in (D) whose least positive residues mod p belong to (f) and modulo q to (f') .

Now the two series (C) and (D) make up the series

$$1, 2, 3, \dots, pq - 1. \quad (E)$$

Consequently the number of numbers in Classes 2 and 3 is the same as the number of terms in (E) whose least positive residues mod p belong to (f) and mod q to (F'). But to any pair of such residues corresponds a unique number in (E), and since the number of such pairs is

$$\frac{p-1}{2} \cdot \frac{q-1}{2},$$

Classes 2 and 3 comprise

$$\frac{p-1}{2} \cdot \frac{q-1}{2}$$

numbers, that is,

$$\beta + \gamma = \frac{p-1}{2} \cdot \frac{q-1}{2},$$

whence, in conjunction with (1) and (2), it follows that

$$\mu + \nu + 2\delta = \frac{p-1}{2} \cdot \frac{q-1}{2}$$

or

$$\mu + \nu \equiv \frac{p-1}{2} \cdot \frac{q-1}{2} \pmod{2},$$

which, as we have seen, is equivalent to the reciprocity law.

It remains to show that the form in which Gauss expressed the reciprocity law follows immediately from the relation

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

In fact, if we introduce Legendre's symbol, the Gaussian form of the reciprocity law amounts to

$$\left(\frac{p}{q}\right) = \left(\frac{(-1)^{\frac{q-1}{2}} q}{p}\right).$$

Now for any two numbers a, a' ,

$$\left(\frac{aa'}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{a'}{p}\right),$$

and so

$$\left(\frac{(-1)^{\frac{q-1}{2}} q}{p}\right) = \left(\frac{(-1)^{\frac{q-1}{2}}}{p}\right)\left(\frac{q}{p}\right).$$

But for the same reason

$$\left(\frac{(-1)^{\frac{q-1}{2}}}{p}\right) = \left(\frac{-1}{p}\right)^{\frac{q-1}{2}} = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

and

$$\left(\frac{(-1)^{\frac{q-1}{2}} q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \left(\frac{q}{p}\right).$$

But this indeed equals (p/q) by virtue of Legendre's relation.

11. Applications. A few examples will show how the second fundamental problem can be solved by means of the reciprocity law.

Example 1. Of what primes are 3 and -3 quadratic residues and nonresidues? By the reciprocity law, 3 is a residue or a nonresidue of p according as

$$(-1)^{\frac{p-1}{2}} p$$

is a residue or a nonresidue of 3; that is, according as

$$(-1)^{\frac{p-1}{2}} p \equiv 1 \quad \text{or} \quad (-1)^{\frac{p-1}{2}} p \equiv -1 \pmod{3}.$$

Let at first $p \equiv 1 \pmod{4}$; then these conditions are equivalent to

$$p \equiv 1, \quad p \equiv -1 \pmod{3}$$

or, modulo 12,

$$p \equiv 1 \pmod{12}, \quad p \equiv 5 \pmod{12}.$$

Secondly, if $p \equiv 3 \pmod{4}$, then

$$p \equiv -1 \pmod{3}, \quad p \equiv 1 \pmod{3}$$

or

$$p \equiv 11 \pmod{12}, \quad p \equiv 7 \pmod{12}.$$

The answer to the first question is

$$\begin{aligned} 3Rp & \text{ if } p \equiv 1 \text{ or } 11 \pmod{12}; \\ 3Np & \text{ if } p \equiv 5 \text{ or } 7 \pmod{12}. \end{aligned}$$

By the same reciprocity law, -3 is a residue or a nonresidue of p according as p is a residue or a nonresidue of 3 . That is,

$$\begin{aligned} -3Rp & \text{ if } p \equiv 1 \pmod{6}; \\ -3Np & \text{ if } p \equiv 5 \pmod{6}. \end{aligned}$$

Example 2. For what primes is 5 a quadratic residue or nonresidue? Since the quadratic residues and nonresidues of 5 are 1, 4, and 2, 3, respectively, 5 will be a residue or nonresidue of p according as

$$(-1)^{\frac{p-1}{2}} p \equiv 1, 4 \pmod{5}$$

or

$$(-1)^{\frac{p-1}{2}} p \equiv 2, 3 \pmod{5}.$$

Distinguishing again two cases: $p \equiv 1, p \equiv 3 \pmod{4}$, the primes of which 5 is a residue are characterized by the simultaneous congruences

$$\begin{aligned} p & \equiv 1 \pmod{4}, & p & \equiv 1, 4 \pmod{5}, \\ p & \equiv 3 \pmod{4}, & p & \equiv 1, 4 \pmod{5}, \end{aligned}$$

whence

$$p \equiv 1, 9, 11, 19 \pmod{20}.$$

Primes of which 5 is a nonresidue are characterized by the congruences

$$\begin{aligned} p & \equiv 1 \pmod{4}, & p & \equiv 2, 3 \pmod{5}, \\ p & \equiv 3 \pmod{4}, & p & \equiv 2, 3 \pmod{5}, \end{aligned}$$

or

$$p \equiv 17, 13, 7, 3 \pmod{20}.$$

The final conclusion is

$$\begin{aligned} 5Rp & \text{ if } p \equiv \pm 1, \pm 9 \pmod{20}. \\ 5Np & \text{ if } p \equiv \pm 3, \pm 7 \pmod{20}. \end{aligned}$$

Example 3. Of which primes is 6 a quadratic residue? The number 6 is a quadratic residue of p if simultaneously $2Rp$ and $3Rp$ or $2Np$ and $3Np$. In the first case, either

$$p \equiv 1 \pmod{8}, \quad p \equiv 1 \pmod{3}$$

or

$$p \equiv -1 \pmod{8}, \quad p \equiv -1 \pmod{3},$$

and in the second case either

$$p \equiv 3 \pmod{8}, \quad p \equiv 1 \pmod{3}$$

or

$$p \equiv -3 \pmod{8}, \quad p \equiv -1 \pmod{3}.$$

These four simultaneous congruences give

$$p \equiv \pm 1, \pm 5 \pmod{24}.$$

Thus

$$\begin{aligned} 6Rp &\text{ if } p \equiv \pm 1, \pm 5 \pmod{24}; \\ 6Np &\text{ if } p \equiv \pm 7, \pm 11 \pmod{24}. \end{aligned}$$

In a similar manner we find that www.dbraulibrary.org.in

$$\begin{aligned} -6Rp &\text{ if } p \equiv 1, 5, 7, 11 \pmod{24}; \\ -6Np &\text{ if } p \equiv -1, -5, -7, -11 \pmod{24}. \end{aligned}$$

For composite numbers the solution requires the consideration of several cases according to the quadratic character of the factors. It can be greatly simplified by the introduction of the generalized Legendre's symbol which was used explicitly for the first time by Jacobi.

C. G. J. Jacobi (1804-1851) was a very outstanding mathematician. Though his best discoveries belong to analysis, in the field of number theory Jacobi made important contributions to cyclotomy, with its many ramifications, and to that peculiar branch of the theory of numbers which is closely related to elliptic functions.

12. Jacobi's Symbol. Let Q be an odd positive number and P any number relatively prime to Q . If

$$Q = q_1 q_2 \cdots q_k,$$

where the primes q_1, q_2, \dots, q_k need not be necessarily distinct, then Jacobi's symbol

$$\left(\frac{P}{Q}\right)$$

is defined by

$$\left(\frac{P}{Q}\right) = \left(\frac{P}{q_1}\right)\left(\frac{P}{q_2}\right) \cdots \left(\frac{P}{q_k}\right),$$

the right-hand side containing ordinary Legendre's symbols. Jacobi's symbol possesses properties quite analogous to those of Legendre's symbol.

1. First multiplicative property:

$$\left(\frac{P}{QQ'}\right) = \left(\frac{P}{Q}\right)\left(\frac{P}{Q'}\right)$$

if P is relatively prime to Q and Q' follows immediately from the definition. www.dbralibrary.org.in

2. Second multiplicative property:

$$\left(\frac{PP'}{Q}\right) = \left(\frac{P}{Q}\right)\left(\frac{P'}{Q}\right),$$

if P and P' are relatively prime to Q , follows from the similar property of Legendre's symbol

$$\left(\frac{PP'}{q}\right) = \left(\frac{P}{q}\right)\left(\frac{P'}{q}\right),$$

where q is a prime not dividing P and P' . In particular

$$\left(\frac{c^2P}{Q}\right) = \left(\frac{P}{Q}\right),$$

since

$$\left(\frac{c^2}{Q}\right) = 1.$$

3. Property of invariance mod Q : If $P' \equiv P \pmod{Q}$, then

$$\left(\frac{P'}{Q}\right) = \left(\frac{P}{Q}\right).$$

It follows from the definition, combined with the observation that for any prime divisor q of Q the congruence $P' \equiv P \pmod{Q}$ implies $P' \equiv P \pmod{q}$ and that for Legendre's symbol

$$\left(\frac{P'}{q}\right) = \left(\frac{P}{q}\right).$$

4. The symbol $\left(\frac{-1}{Q}\right)$ is expressed as follows:

$$\left(\frac{-1}{Q}\right) = (-1)^{\frac{Q-1}{2}}.$$

Let $Q = q_1 q_2 \cdots q_k$; then

$$\left(\frac{-1}{q_s}\right) = (-1)^{\frac{q_s-1}{2}},$$

and by definition

$$\left(\frac{-1}{Q}\right) = (-1)^{\frac{q_1-1}{2} + \frac{q_2-1}{2} + \cdots + \frac{q_k-1}{2}}.$$

It remains to show that

$$\frac{Q-1}{2} \equiv \frac{q_1-1}{2} + \frac{q_2-1}{2} + \cdots + \frac{q_k-1}{2} \pmod{2}.$$

We have

$$q_1 q_2 = (1 + q_1 - 1)(1 + q_2 - 1) = 1 + (q_1 - 1) + (q_2 - 1) + (q_1 - 1)(q_2 - 1),$$

but $(q_1 - 1)(q_2 - 1)$ is divisible by 4, and so

$$q_1 q_2 \equiv 1 + (q_1 - 1) + (q_2 - 1) \pmod{4}.$$

Multiplying both members of this congruence by $q_3 = 1 + (q_3 - 1)$, and again neglecting multiples of 4, we have

$$q_1 q_2 q_3 \equiv 1 + (q_1 - 1) + (q_2 - 1) + (q_3 - 1) \pmod{4}.$$

In the same way we find that in general

$$q_1 q_2 q_3 \cdots q_k \equiv 1 + (q_1 - 1) + (q_2 - 1) + \cdots + (q_k - 1) \pmod{4},$$

whence

$$\frac{Q - 1}{2} \equiv \frac{q_1 - 1}{2} + \frac{q_2 - 1}{2} + \cdots + \frac{q_k - 1}{2} \pmod{2}.$$

5. The value of the symbol $(2/Q)$ is

$$\left(\frac{2}{Q}\right) = (-1)^{\frac{Q^2-1}{8}}$$

In fact, for a prime q

$$\left(\frac{2}{q}\right) = (-1)^{\frac{q^2-1}{8}},$$

and so by definition

$$\left(\frac{2}{Q}\right) = (-1)^{\frac{q_1^2-1}{8} + \frac{q_2^2-1}{8} + \cdots + \frac{q_k^2-1}{8}}.$$

It remains to show that

$$\frac{Q^2 - 1}{8} \equiv \frac{q_1^2 - 1}{8} + \frac{q_2^2 - 1}{8} + \cdots + \frac{q_k^2 - 1}{8} \pmod{2}.$$

We have

$$q_1^2 q_2^2 = (1 + q_1^2 - 1)(1 + q_2^2 - 1) = 1 + (q_1^2 - 1) + (q_2^2 - 1) + (q_1^2 - 1)(q_2^2 - 1),$$

but $(q_1^2 - 1)(q_2^2 - 1)$ is divisible by 64, and so

$$q_1^2 q_2^2 \equiv 1 + (q_1^2 - 1) + (q_2^2 - 1) \pmod{16}.$$

Multiplying both members by $q_3^2 = 1 + (q_3^2 - 1)$ and dropping the multiples of 16, we have

$$q_1^2 q_2^2 q_3^2 \equiv 1 + (q_1^2 - 1) + (q_2^2 - 1) + (q_3^2 - 1) \pmod{16},$$

and, in general,

$$q_1^2 q_2^2 \cdots q_k^2 \equiv 1 + (q_1^2 - 1) + (q_2^2 - 1) + \cdots + (q_k^2 - 1) \pmod{16},$$

whence

$$\frac{Q^2 - 1}{8} \equiv \frac{q_1^2 - 1}{8} + \frac{q_2^2 - 1}{8} + \cdots + \frac{q_k^2 - 1}{8} \pmod{2}.$$

6. The reciprocity law for Jacobi's symbol: for positive odd P and Q ,

$$\left(\frac{P}{Q}\right) = \left(\frac{Q}{P}\right) (-1)^{\frac{P-1}{2} \cdot \frac{Q-1}{2}}.$$

We shall prove this, supposing at first that $Q = q$ is a prime. Then

$$\left(\frac{P}{q}\right) = \left(\frac{p_1}{q}\right) \left(\frac{p_2}{q}\right) \cdots \left(\frac{p_i}{q}\right),$$

where $P = p_1 p_2 \cdots p_i$ and the primes are not necessarily distinct. By the reciprocity law

$$\begin{aligned} \left(\frac{p_1}{q}\right) &= \left(\frac{q}{p_1}\right) (-1)^{\frac{q-1}{2} \cdot \frac{p_1-1}{2}}, & \left(\frac{p_2}{q}\right) &= \left(\frac{q}{p_2}\right) (-1)^{\frac{q-1}{2} \cdot \frac{p_2-1}{2}}, \\ & \dots, & \left(\frac{p_i}{q}\right) &= \left(\frac{q}{p_i}\right) (-1)^{\frac{q-1}{2} \cdot \frac{p_i-1}{2}}, \end{aligned}$$

and so

$$\left(\frac{P}{q}\right) = \left(\frac{q}{P}\right) (-1)^{\frac{q-1}{2} \left(\frac{p_1-1}{2} + \frac{p_2-1}{2} + \cdots + \frac{p_i-1}{2}\right)}.$$

Considering that

$$\frac{p_1 - 1}{2} + \frac{p_2 - 1}{2} + \cdots + \frac{p_i - 1}{2} \equiv \frac{P - 1}{2} \pmod{2},$$

we have finally

$$\left(\frac{P}{q}\right) = \left(\frac{q}{P}\right) (-1)^{\frac{P-1}{2} \cdot \frac{q-1}{2}}.$$

In the general case

$$\left(\frac{P}{Q}\right) = \left(\frac{P}{q_1}\right) \left(\frac{P}{q_2}\right) \cdots \left(\frac{P}{q_k}\right).$$

Applying the reciprocity law to each factor, we get

$$\left(\frac{P}{Q}\right) = \left(\frac{Q}{P}\right) (-1)^{\frac{P-1}{2} \left(\frac{q_1-1}{2} + \frac{q_2-1}{2} + \cdots + \frac{q_k-1}{2}\right)}.$$

But again

$$\frac{q_1-1}{2} + \frac{q_2-1}{2} + \cdots + \frac{q_k-1}{2} \equiv \frac{Q-1}{2} \pmod{2},$$

and finally

$$\left(\frac{P}{Q}\right) = \left(\frac{Q}{P}\right) (-1)^{\frac{P-1}{2} \cdot \frac{Q-1}{2}}$$

as announced.

The reciprocity law can also be stated as follows:

If at least one of the numbers P , Q is of the form $4n + 1$, then

$$\left(\frac{P}{Q}\right) = \left(\frac{Q}{P}\right),$$

but if both P , Q are of the form $4n + 3$, then

$$\left(\frac{P}{Q}\right) = -\left(\frac{Q}{P}\right).$$

In fact,

$$\frac{P-1}{2} \cdot \frac{Q-1}{2}$$

is odd only if $P \equiv Q \equiv 3 \pmod{4}$.

Often it is convenient to introduce Jacobi's symbol with a negative Q . It is defined by

$$\left(\frac{P}{Q}\right) = \left(\frac{P}{-Q}\right).$$

Also, by definition,

$$\left(\frac{P}{1}\right) = 1.$$

It is easy to see that the reciprocity law holds unless both numbers P and Q are negative.

13. The Evaluation of Jacobi's Symbol. The reciprocity law allows a very expedient evaluation of any Jacobi's symbol (P/Q) . First, we may suppose that P is positive, odd, and $< \frac{1}{2}Q$. If it is not so at the beginning, we can set

$$P \equiv (-1)^a 2^b R \pmod{Q}$$

where R is positive, odd, and $< \frac{1}{2}Q$, and where $a \geq 0$, $b \geq 0$. Then, by the property of the invariance mod Q ,

$$\left(\frac{P}{Q}\right) = \left(\frac{(-1)^a 2^b R}{Q}\right);$$

and by the second multiplicative property

$$\left(\frac{P}{Q}\right) = \left(\frac{-1}{Q}\right)^a \left(\frac{2}{Q}\right)^b \left(\frac{R}{Q}\right)$$

where the symbols

$$\left(\frac{-1}{Q}\right), \left(\frac{2}{Q}\right)$$

are determined by inspection. Thus we can suppose at the outset that P is positive, odd, and $< \frac{1}{2}Q$. By the reciprocity law

$$\left(\frac{P}{Q}\right) = \epsilon \left(\frac{Q}{P}\right)$$

where ϵ is a known unit. On dividing Q by P , we have

$$Q = Pm + (-1)^a 2^b R$$

where R is positive, odd, and $< \frac{1}{2}P$. Consequently

$$\left(\frac{Q}{P}\right) = \epsilon \left(\frac{R}{P}\right)$$

where ϵ' is a known unit, and

$$\left(\frac{P}{Q}\right) = \epsilon \epsilon' \left(\frac{R}{P}\right).$$

The same process can be applied to (R/P) , and in a few steps the value of the symbol (P/Q) will be determined.

Example. Determine whether 3,422 is a quadratic residue or a non-residue of the prime 5,683. First

$$3,422 = 5,683 \cdot 1 - 2,261$$

and

$$\left(\frac{3,422}{5,683}\right) = \left(\frac{-1}{5,683}\right) \left(\frac{2,261}{5,683}\right) = -\left(\frac{2,261}{5,683}\right).$$

By the reciprocity law

$$\left(\frac{2,261}{5,683}\right) = \left(\frac{5,683}{2,261}\right).$$

But

$$5,683 = 2,261 \cdot 3 - 1,100 = 2,261 \cdot 3 - 4 \cdot 5^2 \cdot 11,$$

and so

$$\left(\frac{5,683}{2,261}\right) = \left(\frac{5^2 \cdot 11}{2,261}\right) = \left(\frac{11}{2,261}\right).$$

Again

$$\left(\frac{11}{2,261}\right) = \left(\frac{2,261}{11}\right) = \left(\frac{-5}{11}\right) = -\left(\frac{5}{11}\right)$$

and

$$\left(\frac{5}{11}\right) = \left(\frac{11}{5}\right) = \left(\frac{1}{5}\right) = 1.$$

Finally

$$\left(\frac{2,261}{5,683}\right) = -1, \quad \left(\frac{3,422}{5,683}\right) = +1;$$

that is, 3,422 is a quadratic residue of 5,683.

14. Solution of the Equation $(P/Q) = \pm 1$ for Q . The use of Jacobi's symbol simplifies considerably the solution of the second fundamental problem in the theory of quadratic residues. If P is any given integer even or odd, positive or negative, we can always represent it in the form

$$P = (-1)^a 2^b c^2 R$$

with a positive odd R , nondivisible by a square > 1 . Since

$$\left(\frac{P}{Q}\right) = (-1)^{a\frac{Q-1}{2} + b\frac{Q^2-1}{8}} \left(\frac{R}{Q}\right),$$

the equation

$$\left(\frac{P}{Q}\right) = \pm 1,$$

where Q is considered as an unknown, reduces to the form

$$\left(\frac{R}{Q}\right) = \pm (-1)^{a\frac{Q-1}{2} + b\frac{Q^2-1}{8}},$$

and this, by the reciprocity law, is equivalent to

$$\left(\frac{Q}{R}\right) = \pm (-1)^{a\frac{Q-1}{2} + b\frac{Q^2-1}{8} + \frac{Q-1}{2} \cdot \frac{R-1}{2}} = \epsilon,$$

the unit ϵ being determined for each of the four possible cases

$$Q \equiv 1, 3, 5, 7 \pmod{8}.$$

In case $R > 1$, let α and β represent all the numbers $< R$ and relatively prime to R for which

$$\left(\frac{\alpha}{R}\right) = +1 \quad \text{or} \quad \left(\frac{\beta}{R}\right) = -1,$$

respectively. Then the equation

$$\left(\frac{Q}{R}\right) = +1$$

is satisfied for

$$Q \equiv \alpha \pmod{R},$$

and the equation

$$\left(\frac{Q}{R}\right) = -1$$

is satisfied for

$$Q \equiv \beta \pmod{R}.$$

As to the values of α and β , they are found by trials, simplified, however, by various particular devices.

It is remarkable that the classes of numbers α and β are equally numerous, each class containing exactly $\frac{1}{2}\phi(R)$ numbers. To prove this, consider the sum

$$S = \sum_x \left(\frac{x}{R}\right)$$

extended over all the numbers belonging to any reduced system of residues mod R . Let r_1, r_2, \dots, r_s be prime divisors of R , and choose for k any nonresidue of r_1 . The number l defined by the simultaneous congruences

$$l \equiv k \pmod{r_1}, \quad l \equiv 1 \pmod{r_2}, \quad \dots, \quad l \equiv 1 \pmod{r_s}$$

is such that

$$\left(\frac{l}{R}\right) = \left(\frac{l}{r_1}\right)\left(\frac{l}{r_2}\right) \dots \left(\frac{l}{r_s}\right) = -1.$$

Now lx runs over the reduced system of residues mod R together with x ; hence

$$S = \sum_x \left(\frac{lx}{R}\right) = \left(\frac{l}{R}\right) \sum_x \left(\frac{x}{R}\right) = -S;$$

that is, $S = 0$. But S is the difference between the number of α 's and the number of β 's, and so the numbers α and the numbers β are equally numerous. Thus the numbers Q , satisfying either one of the equations

$$\left(\frac{Q}{R}\right) = +1 \quad \text{or} \quad \left(\frac{Q}{R}\right) = -1,$$

are distributed in $\frac{1}{2}\varphi(R)$ arithmetic progressions with the difference R . Combining these with the four progressions $8n + 1$, $8n + 3$, $8n + 5$, $8n + 7$, we conclude, finally, that all solutions of either one of the equations

$$\left(\frac{P}{Q}\right) = +1 \quad \text{or} \quad \left(\frac{P}{Q}\right) = -1$$

are distributed in $2\varphi(R) = \varphi(4R)$ progressions with the difference $8R$.

Example. Characterize all positive whole numbers Q prime to 30, for which

$$\left(\frac{30}{Q}\right) = +1 \quad \text{or} \quad \left(\frac{30}{Q}\right) = -1.$$

In this case

$$\left(\frac{30}{Q}\right) = (-1)^{\frac{Q^2-1}{8}} \left(\frac{15}{Q}\right) = (-1)^{\frac{Q^2-1}{8} + \frac{Q-1}{2}} \left(\frac{Q}{15}\right),$$

and the first equation is equivalent to

$$\left(\frac{Q}{15}\right) = (-1)^{\frac{Q^2-1}{8} + \frac{Q-1}{2}};$$

that is,

$$\left(\frac{Q}{15}\right) = +1 \quad \text{if} \quad Q \equiv 1, 3 \pmod{8}$$

and

$$\left(\frac{Q}{15}\right) = -1 \quad \text{if} \quad Q \equiv 5, 7 \pmod{8}.$$

Since for $R = 15$ the numbers α and β are

$$\alpha = 1, 2, 4, 8; \quad \beta = 7, 11, 13, 14,$$

by solving 16 simultaneous congruences, eight in each group,

$$\begin{aligned} Q &\equiv 1, 2, 4, 8 \pmod{15}, & Q &\equiv 1, 3 \pmod{8} \\ Q &\equiv 7, 11, 13, 14 \pmod{15}, & Q &\equiv 5, 7 \pmod{8}, \end{aligned}$$

we find that the equation

$$\left(\frac{30}{Q}\right) = +1$$

is satisfied by

$$Q = 1, 7, 13, 17, 19, 29, 37, 49, 71, 83, 91, 101, 103, 107, 113, 119 \pmod{120},$$

and the other equation

$$\left(\frac{30}{Q}\right) = -1$$

is satisfied by

www.dbraulibrary.org.in

$$Q = 11, 23, 31, 41, 43, 47, 53, 59, 61, 67, 73, 77, 79, 89, 97, 109 \pmod{120}.$$

Exercises and Problems

1. Determine the quadratic character of 231, 783, 563 for the prime modulus 997. *Ans. R, N, R.*

2. Is 56,737 a quadratic residue of the prime 1,001,983? *Ans. Yes.*

3. For what primes is 7 a quadratic residue?

$$\text{Ans. } p \equiv 1, 3, 9, 19, 25, 27 \pmod{28}.$$

4. For what primes is -10 a quadratic residue?

$$\text{Ans. } p \equiv 1, 7, 9, 11, 13, 19, 23, 37 \pmod{40}.$$

5. For what numbers is

$$\left(\frac{-35}{n}\right) = 1?$$

$$\text{Ans. } n \equiv 1, 3, 4, 9, 11, 12, 13, 16, 17, 27, 29, 33 \pmod{35}.$$

6. Show that Euler's theorem in Sec. 8 is entirely equivalent to the reciprocity law in the usual form.

7. Using the reciprocity law for Jacobi's symbols, show that

$$\left(\frac{-1}{P}\right) = (-1)^{\frac{P-1}{2}}, \quad \left(\frac{2}{P}\right) = (-1)^{\frac{P^2-1}{8}}.$$

8. Prove that $4abc - b^2 - c^2$ cannot be a square for positive integers a, b, c .

9. Let N be one of the numbers 3, 5, 10. Show that

$$p = 2^{2^n} + 1$$

is prime if and only if the first power in the series

$$N^2, N^4, N^8, N^{16}, \dots$$

congruent $-1 \pmod p$ is

$$N^{\frac{p-1}{2}}.$$

10. If p, q are two different odd primes, $2Nq$ and

$$\frac{q^{p-1} - 1}{p} \pmod{q^2}$$

then necessarily $q = 3, p = 5$.

11. By analytical methods it is proved that for any prime $p \equiv 1 \pmod 8$ there exists a prime $q \equiv 3 \pmod 4$ of which p is a quadratic non-residue. Show that there are such primes q below $\sqrt{\frac{1}{2}p}$.

12. Prove that all prime divisors of $f^4 - f^2 + 1$ are of the form $12n + 1$.

13. Prove that $12f^2 - 1$ is divisible by at least one prime of the form $12n + 11$.

14. Prove that $4f^2 + 3$ is divisible by at least one prime of the form $12n + 7$ if f is prime to 3.

15. Prove that $4f^2 + 1$ for f odd and nondivisible by 3 has at least one prime divisor of the form $12n + 5$.

16. Show that each of the arithmetic progressions $12n + 1, 12n + 5, 12n + 7, 12n + 11$ contains infinitely many primes.

15. Quadratic Residues of Composite Moduli. A number which is a quadratic residue of a composite modulus is necessarily a quadratic residue of any of its prime factors. To see whether this necessary condition is sufficient, we shall

start with moduli which are powers of primes. Again we must distinguish here two cases: when the modulus is a power of an odd prime p , and when it is a power of 2.

Let a , which we shall suppose prime to p , be a quadratic residue of p . Then it will be a quadratic residue of any power p^m , and the congruence

$$x^2 \equiv a \pmod{p^m}$$

will have exactly two solutions. This can be derived from the general considerations of Sec. 8, Chap. VII, but can be proved independently, as follows.

Let α be some solution of the congruence

$$x^2 \equiv a \pmod{p},$$

and let the two integers P_m, Q_m be determined by

$$\begin{aligned} P_m + Q_m\sqrt{a} &= (\alpha + \sqrt{a})^m \\ P_m - Q_m\sqrt{a} &= (\alpha - \sqrt{a})^m \end{aligned}$$

for $m = 1, 2, 3, \dots$. Clearly

$$P_m \pm Q_m\sqrt{a} = (P_{m-1} \pm Q_{m-1}\sqrt{a})(\alpha \pm \sqrt{a}),$$

whence

$$P_m = P_{m-1}\alpha + Q_{m-1}a, \quad Q_m = P_{m-1} + Q_{m-1}\alpha.$$

These recurrence relations for $m = 1, 2, 3, \dots$ determine successively $P_1, Q_1; P_2, Q_2; \dots$ starting with $P_0 = 1, Q_0 = 0$, and it is evident that P_m, Q_m are integers as announced. Moreover,

$$P_m + \alpha Q_m = 2\alpha P_{m-1} + Q_{m-1}(a + \alpha^2) \equiv 2\alpha(P_{m-1} + \alpha Q_{m-1}) \pmod{p},$$

whence, by repeated applications of this congruence, it follows that

$$P_m + \alpha Q_m \equiv (2\alpha)^m \pmod{p},$$

so that $P_m + aQ_m$ is not divisible by p . On the other hand,

$$P_m - aQ_m = Q_{m-1}(a - a^2)$$

is divisible by p ; hence $2aQ_m$, and consequently Q_m is prime to p . Now

$$P_m^2 - aQ_m^2 = (\alpha^2 - a)^m$$

is divisible by p^m , and the congruence

$$P_m^2 - aQ_m^2 \equiv 0 \pmod{p^m}$$

shows that the fraction P_m/Q_m modulo p , which for brevity we shall denote by β , satisfies the congruence

$$\beta^2 \equiv a \pmod{p^m},$$

which proves the first part of the statement.

Let x be any root of the congruence

$$x^2 \equiv a \pmod{p^m};$$

then

$$(x - \beta)(x + \beta) \equiv 0 \pmod{p^m},$$

but $x - \beta$ and $x + \beta$ cannot be both divisible by p ; otherwise 2β or β would be divisible by p , which is impossible. Consequently, either

$$x \equiv \beta \quad \text{or} \quad x \equiv -\beta \pmod{p^m};$$

that is, there are only two distinct roots β and $-\beta$ of the congruence

$$x^2 \equiv a \pmod{p^m}.$$

Example. Solve the congruence

$$x^2 \equiv 2 \pmod{7^3}.$$

One solution of the congruence

$$x^2 \equiv 2 \pmod{7}$$

is $\alpha = 3$, so that

$$P_1 = 3, \quad Q_1 = 1.$$

Then

$$\begin{aligned} P_2 &= 3 \cdot 3 + 2 \cdot 1 = 11, & Q_2 &= 3 + 1 \cdot 3 = 6 \\ P_3 &= 3 \cdot 11 + 2 \cdot 6 = 45, & Q_3 &= 11 + 6 \cdot 3 = 29, \end{aligned}$$

and $4\frac{5}{2}_9 \pmod{343}$ is 108. Hence the two roots of the proposed congruence are 108 and 235.

16. Moduli 2^m . In this case a is an odd number. In case $m = 1$, the congruence

$$x^2 \equiv a \pmod{2}$$

has the unique solution $x \equiv 1 \pmod{2}$. For $m = 2$, the congruence

$$x^2 \equiv a \pmod{4}$$

is possible only if $a \equiv 1 \pmod{4}$, and then it has the two solutions $x \equiv 1$ or $x \equiv -1 \pmod{4}$. For $m \geq 3$, the congruence

$$\begin{aligned} &\text{www.dbraulibrary.org.in} \\ &x^2 \equiv a \pmod{2^m} \end{aligned}$$

is impossible unless $a \equiv 1 \pmod{8}$. But if this condition is satisfied, it has always four solutions mod 2^m . We shall prove first that it has four solutions once it is possible.

Let α be one solution, so that

$$\alpha^2 \equiv a \pmod{2^m}$$

and x any other. Since x and α are both odd, the congruence

$$x^2 \equiv \alpha^2 \pmod{2^m}$$

is equivalent to

$$\frac{x + \alpha}{2} \cdot \frac{x - \alpha}{2} \equiv 0 \pmod{2^{m-2}}.$$

But of the two numbers

$$\frac{x + \alpha}{2} \quad \text{and} \quad \frac{x - \alpha}{2},$$

only one is even and the other is odd. Consequently, with the proper choice of sign \pm ,

$$\frac{x \mp \alpha}{2} \equiv 0 \pmod{2^{m-2}}$$

or

$$x \equiv \pm \alpha \pmod{2^{m-1}};$$

that is,

$$x = \pm \alpha + 2^{m-1}t.$$

Now, distinguishing the cases of odd and even t , we have one of the four cases

$$\begin{aligned} x &\equiv \alpha, & x &\equiv -\alpha, & x &\equiv \alpha + 2^{m-1}, \\ x &\equiv -\alpha + 2^{m-1} \pmod{2^m}. \end{aligned}$$

Conversely, for each of them we have a solution of the proposed congruence, and all four solutions are distinct modulo 2^m .

It remains to show that for $a \equiv 1 \pmod{8}$ the congruence

$$x^2 \equiv a \pmod{2^m}$$

is possible, and this we shall do by exhibiting explicitly one of its solutions, following a method of Legendre.

We shall start with the following algebraic problem: To determine a polynomial

$$P_n(x) = 1 + \alpha_1 x + \alpha_2 x^2 + \cdots + \alpha_n x^n$$

of degree n for which the difference

$$P_n(x)^2 - 1 - x$$

is divisible by x^{n+1} . In other words, $P_n(x)$ must be such that

$$P_n(x)^2 - 1 - x = x^{n+1}Q(x), \tag{A}$$

where $Q(x)$ is a polynomial. On taking the derivative, we get

$$2P_n(x)P'_n(x) - 1 = x^n R(x),$$

whence, multiplying both sides by $P_n(x)$ and using equation (A) again,

$$2(1+x)P'_n(x) - P_n(x) = x^n S(x),$$

where $S(x)$ is some polynomial. But since the degree of the left-hand side is n , this polynomial must reduce to a constant, and so

$$2(1+x)P'_n(x) - P_n(x) = cx^n. \quad (B)$$

Conversely, the polynomial $P_n(x)$ satisfying (B), and such that $P_n(0) = 1$, will satisfy (A). To prove this, let

$$P_n(x)^2 = 1 + x + g(x).$$

Then by virtue of (B)

$$(1+x)g'(x) - g(x) = cx^n P_n(x). \quad (C)$$

Since $g(0) = 0$, $g(x)$ is divisible by x . Let $g(x) = x^\alpha f(x)$ where $f(x)$ is no longer divisible by x . On substituting into (C) and dividing by $x^{\alpha-1}$, we have

$$[\alpha(1+x) - x]f(x) + x(1+x)f'(x) = cx^{\alpha+1-n}P_n(x),$$

which shows that α cannot be less than $n+1$. For otherwise the right-hand side vanishes for $x=0$, while the left-hand side reduces to

$$\alpha f(0),$$

which is not 0. Again, α cannot be greater than $n+1$ unless $c=0$, in which case we reach the contradictory result $f(0) = 0$.

Thus $g(x)$ is exactly divisible by x^{n+1} . On substituting

$$P_n(x) = 1 + \alpha_1 x + \dots + \alpha_n x^n$$

in (B) and equating coefficients of like powers of x in both members, we get for $k = 0, 1, 2, \dots, n-1$

$$\alpha_{k+1} = -\frac{2k-1}{2k+2}\alpha_k, \quad \alpha_0 = 1,$$

whence

$$\alpha_1 = \frac{1}{2}, \quad \alpha_2 = -\frac{1}{8}, \quad \alpha_3 = \frac{3}{6 \cdot 8}, \dots,$$

and, in general,

$$\alpha_k = (-1)^{k-1} \frac{1 \cdot 3 \cdot 5 \cdots (2k-3)}{2 \cdot 4 \cdot 6 \cdots 2k}.$$

Thus the algebraic problem is solved by the polynomial

$$P_n(x) = 1 + \frac{1}{2}x - \frac{1}{8}x^2 + \cdots + (-1)^{n-1} \frac{1 \cdot 3 \cdot 5 \cdots (2n-3)}{2 \cdot 4 \cdot 6 \cdots 2n} x^n,$$

which naturally represents the $n+1$ first terms of the expansion $\sqrt{1+x}$ by the binomial theorem. In Sec. 19, Chap. IV, it was proved that

$$\frac{1 \cdot 3 \cdot 5 \cdots (2k-1)}{2 \cdot 4 \cdot 6 \cdots 2k} = \frac{G}{2^{2k-1}}$$

where G is an integer. Then

$$(2k-1)2^{2k-1}\alpha_k$$

is an integer, and so is

$$2k \cdot 2^{2k-1}\alpha_k;$$

consequently

$$\alpha_k = \frac{g_k}{2^{2k-1}},$$

where g_k is an integer. Now if we substitute $8r$ for x in $P_n(x)$, the resulting polynomial in r ,

$$P_n(8r),$$

will have integer coefficients, and the coefficient of r^k will be divisible by 2^{k+1} . Then all the coefficients of the polynomial

$$P_n(8r)^2 - 1 - 8r$$

will be divisible by 2^{n+3} .

Now if $a \equiv 1 \pmod{8}$, we can set $a = 1 + 8r$; from the remark just made

$$P_n(8r)^2 - 1 - 8r$$

is an integer divisible by 2^{n+2} . Consequently $P_{m-3}(8r)$ exhibits one solution of the congruence

$$x^2 \equiv a \pmod{2^m}$$

in explicit form.

Example. Solve the congruence

$$x^2 \equiv 17 \pmod{128}$$

by Legendre's method. Here $m = 7$, and correspondingly

$$P_4(x) = 1 + \frac{1}{2}x - \frac{1}{8}x^2 + \frac{1}{16}x^3 - \frac{5}{128}x^4,$$

$$P_4(8r) = 1 + 4r - 8r^2 + 32r^3 - 160r^4.$$

For $r = 2$, as in our example, $P_4(16) = -23 \pmod{128}$,

$$P_4(16) \equiv -23 \pmod{128},$$

and so the four roots of the proposed congruence are

$$\pm 23, \pm 41.$$

17. General Conclusion. Combining the results of the preceding section with the general considerations in Sec. 7, Chap. VII, we arrive at the following general conclusion: A number a , prime to a composite modulus m , is a quadratic residue of m if it is a quadratic residue of all odd prime divisors of m and, in addition, if it is $\equiv 1 \pmod{4}$ in case m is divisible by 4 and not by 8, and $\equiv 1 \pmod{8}$ in case m is divisible by 8. The congruence

$$x^2 \equiv a \pmod{m}$$

is impossible except under the stated circumstances. When it is possible, it has exactly

$$2^{\mu+\sigma}$$

solutions, denoting by μ the number of distinct odd prime divisors of m and putting

$$\begin{aligned} \sigma &= 0 & \text{if} & \quad m \equiv 1 \pmod{2} \text{ or } m \equiv 2 \pmod{4} \\ \sigma &= 1 & \text{if} & \quad m \equiv 4 \pmod{8} \\ \sigma &= 2 & \text{if} & \quad m \equiv 0 \pmod{8}. \end{aligned}$$

In particular the congruence

$$x^2 + 1 \equiv 0 \pmod{m}$$

is possible only if all odd prime divisors of m are of the form $4n + 1$, and m , in case it is even, is not divisible by 4.

Again the congruence

$$x^2 + 2 \equiv 0 \pmod{m}$$

is possible for an odd m only if all prime divisors of m are of one of the forms $8n + 1$ or $8n + 3$ and the series of similar theorems can be extended.

In case a is not prime to m , the conditions for the possibility of the congruence

$$x^2 \equiv a \pmod{m}$$

cannot be stated so simply, and we shall not discuss them here.

18. Solution of Quadratic Congruences for Prime Moduli.

The general quadratic congruence

$$rx^2 + sx + t \equiv 0 \pmod{m}$$

can be replaced by an equivalent congruence

$$(2rx + s)^2 + 4rt - s^2 \equiv 0 \pmod{4rm},$$

the solution of which in the last instance depends on that of the congruence

$$x^2 \equiv a \pmod{p}$$

with a prime modulus p and a nondivisible by p . No expedient method for the actual solution, in case of a large p , is

known. For moderately large p not $\equiv 1 \pmod{8}$, the following method can be used with advantage, especially when a calculating machine is available.

First, suppose $p = 4n + 3$. By Euler's criterion

$$a^{2n+1} \equiv 1 \pmod{p}$$

if the proposed congruence is possible at all. Hence

$$a^{2n+2} \equiv a \pmod{p};$$

that is,

$$x \equiv \pm a^{n+1} \pmod{p}$$

is the solution.

Next let $p = 8n + 5$; then by Euler's criterion

$$a^{4n+2} \equiv 1 \pmod{p}$$

so that either

$$a^{2n+1} \equiv 1 \pmod{p}$$

or

$$a^{2n+1} \equiv -1 \pmod{p}.$$

In the first case

$$x \equiv \pm a^{n+1} \pmod{p}$$

is the requested solution. In the second case we use the fact that 2 is a nonresidue of p ; then

$$2^{4n+2} \equiv -1 \pmod{p}$$

and

$$2^{4n+2} a^{2n+1} \equiv 1 \pmod{p},$$

whence

$$x \equiv \pm \frac{1}{2}(4a)^{n+1} \pmod{p}.$$

Example 1. Solve the congruence

$$x^2 \equiv 3 \pmod{227}.$$

First we ascertain that the congruence is solvable as explained in Sec. 13. Next $227 = 4 \cdot 56 + 3$, and so

$$x \equiv \pm 3^{57} \pmod{227}.$$

It remains to reduce

$$3^{57}$$

mod 227 to its absolutely least residue. We have

$$57 = 32 + 16 + 8 + 1$$

and

$$3^1 \equiv 3, \quad 3^2 \equiv 9, \quad 3^4 \equiv 81, \quad 3^8 \equiv -22$$

$$3^{16} \equiv 30, \quad 3^{32} \equiv -8$$

whence

$$3^{57} \equiv -50 \pmod{227}.$$

Finally

$$x \equiv \pm 50 \pmod{227}.$$

Example 3. Solve the congruence

$$x^2 \equiv 11 \pmod{269}.$$

Here $269 = 8 \cdot 33 + 5$, $n = 33$, $2n + 1 = 67$, and

$$11^1 \equiv 11, \quad 11^2 \equiv 121, \quad 11^4 \equiv 115, \quad 11^8 \equiv 44$$

$$11^{16} \equiv 53, \quad 11^{32} \equiv 119, \quad 11^{64} \equiv -96.$$

Hence

$$11^{67} \equiv -1 \pmod{269},$$

and correspondingly

$$x \equiv \pm \frac{1}{2} \cdot 44^{34} \pmod{269}.$$

Now

$$44^2 \equiv 53, \quad 44^4 \equiv 119, \quad 44^8 \equiv -96, \quad 44^{16} \equiv 70, \quad 44^{32} \equiv 58$$

and

$$x \equiv \pm 77 \pmod{269}.$$

19. The Exclusion Method. More convenient in practice and applicable to all primes without exception is the exclusion method for solving the congruence

$$x^2 \equiv a \pmod{p},$$

based on a simple idea of replacing this congruence by an equivalent equation

$$a + py = x^2.$$

Since a can be supposed to be positive and less than p and x less than $\frac{1}{2}p$, we have to seek integers y , nonnegative and less than $\frac{1}{2}p$, which make $a + py$ a square. But by far not all such integers should be tried, and the great majority of them may be excluded. Let us take any number E , prime to p , usually prime or a power of a prime, and mark all of its quadratic nonresidues which we shall denote by β . Clearly all numbers y satisfying the congruences

$$a + py \equiv \beta \pmod{E}$$

must be excluded from the trials. To find in the simplest way solutions of this congruence corresponding to different values of β , let c be a value of the fraction $-a/p \pmod{E}$ so that

$$a + pc \equiv 0 \pmod{E}.$$

Then

$$a(y + c) \equiv \beta \pmod{E}.$$

Supposing, for simplicity, E to be prime, and letting β run through the nonresidues of E , it is clear that $y + c$ will run through the nonresidues or residues of E according as pRE or pNE . In the first case all the values of y to be excluded for the excludent E are

$$y \equiv \beta + c \pmod{E},$$

and in the second case

$$y \equiv \alpha + c \pmod{E},$$

where α runs through all the quadratic residues of E excluding 0. The case when the excludent is a power of a prime can be treated in a similar way.

The following tables indicate what values of $y \pmod{E}$ should be excluded for $E = 5, 7, 8, 9, 11, 13$.

$E = 5$

$pR5$

$\frac{a}{p} \equiv 0$	1	2	3	4
2	3	4	0	1
3	1	0	1	2

1, 4 R 5

$pN5$

$\frac{a}{p} \equiv 0$	1	2	3	4
1	2	3	4	0
4	0	1	2	3

2, 3 N 5

$x = 1, 2, 3, 4$

$\frac{1}{x} = 1, 3, 2, 4$

$E = 7$

$pR7$

$\frac{a}{p} \equiv 0$	1	2	3	4	5	6
2	4	5	6	0	1	2
3	6	0	1	2	3	4
6	0	1	2	3	4	5

1, 2, 4 R 7

$pN7$

$\frac{a}{p} \equiv 0$	1	2	3	4	5	6
1	2	3	4	5	6	0
2	3	4	5	6	0	1
4	5	6	0	1	2	3

3, 5, 6 N 7

$x = 1, 2, 3, 4, 5, 6$

$\frac{1}{x} = 1, 4, 5, 2, 3, 6$

$E = 8$

$p \equiv 1 \pmod{8}$

$\frac{a}{p} \equiv 0$	1	2	3	4	5	6	7
2	3	4	5	6	7	0	1
3	4	5	6	7	0	1	2
5	6	7	0	1	2	3	4
6	7	0	1	2	3	4	5
7	0	1	2	3	4	5	6

$p \equiv 3 \pmod{8}$

$\frac{a}{p} \equiv 0$	1	2	3	4	5	6	7
1	2	3	4	5	6	7	0
2	3	4	5	6	7	0	1
5	6	7	0	1	2	3	4
6	7	0	1	2	3	4	5
7	0	1	2	3	4	5	6

$p \equiv 5 \pmod{8}$

$\frac{a}{p} \equiv 0$	1	2	3	4	5	6	7
1	2	3	4	5	6	7	0
2	3	4	5	6	7	0	1
3	4	5	6	7	0	1	2
6	7	0	1	2	3	4	5
7	0	1	2	3	4	5	6

 $p \equiv 7 \pmod{8}$

$\frac{a}{p} \equiv 0$	1	2	3	4	5	6	7
1	2	3	4	5	6	7	0
2	3	4	5	6	7	0	1
3	4	5	6	7	0	1	2
5	6	7	0	1	2	3	4
6	7	0	1	2	3	4	5

$x = 1, 3, 5, 7$

$\frac{1}{x} = 1, 3, 5, 7$

$E = 9$

 $pR9$

$\frac{a}{p} \equiv 0$	1	2	3	4	5	6	7	8
2	3	4	5	6	7	8	0	1
3	4	5	6	7	8	0	1	2
5	6	7	8	0	1	2	3	4
6	7	8	0	1	2	3	4	5
8	0	1	2	3	4	5	6	7

 $1, 4, 7 R 9$ $pN9$

$\frac{a}{p} \equiv 0$	1	2	3	4	5	6	7	8
1	2	3	4	5	6	7	8	0
3	4	5	6	7	8	0	1	2
4	5	6	7	8	0	1	2	3
6	7	8	0	1	2	3	4	5
7	8	0	1	2	3	4	5	6

 $2, 5, 8 N 9$

$x = 1, 2, 4, 5, 7, 8$

$\frac{1}{x} = 1, 5, 7, 2, 4, 8$

$E = 11$

$pR11$

$\frac{a}{p} \equiv 0$	1	2	3	4	5	6	7	8	9	10
2	3	4	5	6	7	8	9	10	0	1
6	7	8	9	10	0	1	2	3	4	5
7	8	9	10	0	1	2	3	4	5	6
8	9	10	0	1	2	3	4	5	6	7
10	0	1	2	3	4	5	6	7	8	9

$pN11$

$\frac{a}{p} \equiv 0$	1	2	3	4	5	6	7	8	9	10
1	2	3	4	5	6	7	8	9	10	0
3	4	5	6	7	8	9	10	0	1	2
4	5	6	7	8	9	10	0	1	2	3
5	6	7	8	9	10	0	1	2	3	4
9	10	0	1	2	3	4	5	6	7	8

1, 3, 4, 5, 9 $R 11$

2, 6, 7, 8, 10 $N 11$

$x \equiv 1, 2, 3, 4, 5, 6, 7, 8, 9, 10$

$\frac{1}{x} \equiv 1, 6, 4, 3, 9, 2, 8, 7, 5, 10$

$E = 13$

$pR13$

$\frac{a}{p} \equiv 0$	1	2	3	4	5	6	7	8	9	10	11	12
2	3	4	5	6	7	8	9	10	11	12	0	1
5	6	7	8	9	10	11	12	0	1	2	3	4
6	7	8	9	10	11	12	0	1	2	3	4	5
7	8	9	10	11	12	0	1	2	3	4	5	6
8	9	10	11	12	0	1	2	3	4	5	6	7
11	12	0	1	2	3	4	5	6	7	8	9	10

1, 3, 4, 9, 10, 12 $R 13$

pN13

$\frac{a}{p} \equiv 0$	1	2	3	4	5	6	7	8	9	10	11	12
1	2	3	4	5	6	7	8	9	10	11	12	0
3	4	5	6	7	8	9	10	11	12	0	1	2
4	5	6	7	8	9	10	11	12	0	1	2	3
9	10	11	12	0	1	2	3	4	5	6	7	8
10	11	12	0	1	2	3	4	5	6	7	8	9
12	0	1	2	3	4	5	6	7	8	9	10	11

2, 5, 6, 7, 8, 11 N 13

 $x \equiv 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12$ $\frac{1}{x} \equiv 1, 7, 9, 10, 8, 11, 2, 5, 3, 4, 6, 12.$

With these few excludents only one or two numbers, on the average, are left out of 100, and the exclusions themselves can be carried out automatically by means of mechanical devices of easy construction. When the necessity arises of making exclusions out of thousands of numbers, more excludents must be used and the process of exclusion is then carried out by a complicated machine constructed for this purpose by Dr. D. H. Lehmer. The description of this machine can be found in Dr. Lehmer's article: "A Photo Electric Number Sieve," *American Mathematical Monthly*, **40**, p. 401, (1933).

Example. Solve the congruence

$$x^2 \equiv 6 \pmod{337}.$$

To show the use of the preceding tables, we begin with $E = 5$. Since $337 \equiv 2 \pmod{5}$ and

$$-\frac{a}{p} \equiv -\frac{6}{2} \equiv 2 \pmod{5};$$

in the table for $E = 5$, $pN5$ we find 1, 3. Thus all numbers $\equiv 1$ or 3 should be excluded. Similarly we find that for

- $E = 7$ all numbers $\equiv 0, 4, 6$
- $E = 8$ all numbers $\equiv 0, 1, 4, 5, 7$
- $E = 9$ all numbers $\equiv 0, 2, 5, 6, 8$
- $E = 11$ all numbers $\equiv 0, 1, 5, 8, 10$
- $E = 13$ all numbers $\equiv 0, 1, 4, 8, 11, 12$

must be excluded. In our case we have to make exclusions out of the numbers $y = 1, 2, 3, \dots, 84$. It happens that only one number, $y = 75$, remains; correspondingly

$$337 \cdot 75 + 6 = 25,281 = 159^2,$$

so that the proposed congruence is satisfied by

$$x \equiv \pm 159 \pmod{337}.$$

Exercises and Problems

1. Solve the congruences (a) $x^2 \equiv 14 \pmod{25}$; (b) $x^2 \equiv 41 \pmod{256}$; (c) $x^2 \equiv 73 \pmod{1,296}$.

Ans. (a) ± 83 ; (b) $\pm 51, \pm 77$; (c) $\pm 37, \pm 125, \pm 523, \pm 611$.

2. Solve the congruences (a) $x^2 \equiv 10 \pmod{107}$; (b) $x^2 \equiv 5 \pmod{149}$.

Ans. (a) ± 44 ; (b) ± 68 .

3. Devise a method for solving the congruence $x^2 \equiv a \pmod{p}$ if the prime $p \equiv 1 \pmod{8}$ and one quadratic nonresidue of p is known. Solve the congruence $x^2 + 7 \equiv 0 \pmod{281}$ by using the fact that $3N281$.

Ans. $x \equiv \pm 67 \pmod{281}$.

4. Solve by the exclusion method the congruences (a) $x^2 \equiv 11 \pmod{257}$; (b) $x^2 \equiv 87 \pmod{389}$.

Ans. (a) ± 36 ; (b) ± 101 .

5. Show that the number of quadratic residues in a reduced system for a composite modulus m is

$$\frac{\varphi(m)}{2^{\mu+\sigma}}$$

where μ and σ have the same meaning as in Sec. 17.

6. Show that a number $A p^\nu$, where A is nondivisible by an odd prime p , is a quadratic residue of p^μ under the following circumstances only:

(a) ν even and ARp if $\nu < \mu$; (b) $\nu \geq \mu$ without any condition on A . The congruence

$$x^2 \equiv Ap^\nu \pmod{p^\mu}$$

has $2p^{\nu/2}$ solutions mod p^μ in case (a) and $p^{[\mu/2]}$ solutions in case (b).

7. Prove that the number of all quadratic residues mod p^n is

$$\frac{p^{n+1} - p}{2(p+1)} + 1 \quad \text{if } n \text{ is even;}$$

$$\frac{p^{n+1} - 1}{2(p+1)} + 1 \quad \text{if } n \text{ is odd.}$$

8. Show that the general congruence of the second degree

$$rx^2 + sx + t \equiv 0 \pmod{m}$$

is equivalent to a congruence

$$ax^2 + bx + c \equiv 0 \pmod{m},$$

in which a is a divisor of m . If $m = a\mu\nu$, where ν is prime to a while μ consists of the same prime factors as a , the solution of the congruence

$$ax^2 + bx + c \equiv 0 \pmod{a\mu}$$

depends on congruences of the first degree, while the congruence

$$ax^2 + bx + c \equiv 0 \pmod{\nu}$$

can be replaced by

$$x^2 + \sigma x + \tau \equiv 0 \pmod{\nu}.$$

If σ is even (which can always be supposed in case ν is odd), the last congruence can be reduced to its simplest form

$$\left(x + \frac{\sigma}{2}\right)^2 + \tau - \frac{\sigma^2}{4} \equiv 0 \pmod{\nu}.$$

If σ is odd and ν even, then

$$(2x + \sigma)^2 + 4\tau - \sigma^2 \equiv 0 \pmod{4\nu}.$$

CHAPTER XI

SOME PROBLEMS CONNECTED WITH QUADRATIC FORMS

1. Object of This Chapter. Among the important theorems discovered by Fermat and announced by him repeatedly in his correspondence, though without any indication of the proof, many belong to the vast and interesting theory of quadratic forms. By a quadratic form is meant a homogeneous function of the second degree in its indeterminates or variables. According to the number of variables involved, quadratic forms are classified as binary, ternary, quaternary, etc. For example

$$ax^2 + bxy + cy^2$$

is a general binary quadratic form in the variables x, y . The forms

$$x^2 + y^2 + z^2, \quad xy + xz + yz, \quad x^2 - yz$$

are particular ternary quadratic forms, while

$$x^2 + y^2 + z^2 + t^2, \quad xy + zt$$

exemplify quaternary forms.

The desire to prove theorems announced by Fermat led Euler and especially Lagrange to the creation of the arithmetical theory of binary quadratic forms which later was brought to completion by Gauss. Gauss also laid the foundations of the theory of ternary quadratic forms, and by the combined efforts of many prominent men, following his footsteps, a vast theory has been developed. In this ele-

mentary book we cannot present even the comparatively simple theory of binary quadratic forms and much less can we enter into the general theory. It must suffice to give a fleeting glimpse of the wealth of arithmetical truths, including Fermat's theorems, which have their origin in the theory of quadratic forms. All that we need can be presented in a very elementary manner by developing an idea which goes back to Lagrange.

2. Fundamental Lemma. Let a be a positive or negative integer but not a square, and m a number of which a is a quadratic residue, so that the congruence

$$x^2 \equiv a \pmod{m}$$

has solutions. Let N be any root of this congruence. The lemma, which is the object of this section, consists in the following statement:

For some multiplier λ numerically not exceeding

$$\sqrt{\frac{4}{3}|a|},$$

two integers x, y can be found satisfying the equation

$$\lambda m = x^2 - ay^2,$$

and the congruence

$$x - Ny \equiv 0 \pmod{m}.$$

Moreover, the greatest common divisor of x and y divides both λ and m .

We shall suppose at first that

$$|m| > \sqrt{\frac{4}{3}|a|}.$$

As to the root of the congruence

$$N^2 \equiv a \pmod{m},$$

it can be taken at the outset as not exceeding numerically $\frac{1}{2}|m|$. Since $N^2 - a$ is divisible by m , we can set

$$N^2 - a = mm_1,$$

whence

$$m_1 = \frac{N^2 - a}{m}$$

and

$$|m_1| \leq \frac{|m|}{4} + \frac{|a|}{|m|}.$$

The inequality

$$\frac{|m|}{4} + \frac{|a|}{|m|} < |m|$$

is satisfied by

$$|m| > \sqrt{\frac{4}{3}|a|},$$

as we suppose. Thus $|m_1| < |m|$. Reduce now N mod m_1 to its absolutely least residue N_1 so that

$$N_1 = N - \delta_1 m_1,$$

where the integer δ_1 is so chosen that

$$|N_1| \leq \frac{1}{2}|m_1|.$$

Since

$$N^2 - a \equiv 0 \pmod{m_1},$$

we shall have also

$$N_1^2 - a \equiv 0 \pmod{m_1},$$

so that

$$N_1^2 - a = m_1 m_2$$

with some integer $m_2 \neq 0$. Again,

$$|m_2| \leq \frac{|m_1|}{4} + \frac{|a|}{|m_1|},$$

so that $|m_2| < |m_1|$ if

$$|m_1| > \sqrt{\frac{4}{3}|a|}.$$

Supposing this to be the case, we choose δ_2 so that

$$N_2 = N_1 - \delta_2 m_2$$

satisfies the inequality

$$|N_2| \leq \frac{1}{2} |m_2|.$$

Then

$$N_2^2 - a = m_2 m_3$$

and $|m_3| < |m_2|$ as long as

$$|m_2| > \sqrt{\frac{4}{3}|a|}.$$

Continuing in this way, we get a series of decreasing positive integers

$$|m| > |m_1| > |m_2| > |m_3| > \dots,$$

which cannot be continued indefinitely. Hence the numbers

$$m, m_1, m_2, m_3, \dots$$

decrease numerically up to, say, m_{k+1} , which is not greater in absolute value than the next following term m_{k+2} . Of necessity

$$|m_{k+1}| \leq \sqrt{\frac{4}{3}|a|},$$

while m, m_1, m_2, \dots, m_k are all greater numerically than

$$\sqrt{\frac{4}{3}|a|}.$$

For simplicity, denote m_{k+1} by λ . Then from the equation

$$\lambda m_k = N_k^2 - a$$

it follows that

$$\lambda m_k = (m_k z_k + N_k y_k)^2 - a y_k^2$$

is satisfied by $z_k = 0, y_k = 1$. Substituting here

$$N_k = N_{k-1} - \delta_k m_k$$

and setting

$$y_{k-1} = z_k - \delta_k y_k, \quad z_{k-1} = y_k,$$

we have also

$$\lambda m_k = (m_k y_{k-1} + N_{k-1} z_{k-1})^2 - a z_{k-1}^2,$$

whence

$$\lambda = m_k y_{k-1}^2 + 2N_{k-1} y_{k-1} z_{k-1} + m_{k-1} z_{k-1}^2$$

and

$$\lambda m_{k-1} = (m_{k-1} z_{k-1} + N_{k-1} y_{k-1})^2 - a y_{k-1}^2$$

because

$$m_k m_{k-1} = N_{k-1}^2 - a.$$

Notice that y_{k-1} , z_{k-1} are relatively prime, since y_k and z_k are. Substituting

$$N_{k-1} = N_{k-2} - \delta_{k-1} m_{k-1}$$

and setting again

$$y_{k-2} = z_{k-1} - \delta_{k-1} y_{k-1}, \quad z_{k-2} = y_{k-1},$$

we have

$$\lambda m_{k-1} = (m_{k-1} y_{k-2} + N_{k-2} z_{k-2})^2 - a z_{k-2}^2,$$

whence, in the same way as before,

$$\lambda m_{k-2} = (m_{k-2} z_{k-2} + N_{k-2} y_{k-2})^2 - a y_{k-2}^2.$$

As to y_{k-2} , z_{k-2} , they are relatively prime, since y_{k-1} , z_{k-1} are. It is clear that by continuing in the same way we find two relatively prime integers y , z satisfying the equation

$$\lambda m = (mz + Ny)^2 - ay^2.$$

If at the outset

$$|m| \leq \sqrt{\frac{4}{3}|a|},$$

and at the same time

$$|m_1| \leq \sqrt{\frac{4}{3}|a|},$$

the reasoning and the conclusion remain the same. If, however,

$$|m_1| > \sqrt{\frac{4}{3}|a|},$$

then by what has been proved

$$\lambda m_1 = (m_1 y + Nz)^2 - az^2$$

for y and z relatively prime, whence again

$$\lambda m = (mz + Ny)^2 - ay^2.$$

The algorithm whereby the numbers

$$x = mz + Ny, \quad y$$

satisfying the equation

$$\lambda m = x^2 - ay^2$$

and the congruence

$$x - Ny \equiv 0 \pmod{m}$$

are found can be presented as follows:

Starting with

$$x_k = mz_k + Ny_k, \quad y_k$$

determine by recurrence the sequence of pairs

$$x_{k-1}, y_{k-1}; \quad x_{k-2}, y_{k-2}; \quad \dots, \quad x_1, y_1; \quad z_i, y_i,$$

using the formulas

$$y_{i-1} = \frac{x_i - N_{i-1}y_i}{m_i}, \quad x_{i-1} = m_{i-1}y_i + N_{i-1}y_{i-1}$$

for $i = k, k-1, \dots, 2, 1$. These formulas are easily obtained from the relations

$$y_{i-1} = z_i - \delta_i y_i, \quad z_{i-1} = y_i$$

by introducing

$$x_i = m_i z_i + N_i y_i$$

instead of z_i .

Since y and z are relatively prime, the greatest common divisor of

$$x = mz + Ny, \quad y$$

divides m . On the other hand,

$$\lambda = mz^2 + 2Nzy + \frac{N^2 - a}{m}y^2,$$

whence it is clear that the g.c.d. of x, y divides λ also. The fundamental lemma is thus completely proved.

Example 1. Let us take $a = -14$ and $m = 113$. The congruence

$$N^2 \equiv -14 \pmod{113}$$

is satisfied by $N = 41$. Now

$$41^2 + 14 = 113 \cdot 15; \quad m_1 = 15$$

and

$$N_1 = 41 - 15 \cdot 3 = -4; \quad \delta_1 = 3.$$

Again,

$$(-4)^2 + 14 = 15 \cdot 2; \quad m_2 = 2,$$

and since

$$2 < \sqrt{\frac{58}{3}}$$

the operations stop here. We have $x = 113 \cdot 1 + 41(-3) = -10$

$$y = \frac{-4 - 41}{15} = -3, \quad x = 113 \cdot 1 + 41(-3) = -10$$

and

$$\begin{aligned} (-10)^2 + 14 \cdot (-3)^2 &= 2 \cdot 113 \\ -10 &\equiv -3 \cdot 41 \pmod{113}. \end{aligned}$$

The multiplier $\lambda = m_2 = 2$.

Example 2. Let $a = 71, m = 127$. The congruence

$$N^2 \equiv 71 \pmod{127}$$

is satisfied by $N = 43$. Now

$$\begin{aligned} 43^2 - 71 &= 127 \cdot 14; & m_1 &= 14 \\ N_1 = 43 - 3 \cdot 14 &= 1; & \delta_1 &= 3 \\ 1^2 - 71 &= 14 \cdot -5; & m_2 &= -5. \end{aligned}$$

Here the operations stop, since

$$5 < \sqrt{\frac{234}{3}}.$$

Thus $\lambda = -5$ and $x_1 = 1, y_1 = 1$. Next

$$y = \frac{1 - 43 \cdot 1}{14} = -3, \quad x = 127 \cdot 1 + 43(-3) = -2.$$

As it should be,

$$x - 43y \equiv 0 \pmod{127}$$

and

$$(-2)^2 - 71 \cdot (-3)^2 = -5 \cdot 127.$$

3. The Equation $x^2 - ay^2 = m$. Integers x, y satisfying the equation

$$x^2 - ay^2 = m$$

constitute a *solution* of this equation. The solution is said to be primitive if x and y are relatively prime. Since any other solution can be derived from primitive solutions of equations of the type

$$\frac{x'^2}{d^2} - a \frac{y'^2}{d^2} = \frac{m}{d^2}$$

corresponding to various square divisors d^2 of m by multiplying x' and y' by d , it follows that we may confine our attention to primitive solutions only.

For a primitive solution, y is necessarily relatively prime to m ; hence the congruence

$$x \equiv Ny \pmod{m}$$

determines a class of numbers $N \pmod{m}$. By virtue of this congruence and the equation itself

$$(N^2 - a)y^2 \equiv 0 \pmod{m}$$

or

$$N^2 \equiv a \pmod{m}.$$

Consequently the previously introduced number N is a root of the congruence

$$z^2 \equiv a \pmod{m}.$$

If this congruence is impossible, the proposed equation has no primitive solutions. In case the congruence is possible, all primitive solutions of the equation

$$x^2 - ay^2 = m, \quad (A)$$

if they exist, are distributed into groups so that to solutions of the same group corresponds by the congruence

$$x \equiv Ny \pmod{m} \quad (B)$$

the same root N of the congruence

$$z^2 \equiv a \pmod{m}. \quad (C)$$

Primitive solutions of (A) satisfying the congruence (B) are said to belong to the root N .

A remarkable relation exists between solutions belonging to the same root N of (C). Let x, y and x', y' be any two such solutions. Then

$$x \equiv Ny, \quad x' \equiv Ny' \pmod{m},$$

whence

$$xy' - x'y \equiv 0, \quad xx' \equiv N^2yy' \equiv ayy' \pmod{m},$$

so that

$$xy' - x'y = mu, \quad xx' - ayy' = mt$$

where t and u are integers. Now the quotient

$$\frac{x' + y'\sqrt{a}}{x + y\sqrt{a}} = \frac{xx' - ayy' + (xy' - x'y)\sqrt{a}}{x^2 - ay^2};$$

but, because

$$x^2 - ay^2 = m,$$

this reduces to

$$\frac{x' + y'\sqrt{a}}{x + y\sqrt{a}} = t + u\sqrt{a}$$

or

$$x' + y'\sqrt{a} = (t + u\sqrt{a})(x + y\sqrt{a}). \quad (D)$$

Since \sqrt{a} is not a rational number, by changing \sqrt{a} into $-\sqrt{a}$ we have another relation,

$$x' - y'\sqrt{a} = (t - u\sqrt{a})(x - y\sqrt{a}),$$

and on multiplying both

$$x'^2 - ay'^2 = (t^2 - au^2)(x^2 - ay^2)$$

or, canceling $x'^2 - ay'^2 = x^2 - ay^2 = m$,

$$t^2 - au^2 = 1. \quad (E)$$

Thus, two solutions belonging to the same root of (C) are connected by the relation (D) in which t and u are integers satisfying equation (E). Vice versa, for any solution of (E), x' , y' as determined by (D) constitute a primitive solution of (A) belonging to N . It suffices to show that x' , y' are relatively prime and that

$$x'^2 - ay'^2 \equiv N^2 \pmod{m}$$

since the equation

$$x'^2 - ay'^2 = m$$

is certainly satisfied.

By separating the rational and nonrational terms in (D), we get

$$x' = tx + auy, \quad y' = ux + ty$$

and also

$$x = tx' - auy', \quad y = -ux' + ty'.$$

Hence x' and y' are relatively prime. On the other hand,

$$x' - Ny' = t(x - Ny) + u(ay - Nx).$$

But

$$ay - Nx \equiv N^2y - Nx \equiv -N(x - Ny),$$

and so

$$x' - Ny' \equiv (t - Nu)(x - Ny) \equiv 0 \pmod{m}.$$

Thus it suffices to know one solution belonging to the root N to be able to find all of them if all the integers satisfying (E)

can be found. This equation is quite trivial when $a = -A$ is a negative number. Then the equation

$$t^2 + Au^2 = 1$$

has only two solutions, $t = \pm 1, u = 0$, if $A > 1$; and four solutions

$$\begin{aligned} t &= \pm 1, & u &= 0, \\ t &= 0, & u &= \pm 1, \end{aligned}$$

if $A = 1$. Accordingly, the group of solutions belonging to the same root consists of two solutions

$$x, y; \quad -x, -y$$

if $A > 1$, and four solutions

$$x, y; \quad -x, -y; \quad -y, x; \quad y, -x$$

if $A = 1$.

When a is positive and not a square, the equation

$$t^2 - au^2 = 1$$

is by no means trivial. It was proposed by Fermat in 1657 as a challenge to English mathematicians of the time to prove that the equation has infinitely many solutions and to invent a method for the discovery of all of them. The challenge was only partially answered by Lord Brouncker, noted statesman and scholar of that epoch, who invented a method for solving Fermat's equation without being able to prove that this method will always work. The first complete proof and exhaustive discussion of Fermat's equation was made by Lagrange in 1767, and his work stands as an outstanding achievement in the history of the theory of numbers. In Sec. 5 we shall reproduce Lagrange's proof as essentially simplified by Dirichlet. Equation (\mathcal{E}) is often called the Pellian equation because of a mistaken reference by Euler. Pell never was

concerned with this equation, and, by all rights, it should be named after Fermat.

4. Application of the Fundamental Lemma. For particular values of a the fundamental lemma of Sec. 2 yields a number of interesting and important theorems, some known already to Fermat, others derived much later as corollaries of the general theory of quadratic forms. Here we shall consider the cases $a = -1, -2, -3, -5, -7$, reserving the consideration of positive a until after the Fermat equation has been dealt with.

Case 1. $a = -1$. We suppose that m is any positive number of which -1 is a quadratic residue. Then the multiplier λ will be a positive integer less than

$$\sqrt{\frac{m}{8}}.$$

The only possible choice for λ is $\lambda = 1$. Hence the equation

$$m \equiv x^2 + y^2 \pmod{m} \quad (A)$$

has solutions in integers x, y , necessarily relatively prime since their g.c.d. divides λ , and satisfying the congruence

$$x \equiv Ny \pmod{m}$$

for any chosen root N of the congruence

$$z^2 + 1 \equiv 0 \pmod{m}. \quad (B)$$

In other words, equation (A) has solutions belonging to any root of this congruence. There are exactly four solutions belonging to each root. Hence the number of primitive solutions is four times the number of roots of (B). Now this congruence is possible only if all odd prime divisors of m are of the form $4k + 1$ and m is either odd or double an odd number. The number of its solutions is 2^μ if μ is the number of distinct odd prime divisors of m . Thus we have the following theorem:

A number, which is odd or double an odd number, possessing only odd prime divisors of the form $4k + 1$, can be represented as the sum of squares of two relatively prime integers in exactly 2^{s+2} ways. Two representations

$$m = x^2 + y^2 \quad \text{and} \quad m = x'^2 + y'^2$$

are considered as different unless $x' = x, y' = y$. No number divisible by a prime of the form $4k + 3$ has primitive representations as the sum of two squares.

In particular let p be a prime of the form $4k + 1$. Then the equation

$$p = a^2 + b^2$$

has exactly 8 solutions in positive or negative integers a, b . Disregarding the signs of a, b and the order in which the squares are placed, we have the famous theorem of Fermat:

Every prime of the form $4k + 1$ can be represented as the sum of two squares, and this representation is unique.

The first statement of the theorem occurs in a letter of Fermat to Mersenne, dated December 25, 1640, and is reiterated several times in the correspondence of Fermat with other scholars. The proof of this Fermat theorem was given for the first time by Euler in 1754.

The number of all solutions of equation (A), primitive or not, is the aggregate of numbers of primitive solutions of all the equations

$$x^2 + y^2 = \frac{m}{\delta^2},$$

corresponding to all square divisors δ^2 of m . Now if some prime of the form $4k + 3$ enters into m in an odd power, m/δ^2 will always contain this prime divisor. Hence none of the equations

$$x^2 + y^2 = \frac{m}{\delta^2}$$

will have primitive solutions, and m cannot be represented as the sum of two squares. Suppose now that all prime divisors of the form $4k + 3$ occur in m in even powers; then we can set

$$m = Q^2 M$$

where Q contains only primes of the form $4k + 3$ and M contains only primes of the form $4k + 1$ if m , as we shall assume, is odd. Then x, y in the equation

$$x^2 + y^2 = m$$

must be both divisible by Q , and the number of its solutions will be exactly the same as that of

$$x^2 + y^2 = M.$$

Denote by $\psi(n)$ the numbers of roots of the congruence

$$z^2 + 1 \equiv 0 \pmod{n}.$$

Then the number of all solutions of the equation

$$x^2 + y^2 = M$$

will be

$$4 \sum \psi\left(\frac{M}{\delta^2}\right),$$

where the summation extends over all square divisors of M . But this sum has another very simple arithmetical meaning. The solutions of the equation

$$xy = M$$

again can be classified into primitive and derived solutions. There are 2^μ primitive solutions if M contains μ distinct prime factors and $2^\mu = \psi(M)$. Consequently the total number of solutions will be

$$\sum \psi\left(\frac{M}{\delta^2}\right),$$

but on the other hand it is $\tau(M)$ —the number of divisors of M . Thus the number of all solutions of the equation

$$x^2 + y^2 = Q^2M$$

is $4\tau(M)$. Since $m = Q^2M$ is an odd number, one of the numbers x, y is odd and the other even. Supposing y to be even, the number of solutions will be $2\tau(M)$, and it reduces to $\tau(M)$ if x is positive. If m is not a square, y is different from 0. Taking it positive, the number of solutions becomes $\frac{1}{2}\tau(M)$. In case M is a square $= s^2, s > 0$, there is one solution $x = s, y = 0$, with x positive. For the remaining $\tau(M) - 1$ solutions y is different from 0 and, taking y positive, we have $\frac{1}{2}\tau(M) - \frac{1}{2}$ solutions with positive x and y .

Paying attention to the squares themselves and not to their roots, and disregarding the order of squares, we conclude that the number of *partitions* of M into the sum of two squares is

$$\begin{aligned} & \frac{1}{2}\tau(M) \text{ if } M \text{ is not a square;} \\ & \frac{1}{2}\tau(M) + \frac{1}{2} \text{ if } M \text{ is a square;} \end{aligned}$$

provided M has no prime divisors of the form $4k + 3$. This rule was also given by Fermat.

Let us take, for example, $m = 325 = 5^2 \cdot 13$. Since there are no prime divisors of the form $4k + 3$, we have $Q = 1, M = 325$, and $\tau(325) = 6$. Correspondingly, there are three partitions of 325 into the sum of two squares. Indeed, we find by trial

$$325 = 1^2 + 18^2 = 15^2 + 10^2 = 17^2 + 6^2.$$

For another example take $m = 38,025 = 3^2 \cdot 5^2 \cdot 13^2$, so that $Q = 3, M = 65^2$, and $\tau(M) = 9$. The number of requested partitions is

$$\frac{9}{2} + \frac{1}{2} = 5.$$

They are

$$38,025 = 195^2 + 0^2 = 189^2 + 48^2 = 117^2 + 156^2 \\ = 99^2 + 168^2 = 75^2 + 180^2.$$

The number of all solutions of the equation

$$x^2 + y^2 = m$$

in all cases can be very elegantly expressed through the numerical function

$$\rho(m) = \sum (-1)^{\frac{d-1}{2}},$$

where the summation extends over all odd divisors of m . Clearly

$$\rho(2m) = \rho(m),$$

so that we may confine ourselves to odd values of m only. If all prime divisors of m are of the form $4k + 1$, then for all divisors $d \equiv 1 \pmod{4}$, and $\rho(m)$ coincides with $\tau(m)$. If m is divisible by a prime p of the form $4k + 3$, then we can set $m = p^a m'$ with m' nondivisible by p . All the divisors of m coincide with

$$d', pd', p^2 d', \dots, p^a d',$$

letting d' run through the divisors of m' . But since in general

$$\frac{PQ - 1}{2} \equiv \frac{P - 1}{2} + \frac{Q - 1}{2} \pmod{2}$$

for odd P, Q the sum

$$(-1)^{\frac{d'-1}{2}} + (-1)^{\frac{pd'-1}{2}} + \dots + (-1)^{\frac{p^a d'-1}{2}}$$

is equal to

$$(-1)^{\frac{d'-1}{2}} (1 + (-1) + (-1)^2 + \dots + (-1)^a),$$

which is 0 if a is odd and

$$(-1)^{\frac{a-1}{2}}$$

if a is even. Hence $\rho(m) = 0$ if a prime p of the form $4k + 3$ enters into m in an odd power; otherwise

$$\rho(m) = \rho(m').$$

By repeated application of this result we conclude that for $m = Q^2M$ where Q contains only prime divisors of the form $4k + 3$, while M has no such divisors,

$$\rho(m) = \rho(M) = \tau(M).$$

Referring therefore to the previously established results, we see that for all odd m

$$4\rho(m)$$

gives the number of representations of m by the sum of two squares. The same is also true for an even $m = 2m'$. For both equations

$$x^2 + y^2 = n \quad \text{and} \quad x'^2 + y'^2 = 2n$$

have the same number of solutions, since to any solution of the first corresponds a unique solution of the second, and vice versa, if we take

$$x' = x + y, \quad y' = x - y,$$

whence conversely

$$x = \frac{x' + y'}{2}, \quad y = \frac{x' - y'}{2}$$

Thus the number of solutions is not changed when m is replaced by $2m$, and the same change does not alter the value of the function $\rho(m)$. Hence we derive the elegant result of Jacobi: the number of all representations of m by the sum

of two squares is four times the difference between the number of divisors of m of the forms $4k + 1$ and $4k + 3$, respectively.

Now that we have dwelt at length on the equation

$$x^2 + y^2 = m,$$

the other cases will be discussed only briefly.

Case 2. $a = -2$. The multiplier λ satisfies the inequality

$$\lambda < \sqrt{\frac{8}{3}},$$

whence $\lambda = 1$. Hence if -2 is a quadratic residue of m , the equation

$$x^2 + 2y^2 = m$$

has primitive solutions belonging to any chosen root of the congruence

$$z^2 + 2 \equiv 0 \pmod{m},$$

and to each root correspond exactly two solutions. In particular if p is a prime either of the form $8k + 3$ or of the form $8k + 1$, and we consider only positive solutions, the equation

$$p = x^2 + 2y^2$$

has always one and only one solution. This is another theorem stated by Fermat and proved for the first time by Euler and Lagrange.

Case 3. $a = -3$. The multiplier λ now can have two values 1 and 2, so that either

$$x^2 + 3y^2 = m$$

or

$$x^2 + 3y^2 = 2m.$$

If m is odd, the last equation is impossible, since when x and y are both even or both odd, $x^2 + 3y^2$ is always divisible by 4. Hence for an odd m of which -3 is a quadratic residue, the equation

$$x^2 + 3y^2 = m$$

has primitive solutions belonging to any root of the congruence

$$z^2 + 3 \equiv 0 \pmod{m}$$

and exactly two for each root. In particular, for each prime of the form $6k + 1 = p$ the equation

$$p = x^2 + 3y^2$$

has one and only one solution in positive numbers. This is the third theorem stated by Fermat and proved by Euler.

Case 4. $a = -5$. In this case

$$\lambda < \sqrt{\frac{20}{3}},$$

so that $\lambda = 1$ or $\lambda = 2$, and the fundamental lemma shows that either

$$x^2 + 5y^2 = m$$

or

$$x^2 + 5y^2 = 2m,$$

while

$$x \equiv Ny \pmod{m}$$

for each root of the congruence

$$z^2 + 5 \equiv 0 \pmod{m}.$$

Let m be an odd number nondivisible by 5. Then necessarily

$$\left(\frac{-5}{m}\right) = 1,$$

and by the reciprocity law

$$\left(\frac{m}{5}\right) = (-1)^{\frac{m-1}{2}}.$$

To distinguish between the two equations, notice that they imply the respective congruences

$$m \equiv x^2 \pmod{5} \quad \text{or} \quad m \equiv -2x^2 \pmod{5}.$$

Since $-2N5$, we have correspondingly

$$\left(\frac{m}{5}\right) = 1 \quad \text{or} \quad \left(\frac{m}{5}\right) = -1.$$

Hence if

$$\left(\frac{m}{5}\right) = 1 \quad \text{and} \quad (-1)^{\frac{m-1}{2}} = 1;$$

that is, $m = 20k + 1$ or $m = 20k + 9$; then necessarily

$$x^2 + 5y^2 = m,$$

but

$$x^2 + 5y^2 = 2m$$

if

$$\left(\frac{m}{5}\right) = -1 \quad \text{and} \quad (-1)^{\frac{m-1}{2}} = -1;$$

that is, $m = 20k + 3$ or $m = 20k + 7$, provided that in both cases -5 is a quadratic residue of m . In particular, for every prime of one of the forms $p = 20k + 1$ or $p = 20k + 9$, the equation

$$x^2 + 5y^2 = p$$

has one and only one solution in positive integers, while for primes of one of the forms $20k + 3$ or $20k + 7$, the same is true of the equation

$$x^2 + 5y^2 = 2p.$$

Case 5. $a = -7$. In this case

$$\lambda < \sqrt{\frac{28}{5}},$$

so that $\lambda = 1, 2, 3$. Now since $-7Rm$ by the reciprocity law

$$\left(\frac{m}{7}\right) = 1$$

provided m is odd and not divisible by 7. The equation

$$x^2 + 7y^2 = 3m$$

implies

$$\left(\frac{3m}{7}\right) = 1$$

or

$$\left(\frac{3}{7}\right) = 1,$$

which is not true. On the other hand, the equation

$$x^2 + 7y^2 = 2m$$

is also impossible, since $x^2 + 7y^2$ is divisible by 4 if it is even. Consequently the equation

$$x^2 + 7y^2 = m$$

can be solved in integers so that

$$x \equiv Ny \pmod{m}$$

for any root of the congruence

$$z^2 + 7 \equiv 0 \pmod{m}.$$

provided m is odd and prime to 7. In particular, if p is a prime of one of the forms $7k + 1$, $7k + 2$, $7k + 4$, the equation

$$p = x^2 + 7y^2$$

has one and only one solution in positive integers.

Exercises and Problems

1. Prove that for all primes of one of the forms $p = 24k + 1$ or $p = 24k + 7$, the equation

$$x^2 + 6y^2 = p$$

has one and only one solution in positive integers. For primes $p = 24k + 5$ or $p = 24k + 11$, the same is true of the equation

$$2x^2 + 3y^2 = p.$$

2. Every prime of the form $40k + 1$, $40k + 9$, $40k + 11$, $40k + 19$ can be represented in the form

$$p = x^2 + 10y^2,$$

and every prime of the form $40k + 7$, $40k + 13$, $40k + 23$, $40k + 37$ can be represented in the form

$$p = 2x^2 + 5y^2$$

and in one way only if x and y are positive.

3. Primes $p \equiv 1, 4 \pmod{15}$ can be represented in the form

$$x^2 + 15y^2 = p,$$

and primes $p \equiv 2, 8 \pmod{15}$ can be represented in the form

$$3x^2 + 5y^2 = p$$

in one way only if x and y are positive.

4. The number of all solutions of the equation

$$x^2 + 2y^2 = n$$

is expressed by

$$2 \sum \left(\frac{-2}{d} \right),$$

where the sum extends over all odd divisors of n .

5. The number of all solutions of the respective equations

$$x^2 + 3y^2 = n, \quad x^2 + 7y^2 = n$$

for an odd n is expressed by

$$2 \sum \left(\frac{-3}{d} \right), \quad 2 \sum \left(\frac{-7}{d} \right),$$

the sums extending over all divisors of n .

5. Fermat's Equation. If $m + 1$ or more objects are to be distributed on m places, at least two objects will occupy the same place. This is an evident and trivial principle which is remarkable from the standpoint that in many cases it serves

to prove quite difficult propositions. We shall use it to prove the following lemma:

If ξ is a real number, and $\tau > 1$ is any integer, then two integers r and s can be found satisfying the inequalities

$$|s\xi - r| < \frac{1}{\tau}, \quad 0 < s \leq \tau.$$

Attribute to x integral values $0, 1, 2, \dots, \tau$ and for each of them determine y , so that

$$0 \leq x\xi - y < 1.$$

We get thus $\tau + 1$ differences

$$x\xi - y,$$

all contained between 0 and 1, excluding 1 and including 0. Divide the interval from 0 to 1 into τ equal intervals of length $1/\tau$: from 0 to $1/\tau$ excluding $1/\tau$; from $1/\tau$ to $2/\tau$ excluding $2/\tau$; . . . , from $(\tau - 1)/\tau$ to 1 excluding 1. Since $\tau + 1$ numbers $x\xi - y$ are distributed in τ intervals, at least two numbers

$$x'\xi - y' \quad \text{and} \quad x''\xi - y''; \quad x'' > x'$$

will fall in the same interval. Then, setting

$$x'' - x' = s, \quad y'' - y' = r,$$

we shall have

$$0 < s \leq \tau$$

and

$$|s\xi - r| < \frac{1}{\tau}$$

since if two numbers belong to the same interval of length $1/\tau$ their difference is numerically less than $1/\tau$.

Let now a be a positive integer but not a square, so that \sqrt{a} is an irrational number. By the lemma, for an integer

$\tau > 1$ two integers $r, s > 0$ can be found so that

$$|r - s\sqrt{a}| < \frac{1}{\tau}, \quad 0 < s \leq \tau.$$

Then also

$$|r + s\sqrt{a}| < \frac{1}{\tau} + 2\tau\sqrt{a}$$

and

$$|r^2 - as^2| < 2\sqrt{a} + \frac{1}{\tau^2} < 2\sqrt{a} + 1.$$

That is, integers r, s , making $r - s\sqrt{a}$ as small as we please numerically, can be found in an infinite number for which

$$|r^2 - as^2| < 2\sqrt{a} + 1.$$

Let $[2\sqrt{a} + 1] = g$; then the number of integers, excluding 0, between

$$-2\sqrt{a} - 1 \quad \text{and} \quad 2\sqrt{a} + 1$$

will be $2g$. Take $n = 2g^2$ pairs of integers $r_1, s_1; r_2, s_2; \dots; r_n, s_n$ satisfying the inequalities

$$|r_i^2 - as_i^2| < 2\sqrt{a} + 1; \quad i = 1, 2, \dots, n$$

and so chosen that

$$|r_1 - s_1\sqrt{a}| > |r_2 - s_2\sqrt{a}| > |r_3 - s_3\sqrt{a}| > \dots$$

The differences

$$r_1^2 - as_1^2, \quad r_2^2 - as_2^2, \quad \dots, \quad r_n^2 - as_n^2 \quad (A)$$

represent integers contained between $-2\sqrt{a} - 1$ and $2\sqrt{a} + 1$. Let these integers be L_1, L_2, \dots, L_{2g} , and let M_α denote the number of times L_α occurs in the series (A). Then

$$M_1 + M_2 + \dots + M_{2g} = n = 2g^2$$

and the greatest of the numbers M_1, M_2, \dots, M_{2g} is necessarily $\geq g^3$. That is to say, for some $k = \pm 1, \pm 2, \dots, \pm g$, the equation

$$r^2 - as^2 = k \quad (B)$$

is satisfied by at least $g^3 > g^2 \geq k^2$ pairs of integers r, s .

Let us agree to call two pairs of integers x', y' and x'', y'' congruent mod k if and only if

$$x'' \equiv x', \quad y'' \equiv y' \pmod{k}.$$

Then the number of incongruent pairs is k^2 , and among the $k^2 + 1$ pairs at least two pairs are congruent. Since equation (B) is satisfied by more than k^2 pairs, at least two of them, r'', s'' and r', s' will be congruent mod k , so that

$$\begin{aligned} r''^2 - as''^2 &= r'^2 - as'^2 = k, \\ r'' &\equiv r', \quad s'' \equiv s' \pmod{k}. \end{aligned}$$

Moreover, we can suppose that $\frac{r'' - s''\sqrt{a}}{k} < \frac{r' - s'\sqrt{a}}{k}$.

$$|r'' - s''\sqrt{a}| < |r' - s'\sqrt{a}|.$$

Consider now the quotient

$$\frac{r' - s'\sqrt{a}}{r'' - s''\sqrt{a}} = \frac{r'r'' - as's'' + (r's'' - r''s')\sqrt{a}}{k}$$

By virtue of the congruences $r'' \equiv r', s'' \equiv s' \pmod{k}$,

$$r'r'' - as's'' \equiv r'^2 - as'^2 \equiv 0, \quad r's'' - r''s' \equiv 0 \pmod{k},$$

so that

$$\frac{r'r'' - as's''}{k} = t, \quad \frac{r's'' - r''s'}{k} = u$$

are integers and

$$(r' - s'\sqrt{a}) = (r'' - s''\sqrt{a})(t + u\sqrt{a}),$$

whence

$$r'^2 - s'^2 a = (r''^2 - s''^2 a)(t^2 - au^2)$$

and, canceling $r''^2 - as''^2 = r'^2 - as'^2 = k \neq 0$, we have

$$t^2 - au^2 = 1.$$

Besides,

$$|t + u\sqrt{a}| > 1,$$

so that $u \neq 0$. It is thus proved that Fermat's equation

$$t^2 - au^2 = 1$$

has solutions in integers distinct from the trivial solution $t = \pm 1, u = 0$.

Let T and U be the two smallest positive integers satisfying Fermat's equation; they constitute the so-called *fundamental* solution. If t, u is any solution in positive integers distinct from the fundamental solution, then $u > U$ and

$$t + u\sqrt{a} > T + U\sqrt{a}.$$

Consequently, in the series of powers

$$T + U\sqrt{a}, (T + U\sqrt{a})^2, (T + U\sqrt{a})^3, \dots$$

there are two consecutive terms such that

$$(T + U\sqrt{a})^n \leq t + u\sqrt{a} < (T + U\sqrt{a})^{n+1}.$$

Since

$$(T - U\sqrt{a})(T + U\sqrt{a}) = 1,$$

we can write also

$$1 \leq (t + u\sqrt{a})(T - U\sqrt{a})^n < T + U\sqrt{a}.$$

Now

$$(t + u\sqrt{a})(T - U\sqrt{a})^n$$

can be reduced to the form $p + q\sqrt{a}$ where p, q are integers and

$$p^2 - aq^2 = 1.$$

Consequently

$$1 \leq p + q\sqrt{a} < T + U\sqrt{a}$$

and

$$0 < T - U\sqrt{a} < p - q\sqrt{a} \leq 1.$$

From these inequalities it follows that

$$p > 0, \quad 0 \leq q < U.$$

As to q , it cannot be positive; otherwise there would be a solution in positive integers smaller than T, U . Therefore $p = 1, q = 0$, and

$$t + u\sqrt{a} = (T + U\sqrt{a})^n.$$

In other words, all solutions in positive integers result from this formula for $n = 1, 2, 3, \dots$

If $t > 0, u < 0$, then

$$t - u\sqrt{a} = (T - U\sqrt{a})^n$$

for some positive n , whence

$$t + u\sqrt{a} = (T - U\sqrt{a})^n = (T + U\sqrt{a})^{-n}.$$

Finally, from any solution t, u the solution $\pm t, \pm u$ with $\pm t > 0$ results from a proper choice of the sign \pm . Thus all the solutions of Fermat's equation, without any exception, are obtained from the fundamental solution by equating the rational and irrational parts in the relation

$$t + u\sqrt{a} = \pm (T + U\sqrt{a})^n,$$

in which the signs are chosen arbitrarily and $n = 0, \pm 1, \pm 2, \dots$. As to the fundamental solution, it can be found by a very convenient process based on the use of continued fractions, but we cannot enter into any details concerning this point.

By trials one finds the following fundamental solutions for $a = 2, 3, 5$:

$$\begin{array}{lll} T^2 - 2U^2 = 1; & T = 3, & U = 2 \\ T^2 - 3U^2 = 1; & T = 2, & U = 1 \\ T^2 - 5U^2 = 1; & T = 9, & U = 4. \end{array}$$

6. The Equation $x^2 - ay^2 = m$ with Positive a . We have seen in Sec. 3 that the primitive solutions of this equation, belonging to the same root of the congruence

$$z^2 \equiv a \pmod{m},$$

are obtained from one of them x, y by means of the relation

$$x' + y'\sqrt{a} = (t + u\sqrt{a})(x + y\sqrt{a}),$$

where t, u are solutions of Fermat's equation

$$t^2 - au^2 = 1.$$

Since

$$t + u\sqrt{a} = \pm(T + U\sqrt{a})^n$$

for either one of the signs forms a geometric progression with the ratio $T + U\sqrt{a}$, it is easy to see that in a group of solutions belonging to the same root there will be a unique solution singled out by the inequalities

$$M(T + U\sqrt{a})^{-1} < x + y\sqrt{a} \leq M(T + U\sqrt{a})^{\frac{1}{2}},$$

M being an arbitrary positive number. Supposing $m > 0$, we shall take $M = \sqrt{m}$; considering that

$$x^2 - ay^2 = m,$$

the preceding inequalities will be entirely equivalent to

$$\begin{aligned} (x - y\sqrt{a})(T - U\sqrt{a}) &< x + y\sqrt{a} \\ &\leq (x - y\sqrt{a})(T + U\sqrt{a}) \end{aligned}$$

together with

$$x + y\sqrt{a} > 0.$$

On simplifying them and noticing that

$$\frac{T-1+U\sqrt{a}}{T+1+U\sqrt{a}} = \frac{U\sqrt{a}}{T+1}$$

by virtue of the equation

$$T^2 - aU^2 = 1,$$

we find

$$-\frac{U}{T+1}x < y \leq \frac{U}{T+1}x,$$

where necessarily $x > 0$. Since

$$x + y\sqrt{a} > \frac{x}{T+1}(T+1 - U\sqrt{a})$$

and

$$T > U\sqrt{a},$$

the condition

$$x + y\sqrt{a} > 0$$

will be also fulfilled. Consequently, from all solutions in the group a unique solution is singled out by the inequalities

$$-\frac{U}{T+1}x < y \leq \frac{U}{T+1}x.$$

Combined with the equation itself,

$$x^2 - ay^2 = m,$$

they give

$$x^2 \leq m + a\frac{U^2}{(T+1)^2}x^2$$

or

$$\sqrt{m} \leq x \leq \sqrt{\frac{T+1}{2}m},$$

which for $y \geq 0$ is entirely equivalent to the original inequalities. For $y \geq 0$ they can be also replaced by

$$0 \leq y \leq \sqrt{\frac{T-1}{2a}}m.$$

Now we shall consider the particular cases: $a = 2, 3, 5$.

Case 1. $a = 2$. The multiplier λ in the fundamental lemma satisfies the inequality

$$|\lambda| < \sqrt{\frac{3}{2}},$$

and so $\lambda = 1$ or $\lambda = -1$. In case $\lambda = -1$, integers x', y' exist satisfying the equation

$$x'^2 - 2y'^2 = -m,$$

and the congruence

$$x' - 2y' \equiv N \pmod{m}$$

for any root N of the congruence

$$z^2 \equiv 2 \pmod{m}.$$

But we have identically

$$2(y' - x')^2 - (x' - 2y')^2 = x'^2 - 2y'^2$$

and

$$\begin{aligned} x' - 2y' - N(y' - x') &\equiv x' - Ny' + N(x' - Ny') \\ &\equiv 0 \pmod{m}. \end{aligned}$$

Hence

$$x = x' - 2y', \quad y = y' - x'$$

is a primitive solution of the equation

$$x^2 - 2y^2 = m$$

belonging to N . The existence of such a solution in case $\lambda = 1$ follows directly from the fundamental lemma.

Thus whenever 2 is a quadratic residue of m , there are solutions of the equation

$$x^2 - 2y^2 = m$$

belonging to any chosen root of the congruence

$$z^2 \equiv 2 \pmod{m}.$$

In each group of solutions belonging to the same root, there is one and only one for which

$$-\frac{1}{2}x < y \leq \frac{1}{2}x.$$

In particular, for every prime p of one of the forms $8k + 1$ or $8k + 7$, the equation

$$x^2 - 2y^2 = p$$

has a unique solution in positive integers satisfying the inequalities

$$x > 2y \quad \text{Downloaded from www.dbraulibrary.org.in}$$

equivalent to

$$\sqrt{p} < x < \sqrt{2p}$$

or to

$$y < \sqrt{\frac{1}{2}p}.$$

For the congruence

$$z^2 \equiv 2 \pmod{p}$$

has two roots, N and $-N$, and if the solution x, y in positive integers belongs to N , then $x, -y$ belongs to $-N$.

Case 2. $a = 3$. In this case

$$|\lambda| \leq 2,$$

and so there are four possibilities

$$\begin{array}{ll} (a) \ x^2 - 3y^2 = m, & (b) \ x^2 - 3y^2 = -2m \\ (c) \ x^2 - 3y^2 = -m, & (d) \ x^2 - 3y^2 = 2m, \end{array}$$

while

$$x - Ny \equiv 0 \pmod{m}$$

for any chosen root N of the congruence.

$$z^2 \equiv 3 \pmod{m}.$$

We shall suppose that m is odd and prime to 3; then x and y are necessarily relatively prime. In all cases

$$\left(\frac{3}{m}\right) = (-1)^{\frac{m-1}{2}} \left(\frac{m}{3}\right) = 1,$$

while in cases (a) and (b)

$$\left(\frac{m}{3}\right) = 1,$$

whereas in cases (c) and (d)

$$\left(\frac{m}{3}\right) = -1.$$

Thus if

$$(-1)^{\frac{m-1}{2}} = 1, \quad \left(\frac{m}{3}\right) = 1;$$

that is, if $m \equiv 1 \pmod{12}$, (a) and (b) are the only possibilities; on the contrary, (c) and (d) are the only possibilities if

$$(-1)^{\frac{m-1}{2}} = -1 \quad \left(\frac{m}{3}\right) = -1;$$

that is, if $m \equiv -1 \pmod{12}$.

In cases (b) and (d), x and y are necessarily odd, and we can set $x = 2z + y$, which gives

$$(y - z)^2 - 3z^2 = m$$

corresponding to (b) and

$$(y - z)^2 - 3z^2 = -m$$

corresponding to (d). Now

$$\begin{aligned} y - z - Nz &\equiv \frac{3y - x}{2} - N\frac{x - y}{2} \equiv \frac{N^2y - x}{2} - N\frac{x - y}{2} \\ &\equiv \frac{1}{2}N(Ny - x) + \frac{1}{2}(Ny - x) \equiv 0 \pmod{m}, \end{aligned}$$

and so we come to the following conclusion:

If m is an odd number prime to 3 of which 3 is a quadratic residue, then in case $m \equiv 1 \pmod{12}$, the equation

$$x^2 - 3y^2 = m$$

possesses solutions belonging to any chosen root of the congruence

$$z^2 \equiv 3 \pmod{m};$$

while the same holds for the equation

$$x^2 - 3y^2 = -m$$

in case $m \equiv -1 \pmod{12}$. In the group of solutions belonging to the same root, there is one and only one solution for which

$$-\frac{1}{3}x < y \leq \frac{1}{3}x$$

in case of positive $m \equiv 1 \pmod{12}$ and

$$-y < x \leq y$$

in case of positive $m \equiv -1 \pmod{12}$. The proof of the last statement is left as a problem for the reader.

In particular, for every prime $p \equiv 1 \pmod{12}$ the equation

$$x^2 - 3y^2 = p$$

has only one solution in positive integers satisfying the inequality

$$y < \sqrt{\frac{1}{3}p}$$

or

$$\sqrt{p} < x < \sqrt{\frac{3}{2}p}.$$

For a prime $p \equiv 11 \pmod{12}$, the equation

$$3x^2 - y^2 = p$$

has only one solution in positive integers in which

$$x < \sqrt{\frac{1}{2}p}.$$

Case 3. $a = 5$. In this case

$$|\lambda| < \sqrt{\frac{20}{3}},$$

so that $\lambda = \pm 1, \lambda = \pm 2$. The equations

$$x^2 - 5y^2 = \pm 2m$$

are, however, impossible if m is odd, and so only two cases remain:

$$(a) \quad x^2 - 5y^2 = m \qquad (b) \quad x^2 - 5y^2 = -m.$$

But in case (b)

$$(2x - 5y)^2 - 5(2y - x)^2 = m$$

and

$$2x - 5y - N(2y - x) \equiv 2(x - Ny) + N(x - Ny) \equiv 0 \pmod{m}.$$

That is, equation

$$x^2 - 5y^2 = m$$

has primitive solutions belonging to any root of the congruence

$$z^2 \equiv 5 \pmod{m}$$

provided m is an odd number of which 5 is a quadratic residue.

In the group of solutions belonging to the same root there is only one solution for which

$$-\frac{2}{3}x < y \leq \frac{2}{3}x.$$

In particular, every prime $p \equiv \pm 1 \pmod{5}$ can be represented in the form

$$p = x^2 - 5y^2$$

and in one way only if x, y are positive and

$$y < \sqrt{\frac{4}{5}p}.$$

7. A Test of Primality. The particular equations of the form

$$x^2 - ay^2 = m$$

studied in Secs. 4 and 6 possess primitive solutions belonging to each root of the congruence $z^2 \equiv a \pmod{m}$

$$z^2 \equiv a \pmod{m}$$

whenever the latter is possible. In consequence of this, the prime numbers of which a is a quadratic residue can be represented by the form

$$x^2 - ay^2$$

in one way only with positive x and y limited by additional inequalities in case $a > 0$, while composite numbers either have no such primitive representations at all or more than one, or else have imprimitive representations also. Hence we derive a new and efficient method for testing whether a given number is prime or not, and often can even factorize m if it is not prime. For if there are two representations

$$r^2 - as^2 = r'^2 - as'^2 = m$$

of the requested kind and one of them belongs to the root N , the other must belong to another root N' of the congruence

$$z^2 \equiv a \pmod{m}$$

different from N and $-N$. Then since

$$(N' + N)(N' - N) \equiv 0 \pmod{m},$$

while neither $N' + N$ nor $N' - N$ is divisible by m , the g.c.d. of $N' - N$ or $N' + N$ and m is a factor of m . But from the congruences

$$r \equiv Ns, \quad r' \equiv N's' \pmod{m}$$

it follows that

$$rs' \mp r's \equiv (N \mp N')ss' \pmod{m},$$

and ss' being prime to m , the g.c.d. of $rs' \mp r's$ and m will be the same as the g.c.d. of $N \mp N'$ and m . If it happens that m has no representations by the form $x^2 - ay^2$, then m is certainly composite, but the factorization of m must be sought elsewhere.

The quadratic forms

$$(a) \ x^2 + 4y^2, \quad (b) \ x^2 + 2y^2, \quad (c) \ x^2 - 2y^2$$

suffice to test all integers. That is to say, integers $\equiv 1 \pmod{4}$ can be tested by (a); integers $\equiv 1$ or $3 \pmod{8}$ can be tested by (b); and integers $\equiv 1$ or $7 \pmod{8}$ can be tested by (c).

Another group of forms

$$(a) \ x^2 + 4y^2, \quad (b) \ x^2 + 3y^2, \\ (c) \ x^2 - 3y^2, \quad (d) \ 3x^2 - y^2$$

can serve the same purpose. For numbers $\equiv 1 \pmod{12}$ can be tested by (a), (b), (c); numbers $\equiv 5 \pmod{12}$ by (a); numbers $\equiv 7 \pmod{12}$ by (b); and numbers $\equiv 11 \pmod{12}$ by (d).

8. The Exclusion Method. The testing of a given number for primality by the method explained in the preceding

section requires the solution of equations of the form

$$fx^2 + gy^2 = m$$

in positive integers within a certain range. This can be done by trials greatly abbreviated by the exclusion process similar to the one described in Sec. 19, Chap. X. A number E , usually a small prime or power of a small prime, is taken as the excludent. The equation

$$fx^2 + gy^2 = m$$

is certainly impossible if the congruence

$$fx^2 + gy^2 \equiv m \pmod{E}$$

is impossible. Hence all the values of x which make the fraction

$$\frac{m - fx^2}{g}$$

congruent mod E to a quadratic nonresidue mod E must be eliminated. The application of a few excludents reduces the number of values of x so considerably that the trial of remaining values is not burdensome. To facilitate the use of excludents, it is good to have short auxiliary tables from which values of x to be excluded can be found directly. Such tables are given here for the excludents $E = 5, 7, 8, 9, 11, 13$.

$$E = 5$$

$-fgR5$

$\frac{m}{f} \equiv 1$	2	3	4
2	0	0	1
3	2	1	4
	3	4	

1, 4 R

$-fgN5$

$\frac{m}{f} \equiv 1$	2	3	4
0	1	2	0
	4	3	

2, 3 N

$$E = 7$$

 $-fgR7$

$\frac{m}{f} \equiv 1$	2	3	4	5	6
0	0	1	0	1	2
2	1	3	3	2	3
5	6	4	4	5	4
		6		6	5

1, 2, 4 R

 $-fgN7$

$\frac{m}{f} \equiv 1$	2	3	4	5	6
3	2	0	1	0	0
4	5	2	6	3	1
		5		4	6

3, 5, 6 N

$$E = 8$$

$-fg \equiv 1 \pmod{8}$

$-fg \equiv 5 \pmod{8}$

$-fg \equiv 3 \pmod{8}$

$-fg \equiv 7 \pmod{8}$

$\frac{m}{f} \equiv 1$	3	5	7
0	0	0	1
2	1	2	2
4	3	4	3
6	4	6	5
	5		6
	7		7

$\frac{m}{f} \equiv 1$	3	5	7
0	1	0	0
2	2	2	1
4	3	4	3
6	5	6	4
	6		5
	7		7

$\frac{m}{f} \equiv 1$	5
0	2
4	6

$\frac{m}{f} \equiv 1$	5
2	0
6	4

$-fg \equiv 2, 4, 6 \pmod{8}, f \text{ odd}$

0, 2, 4, 6 (mod 8) are excluded.

$f \equiv 2, 4, 6 \pmod{8}$

c value of the reduced fraction $\frac{m-g}{f} \pmod{4}$ or 2

$c \equiv 0$	1
1	0
3	2
5	4
7	6

$E = 9$

--fgR9

$\frac{m}{f} \equiv 1$	2	4	5	7	8
0	1	0	1	0	1
2	2	1	2	1	2
3	4	3	4	2	4
4	5	4	5	3	5
5	7	5	7	6	7
6	8	6	8	7	8
7		8		8	

1, 4, 7 R

--fgN9

$\frac{m}{f} \equiv 1$	2	4	5	7	8
2	0	1	0	1	0
4	3	4	3	2	3
5	6	5	6	7	6
7		8		8	

2, 5, 8 N

$E = 11$

--fgR11

$\frac{m}{f} \equiv 1$	2	3	4	5	6	7	8	9	10
0	1	0	0	0	1	2	2	0	1
3	2	3	1	1	4	3	4	2	3
5	3	4	5	2	5	5	5	4	4
6	8	7	6	9	6	6	6	7	7
8	9	8	10	10	7	8	7	9	8
	10			10	9	9			10

1, 3, 4, 5, 9 R

--fgN11

$\frac{m}{f} \equiv 1$	2	3	4	5	6	7	8	9	10
2	0	1	3	3	0	0	0	1	0
3	4	5	2	1	4	5	2	3	4
7	5	9	7	6	3	4	3	6	5
9	6	10	8	8	8	7	8	10	6
	7			9	10	10			9

2, 6, 7, 8, 10 N

$E = 13$

--fgR13

$\frac{m}{f} \equiv 1$	2	3	4	5	6	7	8	9	10	11	12
3	0	1	3	0	0	0	0	1	2	0	1
4	2	3	5	4	1	1	1	2	4	2	2
5	3	6	6	5	2	3	4	4	5	3	6
8	6	7	7	6	5	5	6	9	8	4	7
9	7	10	8	7	8	8	7	11	9	9	11
10	10	12	10	8	11	10	9	12	11	10	12
	11			9	12	12	12			11	

1, 3, 4, 9, 10, 12 R

-fgN13

$\frac{m}{f} \equiv 1$	2	3	4	5	6	7	8	9	10	11	12
0	1	0	0	1	3	2	2	0	0	1	0
2	4	2	1	2	4	4	3	5	1	5	3
6	5	5	4	3	6	6	5	6	3	6	4
7	8	8	9	10	7	7	8	7	10	7	9
11	9	11	12	11	9	9	10	8	12	8	10
	12			12	10	11	11			12	

2, 5, 6, 7, 8, 11 N

We shall illustrate now the use and efficiency of the exclusion method by a few examples.

Example 1. Find whether or not 50,321 is a prime number. Since $50,321 \equiv 1 \pmod{8}$, we can use the three forms

$$4x^2 + y^2, \quad x^2 + 4y^2, \quad \text{and} \quad 2y^2.$$

Let us take the first. Accordingly, we must seek all solutions of the equation

$$4x^2 + y^2 = 50,321$$

in positive integers. Evidently

$$x^2 < \frac{50,321}{4},$$

which shows that only the following values of x must be tried:

$$x = 1, 2, 3, \dots, 112.$$

The greatest majority of them will be removed by applying the excludents 5, 7, 8, 9, 11, 13. We have $f = 4$, $g = 1$, $-fg = -4$. Now for $E = 5$

$$-fgR5, \quad \frac{m}{f} \equiv \frac{1}{4} \equiv 4 \pmod{5}.$$

By the corresponding table, values of $x \equiv 1$ or $4 \pmod{5}$ must be excluded. Similarly for other excludents we have

			Numbers to be excluded =
$E = 7;$	$-fgN7;$	$\frac{m}{f} \equiv 3 \pmod{7}$	<u>0, 2, 5</u>
$E = 8;$			<u>1, 3, 5, 7</u>
$E = 9;$	$-fgN9;$	$\frac{m}{f} \equiv 5 \pmod{9}$	<u>0, 3, 6</u>
$E = 11;$	$-fgN11;$	$\frac{m}{f} \equiv 10 \pmod{11}$	<u>0, 2, 5, 6, 9</u>
$E = 13;$	$-fgR13;$	$\frac{m}{f} \equiv 6 \pmod{13}$	<u>0, 1, 2, 5, 8, 11, 12.</u>

The numbers congruent to the underlined numbers for the respective moduli must be excluded. The exclusion process itself is carried out by a simple mechanical device, and out of 112 numbers it leaves only three

$$10, 32, 62$$

to be tried. On trial it is found

$$50,321 - 4 \cdot 10^2 = 49,921$$

$$50,321 - 4 \cdot 32^2 = 46,225$$

$$50,321 - 4 \cdot 62^2 = 34,945,$$

and only the middle number is a square. Hence

$$50,321 = 215^2 + 64^2$$

is the sum of two relatively prime squares in one way only; consequently 50,321 is a prime number.

Example 2. Is 34,579 a prime or not? This number being $\equiv 7 \pmod{12}$, we can use the form

$$3x^2 + y^2.$$

In the equation

$$3x^2 + y^2 = 34,579$$

x is less than

$$\sqrt{\frac{34,579}{3}} = 107+,$$

and only the following values must be tried:

$$x = 1, 2, 3, \dots, 107.$$

In our case $f = 3$, $g = 1$; the excludent 9 cannot be used, as it is not relatively prime to 3. For the other excludents we find

			To be excluded
$E = 5$;	$-fgN5$;	$\frac{m}{f} \equiv 3 \pmod{5}$	<u>2, 3</u>
$E = 7$;	$-fgR7$;	$\frac{m}{f} \equiv 2 \pmod{7}$	<u>0, 1, 6</u>
$E = 8$;	$-fg \equiv 5$;	$\frac{m}{f} \equiv 1 \pmod{8}$	<u>0, 2, 4, 6</u>
$E = 11$;	$-fgN11$;	$\frac{m}{f} \equiv 2 \pmod{11}$	<u>0, 4, 5, 6, 7</u>
$E = 13$;	$-fgR13$;	$\frac{m}{f} \equiv 4 \pmod{13}$	<u>3, 5, 6, 7, 8, 10.</u>

After the exclusions only the following numbers remain:

5, 25, 65, 79, 89,

and on trial we find www.dbraulibrary.org.in

$$34,579 = 148^2 + 3 \cdot 65^2 = 104^2 + 3 \cdot 89^2$$

Hence 34,579 is a composite number, and its factors can be found as shown in Sec. 7. The g.c.d. of

$$148 \cdot 89 - 104 \cdot 65 = 6,412$$

and 34,579 being 229, we have

$$34,579 = 229 \cdot 151,$$

where both factors, 151 and 229, are primes.

Example 3. Is 100,033 a prime or not? To test this number we shall use the form

$$x^2 - 2y^2.$$

Accordingly, we seek all solutions of the equation

$$x^2 - 2y^2 = 100,033$$

in positive integers, confining x to the range

$$\sqrt{100,033} < x < \sqrt{200,066}.$$

As

$$\sqrt{100,033} = 316 +, \quad \sqrt{200,066} = 447 +,$$

only 131 values

$$x = 317, 318, \dots, 447$$

have to be submitted to trials. For the excludents 5, 7, 8, 9, 11, 13 we find:

			To be excluded
$E = 5;$	$-fgN5;$	$\frac{m}{f} \equiv 3 \pmod{5};$	<u>2, 3</u>
$E = 7;$	$-fgN7;$	$\frac{m}{f} \equiv 3 \pmod{7};$	<u>1, 3, 4, 6</u>
$E = 8;$			<u>0, 2, 4, 6</u>
$E = 9;$	$-fgN9;$	$\frac{m}{f} \equiv 7 \pmod{9};$	<u>1, 2, 7, 8</u>
$E = 11;$	$-fgN11;$	$\frac{m}{f} \equiv 10 \pmod{11};$	<u>0, 2, 5, 6, 9</u>
$E = 13;$	$-fgN13;$	$\frac{m}{f} \equiv 11 \pmod{13};$	<u>1, 5, 6, 8, 12.</u>

After the exclusions only

$$329, 355, 399$$

remain to be tried. We find

$$355^2 - 100,033 = 2 \cdot 114^2,$$

$$399^2 - 100,033 = 2 \cdot 172^2,$$

or

$$100,033 = 355^2 - 2 \cdot 114^2 = 399^2 - 2 \cdot 172^2.$$

Since the g.c.d. of

$$355 \cdot 172 - 399 \cdot 114 = 15,574$$

and 100,033 is 599, 100,033 is a composite number divisible by 599; and in fact

$$100,033 = 167 \cdot 599.$$

Exercises and Problems

1. Every prime of the form $p = 24k + 1$ or $p = 24k + 19$ can be represented in the form

$$p = x^2 - 6y^2,$$

and the representation is unique if x, y are positive and $y < \sqrt{\frac{1}{3}p}$.

Every prime $p = 24k + 5$ or $p = 24k + 23$ can be represented in the form

$$p = 6x^2 - y^2,$$

and the representation is unique if x, y are positive and $x < \sqrt{\frac{1}{6}p}$.

2. Every prime $p = 28k + 1, p = 28k + 9, p = 28k + 25$ has unique representation in the form

$$p = x^2 - 7y^2$$

with positive x, y and $y < \sqrt{\frac{1}{2}p}$.

Every prime $p = 28k + 3, p = 28k + 19, p = 28k + 27$ has unique representation in the form

$$p = 7x^2 - y^2$$

with positive x, y and $x < \sqrt{\frac{3}{14}p}$.

3. Every prime of the form $p = 40k + 1, 40k + 9, 40k + 31, 40k + 39$ has unique representation in the form

$$p = x^2 - 10y^2$$

with positive x, y and $y < \sqrt{\frac{3}{16}p}$.

4. Every prime of the form $p = 60k + 1, 60k + 49$ has unique representation in the form

$$p = x^2 - 15y^2$$

with positive x, y and $y < \sqrt{\frac{1}{10}p}$.

Every prime of the form $p = 60k + 11, 60k + 59$ has unique representation in the form

$$p = 15x^2 - y^2$$

with positive x, y and $x < \sqrt{\frac{1}{6}p}$.

5. Prove that the number of all solutions of the equation

$$x^2 - 2y^2 = m$$

with x, y subject to the condition

$$-\frac{1}{2}x < y \leq \frac{1}{2}x$$

is

$$\sum(-1)^{\frac{d^2-1}{8}},$$

the sum extending over all odd divisors of m .

6. Test which of the numbers (a) 48,779; (b) 198,889; (c) 262,657; (d) 167,669; (e) 479,819 are prime. *Ans.* (a) Prime; (b) Composite, divisible by 59; (c) Prime; (d) Composite, divisible by 107; (e) Composite, divisible by 257.

9. **Another Application of the Fundamental Lemma.** Let m be an odd number, relatively prime to a , of which a is a quadratic residue. Then a will be a quadratic residue of any power m^i for $i = 1, 2, 3, \dots$, and by the Fundamental Lemma we shall have

$$\lambda m^i = x^2 - ay^2 \quad (A)$$

with

$$x - Niy \equiv 0 \pmod{m^i}$$

for any chosen root N_i of the congruence

$$N_i^2 \equiv a \pmod{m^i}.$$

Moreover,

$$|\lambda| \leq \sqrt{\frac{4}{3}|a|}.$$

and the g.c.d. of x and y divides m^i and λ . Taking for N_1 an arbitrary root of the congruence

$$N_1^2 \equiv a \pmod{m}$$

and choosing N_2, N_3, N_4, \dots for $i = 2, 3, 4, \dots$ so that $N_2 \equiv N_1 \pmod{m}, N_3 \equiv N_2 \pmod{m^2}, N_4 \equiv N_3 \pmod{m^3}, \dots$, we get as many relations of the type (A) as we like. Let

$$g = [\sqrt{\frac{4}{3}|a|}];$$

then, since λ cannot = 0, the number of possible values of λ will be $2g$ and none of them will exceed g numerically. Take $i = 1, 2, 3, \dots, 2g^4$; then among the $2g^4$ relations (A) there will be at least g^3 relations with the same multiplier λ , and among these there will be at least two:

$$\begin{aligned} \lambda m^k &= x^2 - ay^2 \\ \lambda m^{k'} &= x'^2 - ay'^2, \end{aligned} \quad (B)$$

for which

$$x' \equiv x, \quad y' \equiv y \pmod{\lambda}$$

and

$$xy' - x'y \equiv 0 \pmod{\lambda}.$$

On multiplying (B), member by member, we have

$$\lambda^2 m^{k'+k} = (xx' - ayy')^2 - a(xy' - x'y)^2,$$

whence it follows that

$$xx' - ayy' \equiv 0 \pmod{\lambda},$$

so that the quotients

$$\frac{xx' - ayy'}{\lambda} \quad \frac{xy' - x'y}{\lambda}$$

are integers. Let

$$\frac{xx' - ayy'}{\lambda} = \delta t, \quad \frac{xy' - x'y}{\lambda} = \delta u$$

where t and u are relatively prime; then

$$m^{k'+k} = \delta^2(t^2 - au^2),$$

and we are going to show that

$$\delta = m^k$$

if $k' > k$, as we can assume.

Denote by d and d' the g.c.d. of x, y and x', y' , respectively, and notice that λ is divisible by both d and d' . The congruences

$$x' \equiv x \pmod{d}, \quad y' \equiv y \pmod{d}$$

show that x' and y' are divisible by d ; that is, d' is divisible by d . Similarly the congruences

$$x' \equiv x \pmod{d'}, \quad y' \equiv y \pmod{d'}$$

show that d is divisible by d' . In consequence of this, $d' = d$.
From

$$xx' - ayy' = \lambda\delta t, \quad xy' - x'y = \lambda\delta u,$$

it follows that

$$\begin{aligned}(x^2 - ay^2)x' &= \lambda\delta(tx + auy), \\ (x^2 - ay^2)y' &= \lambda\delta(ty + ux).\end{aligned}$$

Now

$$\lambda m^k = x^2 - ay^2$$

and x, y are divisible by d ; hence

$$m^k x' \equiv 0, \quad m^k y' \equiv 0 \pmod{\delta d}$$

and also

$$m^k(x'\xi + y'\eta) \equiv 0 \pmod{\delta d}$$

for arbitrary integers ξ, η . Since the g.c.d. of x', y' is d , the integers ξ, η can be chosen so that

$$x'\xi + y'\eta = d,$$

and then

$$m^k \equiv 0 \pmod{\delta};$$

that is, m^k is divisible by δ . We shall show now that δ is divisible by m^k , which then would lead to the conclusion that $\delta = m^k$.

Let

$$x = dX, \quad y = dY; \quad x' = dX', \quad y' = dY';$$

then

$$X^2 - aY^2 = \frac{m^k \lambda}{d^2}, \quad X'^2 - aY'^2 = \frac{m^k \lambda}{d^2}.$$

Since X, Y as well as X', Y' are relatively prime, roots Γ and Γ' of the congruences

$$\Gamma^2 \equiv a \pmod{\frac{\lambda m^k}{d^2}}, \quad \Gamma'^2 \equiv a \pmod{\frac{\lambda m^k}{d^2}}$$

can be chosen so that

$$X \equiv \Gamma Y \left(\text{mod } \frac{\lambda m^k}{d^2} \right), \quad X' \equiv \Gamma' Y' \left(\text{mod } \frac{\lambda m^{k'}}{d^2} \right). \quad (C)$$

On the other hand,

$$x \equiv N_k y \pmod{m^k}, \quad x' \equiv N_{k'} y' \pmod{m^{k'}}$$

or

$$X \equiv N_k Y \left(\text{mod } \frac{m^k}{d} \right), \quad X' \equiv N_{k'} Y' \left(\text{mod } \frac{m^{k'}}{d} \right).$$

On comparing with the congruences in (C) and remembering that Y is prime to m^k/d and Y' prime to $m^{k'}/d$, we conclude

$$\Gamma \equiv N_k \left(\text{mod } \frac{m^k}{d} \right), \quad \Gamma' \equiv N_{k'} \left(\text{mod } \frac{m^{k'}}{d} \right).$$

But for $k' > k$, by the manner in which N_1, N_2, N_3, \dots are chosen,

$$N_{k'} \equiv N_k \pmod{m^k},$$

and so

$$\Gamma' \equiv \Gamma \left(\text{mod } \frac{m^k}{d} \right). \quad (D)$$

From (C) it follows again that

$$(\Gamma' - \Gamma)Y \equiv 0 \left(\text{mod } \frac{\lambda}{d} \right)$$

because

$$X' \equiv X, \quad Y' \equiv Y \left(\text{mod } \frac{\lambda}{d} \right);$$

but Y and λ/d are relatively prime, and consequently

$$\Gamma' \equiv \Gamma \left(\text{mod } \frac{\lambda}{d} \right). \quad (E)$$

Let Δ be the g.c.d. of

$$\frac{m^k}{d} \quad \text{and} \quad \frac{\lambda}{d},$$

so that

$$\frac{m^k}{d} = \Delta\mu, \quad \frac{\lambda}{d} = \Delta\nu.$$

Then from the congruences (D) and (E) we conclude

$$\Gamma' = \Gamma + \Delta\mu\nu\rho,$$

with ρ an integer, and on substituting this expression into the congruence

$$\Gamma'^2 \equiv a \pmod{\Delta^2\mu\nu},$$

we find

$$2\Gamma\rho \equiv 0 \pmod{\Delta}.$$

But m and a , and a fortiori Γ and Δ , are relatively prime numbers; moreover, Δ is odd. Consequently

$$\rho \equiv 0 \pmod{\Delta}$$

and

$$\Gamma' \equiv \Gamma \pmod{\frac{\lambda m^k}{d^2}},$$

and again, because of (C),

$$X \equiv \Gamma Y, \quad X' \equiv \Gamma Y' \pmod{\frac{\lambda m^k}{d^2}},$$

whence

$$XY' - X'Y \equiv 0, \quad XX' - aYY' \equiv 0 \pmod{\frac{\lambda m^k}{d^2}}$$

and

$$\begin{aligned} xy' - x'y &= \delta\lambda u \equiv 0 \pmod{\lambda m^k}, \\ xx' - ayy' &= \delta\lambda t \equiv 0 \pmod{\lambda m^k} \end{aligned}$$

or

$$\delta u \equiv 0, \quad \delta t \equiv 0 \pmod{m^k}.$$

Since t, u are relatively prime numbers, this implies

$$\delta \equiv 0 \pmod{m^k};$$

that is, δ is divisible by m^k . Having thus proved that $\delta = m^k$, from the equation

$$m^{k'+k} = \delta^2(t^2 - au^2)$$

we conclude

$$m^{k'-k} = t^2 - au^2.$$

Thus if a is a quadratic residue of an odd number m , relatively prime to a , then there exists a positive power of m , say m^h , representable in the form

$$m^h = t^2 - au^2$$

with relatively prime integers t and u . This is an important theorem ordinarily derived from the difficult theory of the composition of quadratic forms.

In addition we can prove this: If $a \equiv \pm 1 \pmod{4}$, p prime and m^h is the lowest power of m representable in the form

$$m^h = t^2 - au^2;$$

then the exponent h of this power is odd.

We shall prove that the supposition $h = 2k$ is impossible. In fact, for $h = 2k$ we have

$$(m^k + t)(m^k - t) = -au^2.$$

If t is even, the factors in the left-hand side are relatively prime, and then with a proper choice of sign we can set

$$m^k \mp t = \epsilon\sigma^2, \quad m^k \pm t = -\epsilon a\tau^2, \quad \epsilon = \pm 1;$$

whence

$$2m^k = \epsilon(\sigma^2 - a\tau^2) \equiv 0 \pmod{4},$$

which is impossible. If t is odd, then

$$\frac{m^k + t}{2}, \quad \frac{m^k - t}{2}$$

are relatively prime, and we can set

$$\frac{m^k \mp t}{2} = \epsilon \sigma^2, \quad \frac{m^k \pm t}{2} = -\epsilon a \tau^2; \quad \epsilon = \pm 1,$$

whence

$$m^k = \epsilon(\sigma^2 - a\tau^2).$$

Suppose at first $\epsilon = 1$; in this case a smaller power of m than m^k would be representable in the form $t^2 - au^2$ with relatively prime t and u , which is impossible by hypothesis. The case $\epsilon = -1$ can present itself only if a is a positive prime $p \equiv 1 \pmod{4}$. But then, as we shall see in the next section, integers f and g exist satisfying the equation

$$f^2 - ag^2 = -1.$$

But from this equation and

$$\sigma^2 - a\tau^2 = \frac{m^k}{\epsilon},$$

it follows again

$$m^k = (f\sigma - ag\tau)^2 - a(f\tau - g\sigma)^2,$$

which is impossible.

10. Kummer's Proof of the Reciprocity Law. Let A be a positive number but not a square, and let T, U be the smallest positive integers satisfying the equation

$$T^2 - AU^2 = 1.$$

If $A \equiv 1 \pmod{4}$, then U is necessarily even; for if U is odd,

$$T^2 = AU^2 + 1 \equiv 2 \pmod{4},$$

which is impossible. If U is even, T is odd, and the equation can be replaced by

$$\frac{T+1}{2} \cdot \frac{T-1}{2} = A \left(\frac{U}{2} \right)^2.$$

The factors in the left-hand side are relatively prime; consequently if α is the g.c.d. of

$$\frac{T+1}{2} \quad \text{and} \quad A$$

and

$$A = \alpha\beta, \quad \frac{T+1}{2} = m\alpha,$$

then $(T-1)/2$ must be divisible by β , and we can set

$$\frac{T-1}{2} = n\beta.$$

After substitution and cancellation of $\alpha\beta$ on both sides, we get

$$mn = \left(\frac{U}{2}\right)^2$$

and, since m and n are positive relatively prime numbers,

$$m = f^2, \quad n = g^2, \quad U = 2fg,$$

so that

$$\frac{T+1}{2} = \alpha g^2, \quad \frac{T-1}{2} = \beta f^2,$$

and by substitution

$$\alpha g^2 - \beta f^2 = 1.$$

Let A at first be a prime $p \equiv 1 \pmod{4}$. There are only two possibilities in this case: $\alpha = 1, \beta = p$; and $\alpha = p, \beta = 1$. In the first case

$$g^2 - pf^2 = 1,$$

but this is impossible because $f < U$ and T, U are the smallest positive integers satisfying the equation

$$t^2 - pu^2 = 1,$$

so that necessarily $\alpha = p, \beta = 1$, or

$$f^2 - pg^2 = -1.$$

In other words, the equation

$$x^2 - py^2 = -1$$

is solvable in integers if p is a prime of the form $4k + 1$. We made use of this fact at the end of the preceding section.

Now let $A = pp'$ where p and p' are primes both $\equiv 3 \pmod{4}$. In this case we have four possibilities:

$$\begin{aligned} \alpha &= 1, & \beta &= pp' \\ \alpha &= pp', & \beta &= 1 \\ \alpha &= p, & \beta &= p' \\ \alpha &= p', & \beta &= p. \end{aligned}$$

The first is impossible because in this case

$$g^2 - pp'f^2 = 1$$

and $f < U$, whereas T, U are the smallest integers satisfying the equation

$$t^2 - pp'u^2 = 1.$$

For the second possibility

$$pp'g^2 - f^2 = 1,$$

and this is impossible because -1 is a quadratic nonresidue of primes $\equiv 3 \pmod{4}$. So now there are only two possibilities:

$$pg^2 - p'f^2 = 1 \quad \text{and} \quad p'g^2 - pf^2 = 1.$$

The first equation requires pRp' ; similarly the second requires $-pRp'$ or pNp' . Since these are mutually exclusive requirements, we conclude that in case pRp' two integers f, g exist satisfying the equation

$$pg^2 - p'f^2 = 1.$$

Kummer's proof of the reciprocity law depends partly on this result and partly on the last theorem in Sec. 9. Let p

and q be two different primes. The positive or negative number

$$(-1)^{\frac{q-1}{2}} q$$

is always $\equiv 1 \pmod{4}$. Suppose now that

$$(-1)^{\frac{q-1}{2}} qRp.$$

By the theorem referred to, the exponent of the smallest power of p representable in the form

$$t^2 - (-1)^{\frac{q-1}{2}} qu^2$$

is odd, so that

$$t^2 - (-1)^{\frac{q-1}{2}} qu^2 = p^{2h+1}.$$

This equation implies the congruence

$$t^2 \equiv p^{2h}p \pmod{q};$$

that is, $p^{2h}p$ and likewise p are quadratic residues of q .

Thus if $(-1)^{\frac{q-1}{2}} qRp$, then pRq .

It remains to prove the second part of the reciprocity law: if $(-1)^{\frac{q-1}{2}} qNp$, then pNq . In this proof we shall distinguish the following four cases:

- (a) $q \equiv p \equiv 1 \pmod{4}$;
- (b) $q \equiv 1, \quad p \equiv 3 \pmod{4}$;
- (c) $q \equiv 3, \quad p \equiv 1 \pmod{4}$;
- (d) $q \equiv p \equiv 3 \pmod{4}$.

In (a) the hypothesis is qNp , and we must show that then pRq is impossible. Since $p \equiv 1 \pmod{4}$

$$p = (-1)^{\frac{p-1}{2}} p,$$

and so pRq is equivalent to

$$(-1)^{\frac{p-1}{2}} pRq.$$

But then qRp , which is contrary to hypothesis.

In (b) the hypothesis is qNp , and we must show that then pRq is impossible. Since $q \equiv 1 \pmod{4}$, the statements pRq and $(-1)^{\frac{p-1}{2}} pRq$ are equivalent. In case

$$(-1)^{\frac{p-1}{2}} pRq,$$

we have qRp , contrary to hypothesis.

In (c) the hypothesis is $-qNp$; since $p \equiv 1 \pmod{4}$, this implies qNp , and we must show that pRq is impossible. Again, pRq and $(-1)^{\frac{p-1}{2}} pRq$ are equivalent statements; but if

$$(-1)^{\frac{p-1}{2}} pRq,$$

then qRp , which is contrary to our supposition.

Case (d) requires a different treatment. Since $p \equiv q \equiv 3 \pmod{4}$ by hypothesis $-qNp$ or qRp ; then two integers f, g exist such that

$$qg^2 - pf^2 = 1,$$

and this implies

$$pf^2 \equiv -1 \pmod{q},$$

whence we conclude that pNq . Thus both parts of the reciprocity law are proved.

11. The Four Squares Theorem. In the eighteenth annotation to Diophantus, Fermat says,

"We found a beautiful and most general proposition; namely that every integer is either a triangular number or composed of two or three triangular numbers; either a square or composed of two, three or four squares; either pentagonal or composed of two, three, four or five pentago-

nal numbers; and in the same way a general and marvelous proposition can be announced for hexagonal, heptagonal and any sort of polygonal numbers. But it is not possible to give the proof of it, derived from many and most recondite mysteries of numbers, here."

Fermat never revealed anything about the way he proved this remarkable property of numbers. The second part of the theorem, namely that every integer is a sum of not more than four squares, was proved for the first time by Lagrange in 1770, and his proof was later considerably simplified by Euler. The first part is equivalent to the statement that numbers of the form $8n + 3$ are the sums of three (necessarily odd) squares; the proof of this and the general solution of the problem concerning the representation of integers by the sums of three squares were given by Gauss. Later Cauchy showed that other parts of the Fermat theorem can be derived in a comparatively elementary but rather long way from the first.

www.dbraulibrary.org.in

We shall end this chapter by proving Fermat's statement for squares, reserving the case of triangular numbers for the last chapter of the book. That every integer is the sum of four squares (some of which may be 0) has been proved in a great many ways. The proof by L. E. Dickson, which we shall adopt here, is perhaps the simplest. But before we proceed to the proof, an important lemma due to Lagrange must be established.

If p is an odd prime and A, B are two integers nondivisible by p , then the congruence

$$x^2 + Ay^2 + B \equiv 0 \pmod{p^n}$$

can be satisfied by integers x and y . Suppose first $n = 1$, and consider the numbers

$$-Ay^2 - B$$

for $y = 0, 1, 2, \dots, (p-1)/2$. These $(p+1)/2$ numbers are incongruent mod p and, since the number of quadratic

nonresidues mod p is $(p - 1)/2$, there must be among them at least one quadratic residue. Let it be

$$-Ay_0^2 - B,$$

and x_0 some solution of the congruence

$$x_0^2 = -Ay_0^2 - B \pmod{p};$$

then

$$x_0^2 + Ay_0^2 + B \equiv 0 \pmod{p}.$$

Notice that x_0 and y_0 cannot both be divisible by p , since B is supposed undivisible by p . To satisfy the congruence

$$x^2 + Ay^2 + B \equiv 0 \pmod{p^2},$$

we take

$$x = x_0 + pt, \quad y = y_0 + pu$$

and obtain for t and u the congruence

$$2x_0t + 2Ay_0u + \frac{x_0^2 + Ay_0^2 + B}{p} \equiv 0 \pmod{p}.$$

At least one of the numbers $2x_0$ and $2Ay_0$ is not divisible by p , for example, $2x_0$. Then u can be taken arbitrarily, and t will be determined by the preceding congruence, so that

$$x = x_0 + pt, \quad y = y_0 + pu$$

will satisfy the congruence

$$x^2 + Ay^2 + B \equiv 0 \pmod{p^2}.$$

In the same way we can show that the congruence

$$x^2 + Ay^2 + B \equiv 0 \pmod{p^n}$$

can be satisfied by integers x, y for $n = 3, 4, 5, \dots$. From this fact we conclude in the usual way that for any odd integer m prime to AB the congruence

$$x^2 + Ay^2 + B \equiv 0 \pmod{m}$$

is possible.

Let $A = B = 1$ and m any odd integer; also let α, β be any two numbers such that

$$\alpha^2 + \beta^2 + 1 \equiv 0 \pmod{m}$$

or

$$\alpha^2 + \beta^2 + 1 = mm'.$$

Suppose that the equation

$$m' = x'^2 + y'^2 + z'^2 + t'^2 \quad (A)$$

can be satisfied by four integers x', y', z', t' so that

$$x' \equiv \alpha z' + \beta t', \quad y' \equiv \beta z' - \alpha t' \pmod{m'}. \quad (B)$$

Then

$$z = \frac{x' - \alpha z' - \beta t'}{m'}, \quad t = \frac{y' - \beta z' + \alpha t'}{m'}$$

$$x = mz' + \alpha z + \beta t, \quad y = mt' + \beta z - \alpha t$$

www.dbraulibrary.org.in

will satisfy the equation

$$m = x^2 + y^2 + z^2 + t^2, \quad (C)$$

and the two congruences

$$x \equiv \alpha z + \beta t, \quad y \equiv \beta z - \alpha t \pmod{m}. \quad (D)$$

By virtue of the congruences (B) we can set

$$x' = m'u + \alpha z' + \beta t', \quad y' = m'v + \beta z' - \alpha t',$$

and on substituting in (A) and dividing through by m' we get

$$m'(u^2 + v^2) + 2u(\alpha z' + \beta t') + 2v(\beta z' - \alpha t') + \frac{\alpha^2 + \beta^2 + 1}{m'}(z'^2 + t'^2) = 1$$

or

$$m'(u^2 + v^2) + 2z'(\alpha u + \beta v) + 2t'(\beta u - \alpha v) + m(z'^2 + t'^2) = 1.$$

Multiply both members by m , complete the square, and replace mm' by $1 + \alpha^2 + \beta^2$; then

$$m = (mz' + \alpha u + \beta v)^2 + (mt' + \beta u - \alpha v)^2 + u^2 + v^2.$$

That is, (C) is satisfied by

$$z = u, \quad t = v, \quad x = mz' + \alpha u + \beta v, \\ y = mt' + \beta u - \alpha v$$

or

$$z = \frac{x' - \alpha z' - \beta t'}{m'}, \quad t = \frac{y' - \beta z' + \alpha t'}{m'}, \\ x = mz' + \alpha z + \beta t, \quad y = mt' + \beta z - \alpha t,$$

and the congruences (D) also hold.

After this preliminary observation we proceed with the proof. Take an odd integer m and find two numbers α, β satisfying the congruence

$$\alpha^2 + \beta^2 + 1 \equiv 0 \pmod{m}$$

so that

$$\alpha^2 + \beta^2 + 1 = mm_1.$$

We can suppose at the outset that

$$|\alpha| \leq \frac{1}{2}m, \quad |\beta| \leq \frac{1}{2}m.$$

Then

$$m_1 \leq \frac{1}{2}m + \frac{1}{m}$$

and $m_1 < m$ as long as $m > 1$. If $m_1 > 1$, determine integers δ_1 and ϵ_1 so that

$$\alpha_1 = \alpha - \delta_1 m_1, \quad \beta_1 = \beta - \epsilon_1 m_1$$

are both numerically $\leq \frac{1}{2}m_1$. Since $\alpha_1 \equiv \alpha, \beta_1 \equiv \beta \pmod{m_1}$, we shall have

$$\alpha_1^2 + \beta_1^2 + 1 \equiv 0 \pmod{m_1}$$

or

$$\alpha_1^2 + \beta_1^2 + 1 = m_1 m_2,$$

and $m_2 < m_1$. If $m_2 > 1$, determine integers δ_2 and ϵ_2 so that

$$\alpha_2 = \alpha_1 - \delta_2 m_2, \quad \beta_2 = \beta_1 - \epsilon_2 m_2$$

are numerically both $\leq \frac{1}{2} m_2$. Then

$$\alpha_2^2 + \beta_2^2 + 1 = m_2 m_3$$

and $m_3 < m_2$.

Proceeding in the same way, we have a decreasing series of integers

$$m > m_1 > m_2 > \cdots > m_n > m_{n+1}$$

which must stop, and this can happen only if we come to a term = 1. Let therefore $m_{n+1} = 1$, while the preceding terms are all greater than 1. Since

www.dbraulibrary.org.in

$$\alpha_n^2 + \beta_n^2 + 1 = m_n,$$

the equation

$$m_n = x_n^2 + y_n^2 + z_n^2 + t_n^2$$

is satisfied by

$$x_n = \alpha_n, \quad y_n = \beta_n, \quad z_n = 1, \quad t_n = 0$$

and so that

$$x_n \equiv \alpha_n z_n + \beta_n t_n, \quad y_n \equiv \beta_n z_n - \alpha_n t_n \pmod{m_n}$$

or

$$x_n \equiv \alpha_{n-1} z_n + \beta_{n-1} t_n, \quad y_n \equiv \beta_{n-1} z_n - \alpha_{n-1} t_n \pmod{m_n},$$

since

$$\alpha_n \equiv \alpha_{n-1}, \quad \beta_n \equiv \beta_{n-1} \pmod{m_n}.$$

But then, by the remark made above, the equation

$$m_{n-1} = x_{n-1}^2 + y_{n-1}^2 + z_{n-1}^2 + t_{n-1}^2$$

is satisfied by

$$z_{n-1} = \frac{x_n - \alpha_{n-1}z_n - \beta_{n-1}t_n}{m_n},$$

$$t_{n-1} = \frac{y_n - \beta_{n-1}z_n + \alpha_{n-1}t_n}{m_n},$$

$$x_{n-1} = m_{n-1}z_n + \alpha_{n-1}z_{n-1} + \beta_{n-1}t_{n-1},$$

$$y_{n-1} = m_{n-1}t_n + \beta_{n-1}z_{n-1} - \alpha_{n-1}t_{n-1},$$

so that

$$x_{n-1} \equiv \alpha_{n-1}z_{n-1} + \beta_{n-1}t_{n-1} \pmod{m_{n-1}}$$

$$y_{n-1} \equiv \beta_{n-1}z_{n-1} - \alpha_{n-1}t_{n-1} \pmod{m_{n-1}}$$

or

$$x_{n-1} \equiv \alpha_{n-2}z_{n-1} + \beta_{n-2}t_{n-1} \pmod{m_{n-1}},$$

$$y_{n-1} \equiv \beta_{n-2}z_{n-1} - \alpha_{n-2}t_{n-1} \pmod{m_{n-1}}.$$

But then again

$$z_{n-2} = \frac{x_{n-1} - \alpha_{n-2}z_{n-1} - \beta_{n-2}t_{n-1}}{m_{n-1}},$$

$$t_{n-2} = \frac{y_{n-1} - \beta_{n-2}z_{n-1} + \alpha_{n-2}t_{n-1}}{m_{n-1}}$$

$$x_{n-2} = m_{n-2}z_{n-1} + \alpha_{n-2}z_{n-2} + \beta_{n-2}t_{n-2},$$

$$y_{n-2} = m_{n-2}t_{n-1} + \beta_{n-2}z_{n-2} - \alpha_{n-2}t_{n-2}$$

will satisfy the equation

$$m_{n-2} = x_{n-2}^2 + y_{n-2}^2 + z_{n-2}^2 + t_{n-2}^2,$$

and the congruences

$$x_{n-2} \equiv \alpha_{n-3}z_{n-2} + \beta_{n-3}t_{n-2} \pmod{m_{n-2}},$$

$$y_{n-2} \equiv \beta_{n-3}z_{n-2} - \alpha_{n-3}t_{n-2}$$

In the same way we proceed further until we find four integers x, y, z, t which satisfy the equation

$$m = x^2 + y^2 + z^2 + t^2$$

and the congruences

$$x \equiv \alpha z + \beta t, \quad y \equiv \beta z - \alpha t \pmod{m}.$$

The algorithm whereby x, y, z, t are finally found consists in the use of the recurrence relations

$$z_{i-1} = \frac{x_i - \alpha_{i-1}z_i - \beta_{i-1}t_i}{m_i}, \quad t_{i-1} = \frac{y_i - \beta_{i-1}z_i + \alpha_{i-1}t_i}{m_i}$$

$$x_{i-1} = m_{i-1}z_i + \alpha_{i-1}z_{i-1} + \beta_{i-1}t_{i-1},$$

$$y_{i-1} = m_{i-1}t_i + \beta_{i-1}z_{i-1} - \alpha_{i-1}t_{i-1}$$

for $i = n, n-1, \dots, 2, 1$, starting with

$$x_n = \alpha_n, \quad y_n = \beta_n, \quad z_n = 1, \quad t_n = 0.$$

It is thus proved that every odd integer is a sum of four squares. For even integers the proof is based on the simple remark that an equation

$$m = x^2 + y^2 + z^2 + t^2$$

implies

$$2m = (x+y)^2 + (x-y)^2 + (z+t)^2 + (z-t)^2.$$

Example. Let us apply this method to $m = 351 = 3^3 \cdot 13$. It is found easily that

$$\alpha \equiv 1, \quad \beta \equiv 5 \pmod{27}$$

satisfy the congruence

$$\alpha^2 + \beta^2 + 1 \equiv 0 \pmod{27}.$$

Also

$$\alpha \equiv 5, \quad \beta \equiv 0 \pmod{13}$$

satisfy the congruence

$$\alpha^2 + \beta^2 + 1 \equiv 0 \pmod{13}.$$

Hence the numbers α, β , satisfying simultaneously the congruences

$$\alpha \equiv 1 \pmod{27}, \quad \alpha \equiv 5 \pmod{13},$$

$$\beta \equiv 5 \pmod{27}, \quad \beta \equiv 0 \pmod{13},$$

will satisfy the congruence

$$\alpha^2 + \beta^2 + 1 \equiv 0 \pmod{351}.$$

We find

$$\alpha = 109, \quad \beta = -130$$

and

$$109^2 + 130^2 + 1 = 351 \cdot 82; \quad m_i = 82.$$

Again

$$\alpha_1 = 109 - 82 \cdot 1 = 27, \quad \beta_1 = -130 + 82 \cdot 2 = 34$$

$$27^2 + 34^2 + 1 = 82 \cdot 23; \quad m_2 = 23$$

and

$$\alpha_2 = 27 - 23 \cdot 1 = 4, \quad \beta_2 = 34 - 23 \cdot 1 = 11$$

$$4^2 + 11^2 + 1 = 23 \cdot 6; \quad m_3 = 6.$$

Furthermore

$$\alpha_3 = 4 - 6 \cdot 1 = -2, \quad \beta_3 = 11 - 6 \cdot 2 = -1$$

$$2^2 + 1^2 + 1 = 6 \cdot 1, \quad m_4 = 1.$$

Since $m_4 = 1$, the first series of operations ends here.

The second series begins by taking

$$x_3 = -2, \quad y_3 = -1, \quad z_3 = 1, \quad t_3 = 0$$

and determining

$$x_2 = \frac{-2 - 4 \cdot 1 - 11 \cdot 0}{6} = -1,$$

$$y_2 = \frac{-1 - 11 \cdot 1 + 4 \cdot 0}{6} = -2$$

$$z_2 = 23 \cdot 1 - 4 \cdot 1 - 11 \cdot 2 = 3$$

$$t_2 = 23 \cdot 0 - 11 \cdot 1 + 4 \cdot 2 = -3,$$

after which we find

$$x_1 = \frac{-3 + 27 \cdot 1 + 34 \cdot 2}{23} = 4,$$

$$t_1 = \frac{-3 + 34 \cdot 1 - 27 \cdot 2}{23} = -1$$

$$x_0 = -82 \cdot 1 + 27 \cdot 4 - 34 \cdot 1 = -8,$$

$$y_0 = -82 \cdot 2 + 34 \cdot 4 + 27 \cdot 1 = -1,$$

and finally

$$z = \frac{-8 - 109 \cdot 4 - 130 \cdot 1}{82} = -7,$$

$$t = \frac{-1 + 130 \cdot 4 - 109 \cdot 1}{82} = 5.$$

$$x = 351 \cdot 4 - 109 \cdot 7 - 130 \cdot 5 = -9,$$

$$y = -351 \cdot 1 + 130 \cdot 7 - 109 \cdot 5 = 14.$$

With these numbers we have

$$(-9)^2 + (14)^2 + (-7)^2 + 5^2 = 81 + 196 + 49 + 25 = 351.$$

CHAPTER XII

SOME DIOPHANTINE PROBLEMS

1. Object of This Chapter. In a general sense a Diophantine problem is any problem requiring the solution of an indeterminate equation or system of equations in integral values of the unknowns. A Diophantine problem is considered as solved if a method is available to decide whether the problem is possible or not and, in case of its possibility, to exhibit all integers satisfying the requirements set forth in the problem. The partial solution of a Diophantine problem has only a very limited interest. There are but very few Diophantine problems of a general type in which the complete solution is known. Thus, for instance, infallible methods are available for solving indeterminate equations of the second degree in two unknowns

$$ax^2 + bxy + cy^2 + dx + ey + f = 0$$

with integral coefficients. On the other hand, the general Diophantine equation of the type

$$f(x, y) = m,$$

where $f(x, y)$ is a homogeneous polynomial of degree $n \geq 3$, is known to have, except in cases of degeneracy, only a limited number of solutions, but no sure method is available to detect all of them. Again, if $f(x, y)$ is a homogeneous polynomial of the fourth degree, there are no sure methods for the solution of the equation

$$f(x, y) = z^2$$

with three unknowns x, y, z except in a few particular cases. Yet many problems set even before the rise of scientific number theory led to just such equations. One can easily understand that Diophantine problems offer an almost unlimited field for research by reason of their variety and that the successful overcoming of difficulties connected with their solution will depend on the further progress of number theory. In this chapter we shall consider a few special Diophantine problems partly because of their historical interest and partly because they offer a good application of the principles explained in the preceding chapters.

2. Equations $x^2 + ay^2 = z^n$. A complete solution of the Pythagorean equation

$$x^2 + y^2 = z^2$$

has already been given in the second chapter of this book. Here we shall consider the solution of equations of the type

$$x^2 + ay^2 = z^n \quad (A)$$

in integers x, y, z of which x and y are relatively prime. The means at our disposal do not suffice to do this for every value of a , and we shall confine ourselves to some particular values of a only.

A solution of (A) in relatively prime integers x, y belongs to some root of the congruence

$$N^2 \equiv -a \pmod{z^n}$$

so that

$$x - Ny \equiv 0 \pmod{z^n}.$$

By the Fundamental Lemma in Sec. 2, Chap. XI, two integers t, u and a multiplier λ can be found in such a manner as to have

$$t^2 + au^2 = \lambda z; \quad t - Nu \equiv 0 \pmod{z}; \quad |\lambda| \leq \sqrt{\frac{4}{3}|a|}$$

and the g.c.d. of t and u will divide λ and z .

Consider now integers P, Q , obtained by equating the rational parts and the coefficients of $\sqrt{-a}$, which is supposed to be either imaginary or an irrational number, in the equation

$$P - Q\sqrt{-a} = (t - u\sqrt{-a})^n.$$

To get P and Q we expand the right-hand side and eliminate powers of $\sqrt{-a}$ higher than the first by means of the equality $(\sqrt{-a})^2 = -a$. Suppose now that instead of $\sqrt{-a}$ we take N and eliminate powers of N higher than the first by means of the congruence

$$N^2 \equiv -a \pmod{z^n}.$$

Then it is clear that

$$(t - uN)^n$$

will be congruent to $P - QN \pmod{z^n}$, so that

$$P - QN \equiv (t - uN)^n \equiv 0 \pmod{z^n}.$$

From this congruence combined with

$$x - yN \equiv 0 \pmod{z^n}$$

it follows that

$$Px + aQy \equiv 0, \quad Py - Qx \equiv 0 \pmod{z^n},$$

and we can set

$$Px + aQy = \rho z^n, \quad Py - Qx = \sigma z^n$$

with ρ, σ certain integers. Now

$$\frac{x + y\sqrt{-a}}{P + Q\sqrt{-a}} = \frac{Px + aQy + \sqrt{-a}(Py - Qx)}{P^2 + aQ^2},$$

but

$$P^2 + aQ^2 = \lambda^n z^n,$$

and so

$$x + y\sqrt{-a} = \frac{1}{\lambda^n}(\rho + \sigma\sqrt{-a})(P + Q\sqrt{-a}),$$

whence

$$x^2 + ay^2 = \frac{(\rho^2 + a\sigma^2)(P^2 + Q^2a)}{\lambda^{2n}}$$

or

$$z^n = \frac{(\rho^2 + a\sigma^2)\lambda^n z^n}{\lambda^{2n}}$$

Consequently the integers ρ, σ satisfy the equation

$$\rho^2 + a\sigma^2 = \lambda^n.$$

Thus far the procedure has been quite general. We turn now to such values of a for which we can be sure that $\lambda = \pm 1$. Then to any solution of the equation

$$x^2 + ay^2 = z^n,$$

in which x and y are relatively prime, correspond a pair of integers t, u and a pair of integers ρ, σ connected by the equation

$$\rho^2 + a\sigma^2 = (\pm 1)^n,$$

so that

$$x + y\sqrt{-a} = (\rho + \sigma\sqrt{-a})(t + u\sqrt{-a})^n, \quad (B)$$

It is clear that t, u will be relatively prime. Conversely x, y , as defined by (B) for arbitrary relatively prime t, u constitute a solution of the equation

$$x^2 + ay^2 = z^n$$

in which

$$\pm z = t^2 + au^2.$$

But will x, y be relatively prime? This will be the case if t and au are relatively prime and of different parity. To prove this, suppose that P and Q as defined by

$$P + Q\sqrt{-a} = (t + u\sqrt{-a})^n$$

are divisible by a prime p necessarily odd. Then

$$t^2 + au^2 \equiv 0 \pmod{p}$$

and

$$t \equiv ru \pmod{p}$$

for some root of the congruence

$$r^2 \equiv -a \pmod{p}.$$

But as

$$P + Qr \equiv (t + ru)^n \pmod{p},$$

we shall have

$$t \equiv -ru \pmod{p}$$

and

$$2t \equiv 0, \quad t \equiv 0 \pmod{p},$$

and consequently p divides au^2 , which is impossible since t and au are relatively prime. To draw the final conclusions we turn now to particular cases.

3. Particular Cases. *Case 1.* $a = 1$. The congruence

$$\xi^2 \equiv -1 \pmod{z^n}$$

being impossible if z is even and $n \geq 2$, x and y in the equation

$$x^2 + y^2 = z^n$$

must be of a different parity. Also $\lambda = 1$ if z is positive, as we shall suppose, and

$$t^2 + u^2 = z,$$

which shows that t and u are two relatively prime integers of different parity. Consequently all solutions of the equation

$$x^2 + y^2 = z^n,$$

in relatively prime x and y , are obtained from

$$x + iy = \epsilon(t + iu)^n,$$

where $i = \sqrt{-1}$, $\epsilon = \pm 1$, $\pm i$ and t and u are relatively prime integers of different parity. Noticing that $-1 = i^2$, we have for $n = 2$ in particular

$$x + iy = (p + iq)^2 \quad \text{or} \quad x + iy = i(p - iq)^2,$$

so either

$$x = p^2 - q^2, \quad y = 2pq$$

or

$$x = 2pq, \quad y = p^2 - q^2$$

with relatively prime p, q of different parity. This was obtained in Chap. II by quite an elementary method.

Since $i = (-i)^3$, $-1 = (-1)^3$, the result for $n = 3$ is

$$x + iy = (p + iq)^3.$$

That is, all solutions of the equation

$$x^2 + y^2 = z^3$$

with relatively prime x, y and positive z are given by

$$x = p^3 - 3pq^2, \quad y = 3p^2q - q^3, \quad z = p^2 + q^2$$

with p, q relatively prime and of different parity.

Case 2. $a = 2$. The congruence

$$\xi^2 \equiv -2 \pmod{z^n}$$

being impossible if z is even and $\lambda = 1$, t and $2u$ must be relatively prime and of different parity. All the solutions of the equation

$$x^2 + 2y^2 = z^n$$

in relatively prime x, y and positive z are given by

$$x + y\sqrt{-2} = \pm(p + q\sqrt{-2})^n, \quad z = p^2 + 2q^2$$

with $p, 2q$ relatively prime and of different parity.

Case 3. $a = 3$. The congruence

$$\xi^2 \equiv -3 \pmod{z^n}$$

is impossible for an even z if $n \geq 3$; also it is impossible if z is divisible by 3. With an odd z we have necessarily $\lambda = 1$, and so all the solutions of the equation

$$x^2 + 3y^2 = z^n$$

in relatively prime x, y and positive odd z are given by

$$x + y\sqrt{-3} = \pm(p + q\sqrt{-3})^n, \quad z = p^2 + 3q^2,$$

with p and $3q$ relatively prime and of different parity. The double sign \pm is not necessary if n is odd.

In case $n = 2$, though x, y are relatively prime, z might be even. In this case necessarily $\lambda = 2$ and

$$x + y\sqrt{-3} = \frac{\rho + \sigma\sqrt{-3}}{4}(t + u\sqrt{-3})^2, \quad z = \frac{t^2 + 3u^2}{2},$$

while

$$\rho^2 + 3\sigma^2 = 4,$$

so that $\rho = \pm 2, \sigma = 0$, or $\rho = \pm 1, \sigma = \pm 1$. In case $\rho = \pm 2, \sigma = 0$, t and u must be odd. In case $\rho = \pm 1, \sigma = \pm 1$, we notice that

$$\frac{-1 \pm \sqrt{-3}}{2} = \left(\frac{-1 \mp \sqrt{-3}}{2} \right)^2$$

and

$$\begin{aligned} \frac{-1 \pm \sqrt{-3}}{4}(t + u\sqrt{-3})^2 &= \frac{1}{2} \left(\frac{t \mp 3u + (u \pm t)\sqrt{-3}}{2} \right)^2 \\ &= \frac{1}{2}(p + q\sqrt{-3})^2 \end{aligned}$$

if

$$p = \frac{t \mp 3u}{2}, \quad q = \frac{u \pm t}{2}.$$

At the same time

$$p^2 + 3q^2 = t^2 + 3u^2.$$

So that, finally, all solutions of the equation

$$x^2 + 3y^2 = z^2,$$

with relatively prime x , y and positive z , are represented by two sets of formulas

$$x + y\sqrt{-3} = \pm(p + q\sqrt{-3})^2, \quad z = p^2 + 3q^2$$

with p , $3q$ relatively prime and of different parity and

$$x + y\sqrt{-3} = \pm \frac{(p + q\sqrt{-3})^2}{2}, \quad z = \frac{p^2 + 3q^2}{2}$$

with relatively prime odd p and $3q$. This result can be verified by entirely elementary considerations.

Case 4. $a = -2$. The congruence

$$\xi^2 \equiv 2 \pmod{z^n}$$

is impossible for z even. With an odd z , we have $\lambda = 1$; consequently all solutions of the equation

$$x^2 - 2y^2 = z^n$$

in relatively prime x , y are given by

$$x + y\sqrt{2} = (\rho + \sigma\sqrt{2})(t + u\sqrt{2})^n,$$

where ρ , σ are solutions of the equation

$$\rho^2 - 2\sigma^2 = 1$$

and t and $2u$ are relatively prime.

Case 5. $a = -3$. Again z must be odd and prime to 3; λ can be either 1 or -1 . If n is odd, λ must be 1, but when n is even, λ can be 1 or -1 . In all cases solutions of the equation

$$x^2 - 3y^2 = z^n$$

in relatively prime x, y are given by

$$x + y\sqrt{3} = (\rho + \sigma\sqrt{3})(t + u\sqrt{3})^n,$$

where ρ, σ are solutions of the equation

$$\rho^2 - 3\sigma^2 = 1$$

and t and $3u$ are relatively prime numbers of different parity.

Case 6. $a = -5$. In this case z must be prime to 5 but may be even if $n = 2$. Considering only odd values of z , we can suppose $\lambda = 1$. Then all solutions of the equation

$$x^2 - 5y^2 = z^n$$

in relatively prime x, y of different parity are given by

$$x + y\sqrt{5} = (\rho + \sigma\sqrt{5})(t + u\sqrt{5})^n,$$

where ρ, σ are solutions of the equation

$$\rho^2 - 5\sigma^2 = 1$$

and t and $5u$ are relatively prime numbers of different parity.

In Sec. 5, Chap. XI, we have seen that

$$\rho + \sigma\sqrt{5} = \pm(9 + 4\sqrt{5})^r = \pm(2 + \sqrt{5})^{2r}$$

for $r = 0, \pm 1, \pm 2, \dots$. Since

$$(2 + \sqrt{5})^r(t + u\sqrt{5})$$

can be reduced to the form $p + q\sqrt{5}$, all the solutions of the equation

$$x^2 - 5y^2 = z^2$$

in relatively prime x, y of different parity will be given by

$$x + y\sqrt{5} = \pm(p + q\sqrt{5})^2,$$

where again p and $5q$ are relatively prime and of different

parity. This result follows also from entirely elementary considerations.

4. Some Equations of the Type $x^2 + c = y^3$. Equations of this type are very important, but so far a general and sure method for their solution is lacking. We shall consider here only a few particular cases. Let at first $c = 4$. If x is odd, then from the equation

$$x^2 + 4 = y^3$$

it follows that

$$x + 2i = (p + iq)^3,$$

with p, q relatively prime and of different parity. Equating the real and imaginary parts, we have

$$x = p^3 - 3pq^2, \quad 3p^2q - q^3 = 2,$$

and the last equation requires that $q = \pm 1$ or $q = \pm 2$. If $q = \pm 1$, we must have

$$3p^2 - 1 = \pm 2,$$

which cannot be satisfied by an even p . For $q = \pm 2$ we must have

$$3p^2 - 4 = \pm 1,$$

and here only the negative sign may hold, corresponding to which $p = \pm 1, q = -2$, so that the only solutions with an odd x are

$$x = \pm 11, \quad y = 5.$$

Suppose now that $x = 2t$ is even; then

$$t^2 + 1 = 2u^3$$

or

$$\left(\frac{t+1}{2}\right)^2 + \left(\frac{t-1}{2}\right)^2 = u^3.$$

Since

$$\frac{t+1}{2} \quad \text{and} \quad \frac{t-1}{2}$$

are relatively prime, we must have

$$\frac{t+1}{2} + \frac{t-1}{2}i = (r+sz)^3$$

with r, s relatively prime and of different parity. Hence

$$\frac{t+1}{2} = r^3 - 3rs^2, \quad \frac{t-1}{2} = 3r^2s - s^3$$

and

$$r^3 + s^3 - 3rs(r+s) = 1$$

or

$$(r+s)(r^2 - 4rs + s^2) = 1.$$

It follows that necessarily

$$r+s = \pm 1, \quad r^2 - 4rs + s^2 = \pm 1,$$

and the only solutions of this system in integers are

$$r = 1, \quad s = 0; \quad r = 0, \quad s = 1;$$

correspondingly $t = 1$ and $t = -1$, so that the only solutions with an even x are

$$x = \pm 2, \quad y = 2.$$

Next we consider the equation

$$x^2 + 2 = y^3,$$

from which it follows necessarily that

$$x + \sqrt{-2} = (p + q\sqrt{-2})^3,$$

whence

$$x = p^3 - 6pq^2$$

and

$$3p^2q - 2q^3 = 1,$$

so that

$$q = \pm 1; \quad 3p^2 - 2 = \pm 1.$$

Clearly only the positive sign can be accepted, and then

$$p = \pm 1, \quad q = 1, \quad x = \pm 5.$$

Thus

$$x = \pm 5, \quad y = 3$$

are the only solutions of the equation

$$x^2 + 2 = y^3.$$

Speaking of these particular results, Fermat writes in a letter to Digby on August 15, 1657,

"Je lui (Frenicle) avais écrit qu'il n'y a qu'un seul nombre quarré en entiers qui, joint au binaire, fasse un cube, et que le dit quarré est 25, auquel si vous ajoutez 2, il se fait 27, qui est cube. Il a peine à croire cette proposition négative et la trouve trop hardie et trop générale. Mais pour augmenter son étonnement, je dis que, si on cherche un quarré qui, ajouté à 4, fasse un cube, il n'en trouvera jamais que deux en nombres entiers, savoir 4 et 121. Car 4 ajouté à 4 fait 8 qui est cube, et 121 ajouté à 4 fait 125 qui est aussi cube. Mais, de plus, cela, toute l'infinité des nombres n'en saurait fournir un troisième qui a la même propriété."

As a third example we take the equation

$$x^2 - 2 = y^3,$$

the elementary solution of which succeeds by means of a simple device due to A. Brauer. When we substitute

$$y = z - 1$$

into the equation, it becomes

$$z^3 - 3z^2 + 3z + 1 = x^2$$

or

$$(z + 1)^3 = x^2 + 6z^2,$$

where x and z clearly are relatively prime. By the method of Sec. 2, we conclude that

$$x + z\sqrt{-6} = (r + s\sqrt{-6})^3,$$

whence

$$z = 3s(r^2 - 2s^2)$$

and

$$z + 1 = r^2 + 6s^2.$$

On substituting the expression for z , we get

$$r^2(1 - 3s) = 1 - 6s^2 - 6s^3,$$

whence

$$r^2 = \frac{1 - 6s^2 - 6s^3}{1 - 3s} = 2s^2 + \frac{8}{3}s + \frac{8}{9} - \frac{1}{9(3s - 1)}$$

$$9r^2 = 18s^2 + 24s + 8 - \frac{1}{3s - 1},$$

and so necessarily

$$3s - 1 = \pm 1.$$

But only for the negative sign do we get an integral value $s = 0$ to which $r = \pm 1$ corresponds. Hence $z = 0$, $y = -1$, and $x = \pm 1$, so that the only solutions of the equation

$$x^2 - 2 = y^3$$

are

$$x = \pm 1, \quad y = -1.$$

Equations of the type

$$x^2 + c = y^3$$

are known to have only a limited number of solutions. Delaunay devised a method which allows one to show either the impossibility of such equations or to solve them completely in a great many cases. For instance, Delaunay was able to show that the only solutions of the equation

$$x^2 - 17 = y^3$$

with positive x are

$$x = 3, \quad 4, 5, 9, 23, 282, 375, 378, 661$$

$$y = -2, -1, 2, 4, 8, 43, 52, 5, 234.$$

Whether his method will always work is still an open question, and the problem, despite its simple appearance, is a very difficult one.

5. Some Insoluble Diophantine Problems. On many occasions Fermat mentions in his correspondence insoluble Diophantine problems. Such is, for instance, the problem of finding two biquadrates (neither of which is 0) whose sum is a square, or of finding a right-angle triangle in integers whose area is a square. In this section we shall deal with these two problems in order to illustrate the method of proof by descent which Fermat asserted to be his main tool of investigation.

In the first problem it is required to show that the equation

$$x^4 + y^4 = z^2 \quad (A)$$

cannot be satisfied by integers none of which is 0. This is accomplished by showing that once we assume hypothetically the existence of positive integers x, y, z satisfying equation (A), another solution in positive integers x_1, y_1, z_1 can be found, but with $z_1 < z$. Then from this solution a new solution in positive integers x_2, y_2, z_2 is deduced with $z_2 < z_1$, and the same process can be carried out indefinitely. But this implies a contradiction, since the series of positive decreasing numbers

$$z > z_1 > z_2 > \dots$$

cannot be continued indefinitely. Hence equation (A) cannot be satisfied by positive integers.

Thus we have the idea of the method of descent. As to the details, we observe in the first place that x and y can be supposed to be relatively prime; then two relatively prime integers p, q of different parity exist such that

$$x^2 = p^2 - q^2, \quad y^2 = 2pq, \quad z = p^2 + q^2.$$

Now p cannot be even, since otherwise

$$x^2 \equiv -1 \pmod{4},$$

which is impossible. So p is odd and q is even; then

$$\left(\frac{y}{2}\right)^2 = p \cdot \frac{q}{2}$$

and, since p and $\frac{1}{2}q$ are relatively prime and may be taken as positive,

$$p = r^2, \quad q = 2s^2, \quad y = 2rs.$$

Now the integers r, s must satisfy the equation

$$x^2 + 4s^4 = r^4,$$

from which it follows that

$$s^2 = \rho\sigma, \quad r^2 = \rho^2 + \sigma^2$$

with two relatively prime integers ρ, σ . The first equation implies that

$$\rho = f^2, \quad \sigma = g^2$$

and then the second becomes

$$f^4 + g^4 = r^2.$$

This equation is of the same form as (A). It is satisfied by positive integers f, g, r , and it is easy to prove that $r < z$. In fact

$$z = r^4 + 4s^4,$$

whence

$$r < \sqrt[4]{z}$$

and, a fortiori, $r < z$. From this proof it follows that if the equation (A) holds, then either $x = 0$ or $y = 0$, admitting positive or 0 values for the unknowns.

Passing to the second problem, we may confine ourselves to primitive right triangles whose sides are expressed in integers. Then the sides adjoining the right angle are

$$p^2 - q^2, \quad 2pq$$

and the area is

$$(p^2 - q^2)pq.$$

Since p, q are relatively prime and of different parity, the factors $p, q, p^2 - q^2$ are relatively prime in pairs and the area cannot be a square unless p, q and $p^2 - q^2$ are squares. Thus the problem reduces to one of finding integers x, y positive, relatively prime, and of different parity which satisfy the equation

$$x^4 - y^4 = z^2. \quad (B)$$

In this equation x is necessarily odd and y even. Writing it in the form

$$z^2 + y^4 = x^4,$$

we conclude

$$y^2 = 2pq, \quad x^2 = p^2 + q^2.$$

Since p and q are relatively prime and of different parity, we have, supposing p is odd,

$$p = r^2, \quad q = 2s^2, \quad y = 2rs$$

and

$$r^4 + 4s^4 = x^2,$$

whence again

$$r^2 = \rho^2 - \sigma^2; \quad s^2 = \rho\sigma.$$

Furthermore

$$\rho = f^2, \quad \sigma = g^2$$

and

$$f^4 - g^4 = r^2.$$

This equation, of the same form as (B), is satisfied by two positive relatively prime numbers f, g of different parity. Since

$$s = fg, \quad y = 2rfg, \quad fr > 2,$$

it follows that

$$g < \frac{y}{4} < y,$$

and so the step of descent is accomplished. Equation (B) therefore has no solution in positive integers.

Consider now the same equation but suppose that x, y are of the same parity, necessarily odd if they are relatively prime. Writing (B) in the form

$$y^4 + z^2 = x^4,$$

we have

$$y^2 = p^2 - q^2, \quad z = 2pq, \quad x^2 = p^2 + q^2,$$

whence

$$p^4 - q^4 = (xy)^2.$$

Here p, q are relatively prime and of different parity. Such an equation cannot hold unless $q = 0, p = 1$, but then $x = y = 1$ are the only positive and relatively prime integers satisfying equation (B).

6. Another Fermat Problem. We are now in a position to give complete solution of the equations

$$x^4 - 2y^2 = 1 \quad \text{and} \quad x^4 - 2y^2 = -1$$

in positive integers. These equations can be presented in the form

$$y^4 + x^4 = \left(\frac{x^4 + 1}{2}\right)^2 \quad \text{and} \quad y^4 - x^4 = \left(\frac{x^4 - 1}{2}\right)^2,$$

and, x being odd, the first is satisfied only by $x = 1, y = 0$, while the only solution of the second is $x = 1, y = 1$.

Fermat asserted that the system of Diophantine equations

$$x = 2y^2 - 1, \quad x^2 = 2z^2 - 1$$

has only two solutions in positive integers:

$$x = 1, \quad y = 1, \quad z = 1;$$

and

$$x = 7, \quad y = 2, \quad z = 5.$$

It is easy to prove this. The equation

$$x^2 = 2z^2 - 1$$

can be written in the form

$$\left(\frac{x+1}{2}\right)^2 + \left(\frac{x-1}{2}\right)^2 = z^2.$$

Since

$$\frac{x+1}{2} \quad \text{and} \quad \frac{x-1}{2}$$

are relatively prime numbers we must have, with the proper sign,

$$\frac{x \pm 1}{2} = r^2 - s^2, \quad \frac{x \mp 1}{2} = 2rs,$$

whence

$$r^2 - s^2 - 2rs = \pm 1, \quad x = r^2 - s^2 + 2rs.$$

Suppose at first that the upper sign holds. Then

$$\frac{x+1}{2} = r^2 - s^2 = y^2$$

or

$$s^2 + y^2 = r^2.$$

Since r and s are relatively prime, s and y are also relatively prime and r is odd, s even. Consequently

$$r = \rho^2 + \sigma^2, \quad s = 2\rho\sigma$$

which, being substituted into the equation

$$r^2 - s^2 - 2rs = (r - s)^2 - 2s^2 = 1,$$

gives

$$(\rho - \sigma)^2 - 2s^2 = 1,$$

whence necessarily

$$\rho - \sigma = \pm 1, \quad \rho\sigma = 0;$$

that is, either $\rho = \pm 1$, $\sigma = 0$, or $\rho = 0$, $\sigma = \mp 1$. In both cases $r = 1$, $s = 0$, and $x = 1$.

Consider now the lower sign. Then

$$r^2 - s^2 - 2rs = -1,$$

and s must be odd, r even. Moreover,

$$\frac{x+1}{2} = 2rs = y^2,$$

whence

$$r = 2\rho^2, \quad s = \sigma^2$$

and

$$\sigma^4 + 4\rho^2\sigma^2 - 4\rho^4 = 1$$

or

$$(\sigma^2 + 2\rho^2)^2 = 1 + 2(2\rho^2)^2.$$

By Sec. 2, Case 2, www.dbraulibrary.org.in

$$1 + 2\rho^2\sqrt{-2} = \pm(p + q\sqrt{-2})^2,$$

whence

$$p^2 - 2q^2 = \pm 1, \quad \rho^2 = \pm pq$$

and

$$p = a^2, \quad q = \pm b^2, \quad a^4 - 2b^4 = \pm 1.$$

By the preceding discussion the equation

$$a^4 - 2b^4 = 1$$

is satisfied only by $a = 1$, $b = 0$; then $\rho = 0$, $\sigma = 1$, $y = 0$, $x = -1$, $z = 1$, which is a trivial solution of the system. The equation

$$a^4 - 2b^4 = -1$$

is satisfied only by $a = 1$, $b = 1$. Then $p = 1$, $q = -1$, $\rho = 1$, $\sigma = 1$, and $y = 2$, $x = 7$, $z = 5$, and Fermat's statement is proved.

7. Fermat's Last Theorem. The most famous of Fermat's theorems, in complete form, is stated in the second observation to Diophantus as follows:

"A cube, however, cannot be split into two cubes or a biquadrate into two biquadrates, and in general no power beyond the second can be split into two similar powers. I have discovered a truly wonderful proof of this proposition but the margin is too small to contain it."

In modern notation the theorem asserts that for $n > 2$ the equation

$$x^n + y^n = z^n$$

has no solution in integers none of which is 0. While other theorems of Fermat have been proved, this one—the Last Theorem of Fermat—remains unproved in all generality. It is clear that it suffices to prove it for $n = 4$ and for prime odd values of n . The proof for $n = 4$ was given by Euler, and it follows immediately from the fact that no positive integers exist satisfying the equation

$$x^4 + y^4 = z^2.$$

For $n = 3$ the impossibility of satisfying the equation

$$x^3 + y^3 = z^3$$

by integers none of which is 0 was proved also by Euler. For fifth powers the Fermat theorem was proved in 1825 by Dirichlet and Legendre, and for seventh powers by Lamé in 1840, the latter proof being simplified considerably by V. A. Lebesgue. Soon afterwards Kummer applied his theory of cyclotomic numbers to Fermat's theorem and came to the startling result that the theorem is true for all prime exponents n such that the numerators of the Bernoullian numbers

$$B_1, B_2, B_3, \dots, B_{\frac{n-3}{2}}$$

are not divisible by n . Among the primes below 100 only 37, 59, and 67 do not satisfy this condition. In pursuing his deep investigations Kummer in 1857 published new criteria of a rather complicated nature whereby the cases $n = 37, 59, 67$ were absolved. Thus it was proved that Fermat's theorem holds for all prime exponents below 100.

In recent times H. S. Vandiver, by developing Kummer's method, discovered new criteria assuring the impossibility of Fermat's equation, and was able to verify Fermat's statement for all prime exponents < 617 . Kummer's investigations are deep and are based on the theory of a particular class of algebraic numbers depending on the roots of unity. We cannot possibly enter into this vast and important field, and we shall develop the proof of Fermat's theorem only for $n = 3$. The proofs for $n = 5$ and $n = 7$ are elementary but too long to be given a place here.

Let the three numbers x, y, z , none of which is 0, satisfy the equation

$$x^3 + y^3 = z^3. \quad (A)$$

We can suppose that x, y are relatively prime; then x, y, z will be relatively prime in pairs. Of these numbers two are necessarily odd, and we can suppose that x and y are odd. For if, for instance, x and z are odd, we can write equation (A) in the form

$$x^3 + (-z)^3 = (-y)^3.$$

Supposing, therefore, that x and y are odd, we set

$$x = p + q, \quad y = p - q$$

so that p, q are of different parity and relatively prime. On substitution, we get

$$2p(p^2 + 3q^2) = z^3, \quad (B)$$

whence it is clear that p is different from 0. Now z may or may not be divisible by 3. Let at first z be nondivisible by 3;

but at all events, z is even. Since $2p$ and $p^2 + 3q^2$ are relatively prime, we must have

$$p = 4\alpha^3, \quad p^2 + 3q^2 = \beta^3, \quad z = 2\alpha\beta.$$

Since p and q are relatively prime by Sec. 3, Case 3, the equation

$$p^2 + 3q^2 = \beta^3$$

implies

$$p + q\sqrt{-3} = (r + s\sqrt{-3})^3,$$

whence

$$p = r(r^2 - 9s^2), \quad q = 3s(r^2 - s^2).$$

But

$$p = 4\alpha^3,$$

and so

$$r(r + 3s)(r - 3s) = 4\alpha^3.$$

Since r and $3s$ are relatively prime and of different parity, the factors r , $r + 3s$, $r - 3s$ are relatively prime in pairs; consequently

$$r + 3s = \rho^3, \quad r - 3s = \sigma^3, \quad r = \frac{\tau^3}{2},$$

whence it follows that

$$\rho^3 + \sigma^3 = \tau^3.$$

Clearly none of the numbers ρ , σ , τ is 0, and we shall show that

$$|\tau| < |z|.$$

In fact

$$z = \rho\sigma\beta\tau, \quad \beta = r^2 + 3s^2 > 16,$$

whence it is clear that

$$|\tau| < \left| \frac{z}{16} \right| < |z|.$$

Suppose now that z is divisible by 3. Then by virtue of (B), p is divisible by 3 and, after canceling 9 on both sides, we have

$$\frac{2p}{3} \left(q^2 + 3 \left(\frac{p}{3} \right)^2 \right) = 3 \left(\frac{z}{3} \right)^3.$$

Since the factors on the left are relatively prime, we must have

$$p = 36\alpha^3, \quad q^2 + 3 \left(\frac{p}{3} \right)^2 = \beta^3, \quad z = 6\alpha\beta.$$

Again

$$q + \frac{p}{3} \sqrt{-3} = (r + s\sqrt{-3})^3,$$

whence

$$p = 9s(r^2 - s^2) = 36\alpha^3$$

or

$$s(r^2 - s^2) = 4\alpha^3.$$

But $s, r + s, r - s$ are prime in pairs since r, s are relatively prime and of different parity, hence necessarily

$$r + s = \rho^3, \quad r - s = -\sigma^3, \quad s = \frac{\tau^3}{2}$$

and

$$\rho^3 + \sigma^3 = \tau^3.$$

None of the numbers ρ, σ, τ is 0. Moreover

$$z = -3\rho\sigma\tau\beta, \quad \beta = r^2 + 3s^2 > 48$$

and

$$|\tau| < \left| \frac{z}{144} \right| < |z|.$$

Thus, if three integers none of which is 0 satisfy the equation

$$x^3 + y^3 = z^3, \quad z \text{ even,}$$

three other integers ρ, σ, τ none of which is 0 can be found so that

$$\rho^3 + \sigma^3 = \tau^3, \quad \tau \text{ even,}$$

while τ is numerically less than z . By the method of descent, we conclude that the equation

$$x^3 + y^3 = z^3$$

cannot be satisfied by integers none of which is 0.

Kronecker remarked that this particular case of Fermat's theorem gives a complete solution of the algebraic problem which consists in finding all cubic equations

$$x^3 + lx^2 + mx + n = 0$$

with rational coefficients and the discriminant 1. If x_1, x_2, x_3 are roots of the cubic equation, then its discriminant is by definition

$$D = (x_1 - x_2)^2(x_1 - x_3)^2(x_2 - x_3)^2.$$

The substitution

$$x = y - \frac{l}{3}$$

reduces the equation to the standard form

$$y^3 + ay + b = 0$$

without changing the discriminant. The discriminant of a cubic in standard form is

$$D = -(4a^3 + 27b^2),$$

and the problem amounts to solving the equation

$$4a^3 + 27b^2 + 1 = 0$$

in rational numbers a, b . There is one obvious solution

$$a = -1, \quad b = \frac{1}{3}.$$

To find whether there are other solutions with b different from $\frac{1}{3}$, we set

$$r = \frac{3b + 1}{3b - 1}, \quad s = \frac{2a}{3b - 1}.$$

Then

$$r^3 + s^3 - 1 = \frac{2(4a^3 + 27b^2 + 1)}{(3b - 1)^3} = 0.$$

But by Fermat's theorem the only rational solutions of the equation

$$r^3 + s^3 - 1 = 0$$

are

$$r = 1, \quad s = 0, \quad \text{or} \quad r = 0, \quad s = 1.$$

Now $s = 0$ implies $a = 0$, and the equation

$$27b^2 + 1 = 0$$

cannot be satisfied by a rational number. Consequently, necessarily $r = 0$, whence $b = -\frac{1}{3}$, $a = -1$.

Thus, all cubic equations with rational coefficients and discriminant 1 are

$$y^3 - y + \frac{1}{3} = 0$$

or their transforms by the substitution

$$x = y + c,$$

where c is an arbitrary rational number.

Exercises and Problems

1. Solve the equations

$$(a) x^2 + 1 = y^3; \quad (b) x^2 + 5 = y^3; \quad (c) x^2 + 6 = y^3.$$

Ans. (a) $x = 0, y = 1$; (b) no solution; (c) no solution.

2. Show that the only solution of the equation

$$x^4 + y^4 = 2z^2$$

in positive integers without common divisor is $x = y = z = 1$.

3. Solve in integers

$$\frac{x(x+1)}{2} = y^4$$

Ans. $x = 1$ or $x = -2$, and $y = \pm 1$.

4. Show that the equation

$$x^6 + y^6 = z^2$$

has no solution in positive integers.

5. If

$$x^3 + y^3 = 2z^3$$

and x, y, z are without common divisor, then $x = y = z = \pm 1$.

6. Solve the equations

$$(a) \frac{x(x+1)}{2} = y^3; \quad (b) x^2 - 1 = y^3$$

Ans. (a) $x = 1$ or $x = -2$ and $y = 1$; (b) $x = 0, y = -1; x = \pm 1,$
 $y = 0; x = \pm 3, y = 2.$

7. Neither of the equations

$$x^3 + y^3 = 4z^3, \quad x^3 + y^3 = 3z^3$$

has solutions in integers excluding $x = -y, z = 0$.

8. The only solution of the equation

$$x^4 - 3y^4 = 1$$

is $x = \pm 1, y = 0$.

9. Show that the same holds for the equation

$$x^4 - 3y^2 = 1.$$

10. Show that the only integers satisfying the system

$$x + 1 = y^2, \quad x^2 + 1 = 2z^2$$

are $x = -1, y = 0, z = \pm 1$.

11. The only solution of the system

$$x^2 + 1 = 2y^2, \quad 2y^2 + 1 = 3z^2$$

in positive integers is $x = y = z = 1$.

12. The only solution of the system

$$x^2 - 6y^2 = 1, \quad 2x^2 - z^2 = 1$$

in positive integers is $x = 5, y = 2, z = 7$.

8. One More Fermat Problem. In a letter to Mersenne in August (day unknown), 1643, Fermat mentions a problem

which we state in his own words: "Trouver un triangle duquel le plus grand côté soit carré et la somme des deux autres soit aussi carré." This problem has infinitely many solutions, and the simplest of them indicated by Fermat is expressed in very large numbers:

$$4,687,298,610,289; 4,565,486,027,761; 1,061,652,293,520.$$

In the statement of the problem, of course, a right-angle triangle with integral sides is meant.

Let the sides adjoining the right angle be a and b and the hypotenuse be d^2 ; the problem requires us to find two positive integers a and b such that

$$a + b = c^2, \quad a^2 + b^2 = d^4.$$

We may confine ourselves to seeking only relatively prime a and b . In fact let the g.c.d. of a and b be f^2e , where e has no square factors. Then c and d are both divisible by f . Let, therefore,

$$a = f^2e\alpha, \quad b = f^2e\beta, \quad c = f\gamma, \quad d = f\delta;$$

on substituting, we get

$$e(\alpha + \beta) = \gamma^2, \quad e^2(\alpha^2 + \beta^2) = \delta^4,$$

so that γ^2 and δ^2 are divisible by e and, since e has no square factors, γ and δ will be divisible by e also. Therefore

$$\alpha + \beta \equiv 0 \pmod{e}, \quad \alpha^2 + \beta^2 \equiv 0 \pmod{e^2},$$

whence

$$(\alpha + \beta)^2 + (\alpha - \beta)^2 \equiv 0 \pmod{e^2}$$

and

$$\alpha - \beta \equiv 0 \pmod{e}.$$

Since α and β are relatively prime and of different parity, we must have $e = 1$.

The problem is thus reduced to one of solving the system

$$\alpha + \beta = \gamma^2, \quad \alpha^2 + \beta^2 = \delta^4$$

in relatively prime integers α, β , and all other solutions of the problem will be given by

$$a = f^2\alpha, \quad b = f^2\beta, \quad c = f\gamma, \quad d = f\delta.$$

We can, therefore, limit ourselves at the outset to relatively prime a and b that are also of different parity. Supposing $a > b$, let us set

$$a - b = e.$$

Then the equations

$$a + b = c^2, \quad a^2 + b^2 = d^4$$

give

$$2d^4 - c^4 = e^2 \tag{A}$$

and d, c, e are odd numbers. Since

$$a = \frac{c^2 + e}{2}, \quad b = \frac{c^2 - e}{2}$$

must be positive, $c^2 > e$, which is equivalent to the inequality $c > d$. Thus the problem is reduced to finding all the solutions of equation (A) in positive integers, relatively prime in pairs, d, c, e that satisfy the added condition $c > d$.

Equation (A) can be written in the form

$$\left(\frac{c^2 + e}{2}\right)^2 + \left(\frac{c^2 - e}{2}\right)^2 = d^4,$$

whence, choosing the sign \pm properly,

$$\frac{c^2 \pm e}{2} = p^2 - q^2, \quad \frac{c^2 \mp e}{2} = 2pq$$

and

$$d^2 = p^2 + q^2, \quad c^2 = p^2 - q^2 + 2pq.$$

Since p, q are relatively prime and of different parity, one of them must be even and the other odd; the second equation shows that p is odd. Correspondingly, there are two numbers r, s such that

$$d = r^2 + s^2; \quad p = r^2 - s^2; \quad q = 2rs.$$

The equation

$$c^2 = p^2 - q^2 + 2pq$$

can be written in the form

$$c^2 + 2q^2 = (p + q)^2,$$

whence

$$c + q\sqrt{-2} = \pm(\rho \pm \sigma\sqrt{-2})^2$$

and

$$c = \pm(\rho^2 - 2\sigma^2), \quad q = 2\rho\sigma.$$

As to $p + q$, we can assume it to be positive, since in the contrary case we can change p, q into $-p, -q$. Then

$$p + q = \rho^2 + 2\sigma^2$$

and

$$p = \rho^2 + 2\sigma^2 - 2\rho\sigma = r^2 - s^2; \quad q = 2rs = 2\rho\sigma$$

or

$$rs = \rho\sigma.$$

If

$$\frac{r}{\rho} = \frac{d_1}{c_1},$$

where c_1 and d_1 are relatively prime, then

$$\begin{aligned} r &= td_1, & \rho &= tc_1, \\ s &= uc_1, & \sigma &= ud_1, \end{aligned}$$

t and u being relatively prime integers. On substituting these values into the equation

$$\rho^2 + 2\sigma^2 - 2\rho\sigma = r^2 - s^2,$$

we get

$$(c_1^2 + 2d_1^2)u^2 - 2c_1d_1tu + (c_1^2 - d_1^2)t^2 = 0,$$

whence

$$\frac{u}{t} = \frac{c_1d_1 \pm \sqrt{2d_1^4 - c_1^4}}{c_1^2 + 2d_1^2}.$$

It is necessary, therefore, that $2d_1^4 - c_1^4$ should be a square; let

$$2d_1^4 - c_1^4 = e_1^2;$$

then

$$\frac{u}{t} = \frac{c_1d_1 \pm e_1}{c_1^2 + 2d_1^2}.$$

Thus from one solution d, c, e of equation (A) another solution d_1, c_1, e_1 of the same equation is derived and, unless $q = 0$, in the new solution $d_1 < \frac{1}{2}d$. In fact, if $q \neq 0$,

$$r^2 \leq \frac{1}{4}q^2 < \frac{1}{4}d^2, \quad d_1 \leq r,$$

and so $d_1 < \frac{1}{2}d$. Corresponding to $q = 0$ we have $p = \pm 1$ and $d = c = e = 1$. From this consideration it follows that from any solution with $d > 1$ we can descend to solutions $d_1, c_1, e_1; d_2, c_2, e_2; d_3, c_3, e_3; \dots$ such that

$$d > d_1 > d_2 > d_3 > \dots,$$

and this process of descent will end only when we reach the solution 1, 1, 1. Reversing the process, from this particular solution, we can ascend to any other solution of equation (A). This reversal of the process can be carried out as follows.

First we find two relatively prime integers t, u from

$$\frac{u}{t} = \frac{c_1d_1 \pm e_1}{c_1^2 + 2d_1^2},$$

where c_1, d_1, e_1 is some solution. Next r, s, p, σ are determined by

$$\begin{aligned} r &= td_1, & s &= uc_1 \\ \rho &= tc_1, & \sigma &= ud_1, \end{aligned}$$

and finally

$$\begin{aligned} d &= r^2 + s^2, & c &= \pm(\rho^2 - 2\sigma^2), \\ \pm e &= (r^2 - s^2 - 2rs)^2 - 8r^2s^2. \end{aligned}$$

Let us start with the solution $d_1 = c_1 = e_1 = 1$. Then for the fraction u/t we have two values:

$$\frac{u}{t} = \frac{0}{3}, \quad \frac{u}{t} = \frac{2}{3}.$$

The first possibility does not lead to any new solution. The second possibility gives

$$u = 2, \quad t = 3; \quad r = 3, \quad s = 2; \quad \rho = 3, \quad \sigma = 2,$$

whence

$$d = 13, \quad c = 239.$$

Starting from this solution, we have

$$\frac{u}{t} = \frac{13 - 239}{339} = \frac{-226}{339} = \frac{-2}{3}; \quad \frac{u}{t} = \frac{252}{339} = \frac{84}{113},$$

whence

$$u = -2, \quad t = 3 \quad \text{or} \quad u = 84, \quad t = 113.$$

Correspondingly,

$$\begin{aligned} r &= 39, & s &= -2; & \rho &= 3, & \sigma &= -26 \\ d &= 1,525, & c &= 1,343, & e &= 2,750,257, \end{aligned}$$

and

$$\begin{aligned} r &= 1,469, & s &= 84; & \rho &= 113, & \sigma &= 1,092, \\ d &= 2,165,017, & c &= 2,372,159, & e &= 3,503,833,734,241. \end{aligned}$$

This solution is the first in which $c > d$. The corresponding right triangle of smallest size as required in Fermat's problem has the following sides:

$$a = \frac{c^2 + e}{2} = 4,565,486,027,761;$$

$$b = \frac{c^2 - e}{2} = 1,061,652,293,520,$$

and the hypotenuse

$$d^2 = 4,687,298,610,289.$$

There are infinitely many such triangles, as the equation

$$2d^4 - c^4 = e^2$$

has infinitely many solutions in which $c > d$. The proof of this, which is not difficult, we leave to the reader.

9. An Ancient Problem. It is a characteristic feature of the theory of numbers that simple and easily understandable problems can be given long before any means for their solution are available. Just such a problem was discussed in the Middle Ages by Arab scholars concerning so-called congruent numbers. A positive integer a is called a congruent number if a rational fraction h can be found so that both

$$h^2 + a \quad \text{and} \quad h^2 - a$$

are squares. Clearly if we wish to determine whether or not a is a congruent number, we have to seek integral solutions of the Diophantine system

$$x^2 + ay^2 = z^2, \quad x^2 - ay^2 = t^2.$$

Even at the present time, with mighty tools available, there is no sure and general way of ascertaining the possibility of this system and, in case of its possibility, of finding all solutions for an arbitrarily given a . However, for some particular values of a , such as 5, 6, 7, etc., a complete solution is possible.

Here we shall solve completely the system

$$x^2 + 5y^2 = z^2, \quad x^2 - 5y^2 = t^2$$

in positive and relatively prime integers x, y . We notice first that x and y cannot be both odd, for then $x^2 + 5y^2$ would be divisible only by 2 and not by 4. Moreover, x must be odd and y even. Then the equation

$$x^2 + 5y^2 = z^2$$

is satisfied in the most general way by setting

$$x + y\sqrt{-5} = \pm(r \pm s\sqrt{-5})^2,$$

whence

$$x = \pm(r^2 - 5s^2), \quad y = 2rs, \quad z = r^2 + 5s^2.$$

Similarly the equation

$$x^2 - 5y^2 = f^2$$

is satisfied in the most general way by setting

$$x + y\sqrt{5} = (f + g\sqrt{5})^2,$$

whence

$$x = f^2 + 5g^2, \quad y = 2fg, \quad t = \pm(f^2 - 5g^2).$$

If y , as we suppose, is a positive number, none of the numbers r, s, f, g will be 0. Moreover, r and $5s, f$ and $5g$, are relatively prime and of different parity. Comparing the two values of y , we have

$$rs = fg,$$

and the most general way of satisfying this equation is to set

$$\begin{aligned} r &= ab, & f &= ac \\ s &= cd, & g &= bd. \end{aligned}$$

Since r and f can be assumed to be positive, a, b, c, d will be positive integers and a relatively prime to b, c, d ; b relatively prime to c, d, a ; etc. On comparing the two expressions for x , we get

$$a^2c^2 + 5b^2d^2 = \pm(a^2b^2 - 5c^2d^2),$$

and in the future discussion we must treat the signs \pm separately.

In case of the sign $+$ we have

$$c^2(a^2 + 5d^2) = b^2(a^2 - 5d^2)$$

and, since c and b are relatively prime as well as a and $5d$, we must have

$$a^2 + 5d^2 = b^2, \quad a^2 - 5d^2 = c^2.$$

Thus from one solution of our system we descend to another in which $d < y$, since

$$y = 2abcd.$$

In case of the sign $-$, we have

$$c^2(a^2 - 5d^2) = -b^2(a^2 + 5d^2),$$

whence again

$$a^2 - 5d^2 = -b^2, \quad a^2 + 5d^2 = c^2.$$

In this case we have a system different from the original one. This system can be replaced by an equivalent system

$$c^2 - b^2 = 2a^2, \quad a^2 + 5d^2 = c^2.$$

Now a must be even and b odd. From the first equation, written in the form

$$b^2 + 2a^2 = c^2,$$

it follows that

$$b + a\sqrt{-2} = \pm(p \pm q\sqrt{-2})^2$$

and

$$b = \pm(p^2 - 2q^2), \quad a = 2pq, \quad c = p^2 + 2q^2.$$

On substituting this into the equation

$$c^2 - a^2 = 5d^2,$$

we get

$$p^4 + 4q^4 = 5d^2.$$

Of course neither p nor q is divisible by 5; but then with a proper choice of sign

$$p^2 \mp q^2 \equiv 0 \pmod{5}.$$

The equation itself can be written thus:

$$\left(\frac{p^2 \pm 4q^2}{5}\right)^2 + 4\left(\frac{p^2 \mp q^2}{5}\right)^2 = d^2$$

and, since

$$\frac{p^2 \pm 4q^2}{5} \quad \text{and} \quad \frac{p^2 \mp q^2}{5}$$

are clearly relatively prime, we shall have

$$\frac{p^2 \pm 4q^2}{5} = \rho^2 - \sigma^2, \quad \frac{p^2 \mp q^2}{5} = \rho\sigma, \quad d = \rho^2 + \sigma^2,$$

whence

$$p^2 = \rho^2 - \sigma^2 - 4\rho\sigma, \quad q^2 = \rho^2 - \sigma^2 - \rho\sigma.$$

We shall show now that the minus sign is impossible. Clearly p and q are both odd, and in case the sign $-$ holds,

$$p^2 + q^2 = 5\rho\sigma \equiv 2 \pmod{8},$$

whence

$$\rho\sigma \equiv 2 \pmod{8}.$$

Also

$$q^2 + \rho^2 - \sigma^2 = \rho\sigma \equiv 2 \pmod{8},$$

whence, because q and ρ are odd,

$$q^2 + \rho^2 - \sigma^2 \equiv 2 - \sigma^2 \equiv 2 \pmod{8}$$

or

$$\sigma^2 \equiv 0 \pmod{8},$$

which shows that σ must be divisible by 4, and this is in contradiction to the congruence

$$\rho\sigma \equiv 2 \pmod{8}.$$

Thus

$$p^2 = \rho^2 - \sigma^2 + 4\rho\sigma, \quad q^2 = \rho^2 - \sigma^2 - \rho\sigma$$

and

$$\frac{p+q}{2} \cdot \frac{p-q}{2} = 5\rho\frac{\sigma}{4}$$

Supposing that $\sigma \neq 0$, we find four integers $\alpha, \beta, \gamma, \delta$, none of which is 0, such that

$$\frac{p \pm q}{2} = 5\alpha\beta; \quad \rho = \alpha\gamma,$$

$$\frac{p \mp q}{2} = \gamma\delta; \quad \sigma = 4\beta\delta,$$

whence

$$p = \gamma\delta + 5\alpha\beta.$$

On substituting these expressions in

$$p^2 = \rho^2 - \sigma^2 + 4\rho\sigma,$$

we get, after obvious simplifications,

$$\delta^2(\gamma^2 + 16\beta^2) - 6\alpha\beta\gamma\delta + \alpha^2(25\beta^2 - \gamma^2) = 0,$$

whence

$$\frac{\delta}{\alpha} = \frac{3\beta\gamma \pm \sqrt{\gamma^4 - 25(2\beta)^4}}{\gamma^2 + 16\beta^2}.$$

Since γ and 5β are relatively prime,

$$\gamma^4 - 25(2\beta)^4$$

cannot be a square unless

$$\gamma^2 + 5(2\beta)^2 = \epsilon^2, \quad \gamma^2 - 5(2\beta)^2 = \theta^2,$$

in which case

$$\frac{\delta}{\alpha} = \frac{3\beta\gamma \pm \epsilon\theta}{\gamma^2 + 16\beta^2}.$$

Thus from the original solution of our system we get another solution $\gamma, 2\beta; \epsilon, \theta$, but 2β will be smaller than y . To prove this, notice in the first place that

$$p^2 + 4q^2 = 5(\rho^2 - \sigma^2),$$

so that

$$\rho^2 - \sigma^2 > 0.$$

If $\rho\sigma > 0$, then it follows that

$$4\rho\sigma < p^2.$$

On the other hand,

$$y = 2abcd = 4pqbcd,$$

whence

$$p \leq \frac{y}{4},$$

and so

$$\sigma^2 < \frac{y}{8}, \quad |\sigma| < \frac{y}{8}.$$

But

$$\sigma = 4\beta\delta$$

and finally

$$2\beta \leq \frac{|\sigma|}{2} < \frac{y}{16}.$$

If $\rho\sigma < 0$, then from

$$q^2 = \rho^2 - \sigma^2 - \rho\sigma$$

it follows that

$$\sigma^2 < -\rho\sigma < q^2$$

and

$$|q| \leq \frac{y}{4}$$

Again

$$2\beta \leq \frac{|\sigma|}{2} < \frac{y}{8}.$$

Thus, in all cases, $2\beta < y$.

We shall apply this process to finding some of the solutions not involving excessively large numbers. We start with

$$a = 41, \quad d = 12, \quad b = 49, \quad c = 31 \quad (1)$$

and pass to another solution (1). We have

$$\begin{aligned} f &= 41 \cdot 31 = 1,271, & g &= 49 \cdot 12 = 588 \\ r &= 41 \cdot 49 = 2,009, & s &= 31 \cdot 12 = 372, \end{aligned}$$

and

$$\begin{aligned} x &= f^2 + 5g^2 = 3,344,161, & y &= 1,494,696 \\ z &= r^2 + 5s^2 = 4,728,001, & t &= 113,279, \end{aligned}$$

is another solution (1). Now from

$$\gamma = 41, \quad \beta = 6, \quad \epsilon = 49, \quad \theta = 31$$

we ascend to two solutions (2). First we determine relatively prime δ, α from

$$\frac{\delta}{\alpha} = \frac{3\beta\gamma + \epsilon}{\gamma^2 + 16\beta^2}, \quad \frac{\delta}{\alpha} = \frac{\epsilon\theta}{\gamma^2 + 16\beta^2}.$$

We have

$$\frac{\delta}{\alpha} = \frac{2,257}{2,257} = \frac{1}{1}, \quad \frac{\delta}{\alpha} = \frac{-781}{2,257}.$$

Dropping the second possibility as leading to very large numbers, we take

$$\delta = 1, \quad \alpha = 1$$

and determine

$$\begin{aligned} \rho &= \alpha\gamma = 41, & \sigma &= 4\beta\delta = 24 \\ p &= \gamma\delta + 5\alpha\beta = 71, & \pm q &= 11 \end{aligned}$$

after which

$$a = 1,562, \quad d = 2,257, \quad b = 4,799, \quad c = 5,283$$

is a solution (2). From this solution we ascend to a new solution (1) by computing

$$\begin{aligned} f &= ac = 8,252,046, & g &= bd = 10,831,343 \\ r &= ab = 7,496,038, & s &= cd = 11,923,731 \end{aligned}$$

and

$$\begin{aligned}e &= f^2 + 5g^2 = 654,686,219,104,361 \\y &= 2fg = 178,761,481,355,556 \\z &= r^2 + 5s^2 = 767,067,390,499,249 \\t &= 5g^2 - f^2 = 518,493,692,732,129.\end{aligned}$$

Thus the three solutions of the system

$$x^2 + 5y^2 = z^2, \quad x^2 - 5y^2 = t^2$$

in smallest integers are

$$\begin{array}{llll}x = 41, & y = 12, & z = 49, & t = 31 \\x = 3,344,161, & y = 1,494,696, & z = 3,344,161, & t = 1,494,696 \\z = 4,728,001, & t = 113,279, & & \\x = 654,686,219,104,361, & y = 178,761,481,355,556, & & \\z = 767,067,390,499,249, & t = 518,493,692,732,129, & & \end{array}$$

and there are no other solutions with smaller y .

Exercises and Problems

1. Show that the system www.dbraulibrary.org.in

$$x^2 + 2y^2 = z^2, \quad x^2 - 2y^2 = t^2$$

has no solution in positive integers.

2. Show that the same is true of the system

$$x^2 + py^2 = z^2, \quad x^2 - py^2 = t^2$$

if $p \equiv 3 \pmod{8}$ is a prime.

3. Devise the method for the complete solution of the equation

$$x^4 - 2y^4 = z^2$$

and find two solutions in smallest integers.

4. Do the same for the equation

$$x^4 + 8y^4 = z^2.$$

5. Show that the equation

$$x^4 - 8y^4 = z^2$$

has no solution in positive integers.

6. Show that the system

$$a^2 + 4d^2 = b^2, \quad a^2 + 3d^2 = c^2$$

has no solution in positive integers.

7. The equation

$$x^4 + x^2y^2 + y^4 = z^2$$

likewise has no solution in positive integers.

8. Show that the system

$$c^2 + 9b^2 = d^2, \quad c^2 + 12b^2 = a^2$$

has no solution in positive integers.

9. Show that the only solution of the equation

$$x^4 + x^2y^2 + y^4 = 3z^2$$

in positive relatively prime integers is $x = y = z = 1$.

10. Devise the method for the complete solution of the system

$$2x^2 - y^2 = z^2, \quad 2x^2 + y^2 = 3t^2$$

and find three solutions in smallest integers.

11. Do the same for the system

$$x^2 + 6y^2 = z^2, \quad x^2 - 6y^2 = t^2.$$

12. Show that the fraction

$$\frac{x^2 + 2y^2}{2x^2 + y^2}$$

can be a square only if it is equal to 1.

CHAPTER XIII

LIOUVILLE'S METHODS

1. Object of This Chapter. The theory of numbers borrows its tools of investigation from almost every branch of mathematics. A great many of the important questions are dealt with in the most natural manner by geometric methods, and such developments constitute the so-called "geometry of numbers." The applications of analysis to the solution of arithmetical problems are numerous and are gaining steadily in importance, so that, at the present time, the most brilliant advances in the theory of numbers are due almost exclusively to analytical methods. Naturally, neither the character nor the size of this book permits the inclusion of anything, with one exception, concerning either geometrical or analytical methods in the theory of numbers.

Since its very inception the theory of elliptic functions has been an abundant source of a great many peculiar and interesting arithmetical theorems. It would be, of course, impossible to speak here in detail of elliptic functions. Fortunately, as Liouville (1809-1882) has shown, their use can be superseded by some very general arithmetical identities which either can be derived from various expansions in the theory of elliptic functions or established directly in the most elementary manner. Once the fundamental identities are established, by their specialization and adaptation, innumerable special results are obtained in quite a simple way. In this chapter we shall confine ourselves to only a few applications, intended to show the fertility of Liouville's methods;

and, as a crowning achievement, we shall produce a complete solution of the problem concerning the representation of integers by sums of three squares.

2. Arbitrary Functions. Conditions of Parity. In what follows we shall deal with arbitrary functions

$$F(x, y, z)$$

defined for integral values of the arguments x, y, z and subject to certain conditions of parity. We say that $F(x, y, z)$ is an even function with regard to x if

$$F(-x, y, z) = F(x, y, z)$$

for all integral values of x, y, z . Similarly $F(x, y, z)$ is an odd function with regard to x , if

$$F(-x, y, z) = -F(x, y, z)$$

for all integral values of x, y, z . In particular the latter implies

$$F(0, y, z) = 0.$$

With regard to the pair of variables y, z , the function $F(x, y, z)$ is even or odd according as

$$F(x, -y, -z) = F(x, y, z)$$

or

$$F(x, -y, -z) = -F(x, y, z).$$

As an example,

$$F(x, y, z) = xyz$$

is an odd function with regard to each variable, but is an even function with regard to the pair y, z . Another example is

$$\begin{aligned} F(x, y, z) &= 0 & \text{if } x^2 \neq 1 \\ F(\pm 1, y, z) &= (y - z)^2. \end{aligned}$$

This function is even with regard to x and also even with regard to the pair y, z , but neither even nor odd with regard to y or z taken alone.

3. The First Fundamental Identity. The first fundamental identity involves an arbitrary function $F(x, y, z)$ defined for all integral values of its arguments and satisfying the following conditions of parity:

$$F(-x, y, z) = -F(x, y, z), \quad F(x, -y, -z) = F(x, y, z), \\ F(0, y, z) = 0.$$

Let n be an arbitrary positive integer, $\lambda > \mu > 0$ be two positive numbers the nature of which is not specified. We shall consider partitions of n of the following types:

$$(a) \quad n = \lambda i^2 + \mu i + (\lambda \delta + \mu) d. \\ (b) \quad n = \lambda i^2 - \mu i + (\lambda \delta - \mu) d. \\ (c) \quad n = \lambda h^2 + \mu h + \lambda \Delta \Delta'.$$

In (a) and (b), i is an integer, positive, 0, or negative, while d and δ are positive integers. By virtue of the condition $\lambda > \mu > 0$ there is only a finite number of partitions (a) and (b) if there are such partitions at all. In (c), h is an integer positive, 0, or negative, while Δ and Δ' are positive integers. Clearly there is only a limited number of partitions (c).

The first fundamental identity can be presented thus:

$$\sum_{(a)} F(\delta - 2i, d + i, 2d + 2i - \delta) + \\ \sum_{(b)} F(\delta - 2i, d + i, 2d + 2i - \delta) = \\ \sum_{(c)} F(\Delta + \Delta', h, \Delta - \Delta') + T - U,$$

the summations being extended, respectively, over all partitions (a), (b), (c). As to the complementary terms T, U , they are

$$U = \sum_{(d)} F\left(\Delta + \Delta', \frac{\Delta - \Delta'}{2}, \Delta - \Delta'\right),$$

where the summation extends over all representations of n in the form

$$(d) \quad n = \lambda \left(\frac{\Delta + \Delta'}{2}\right)^2 + \mu \frac{\Delta - \Delta'}{2}; \quad \Delta' \equiv \Delta \pmod{2},$$

with positive integers Δ and Δ' of the same parity; and

$$T = \sum_{(e)} F(2|s| - j, |s|, 2|s| - j); \quad j = 1, 2, 3, \dots, 2|s| - 1,$$

where the summation, for each solution of the equation,

$$(e) \quad n = \lambda s^2 + \mu s$$

is extended over $j = 1, 2, 3, \dots, 2|s| - 1$. It must be understood that whenever partitions of one of the indicated types are absent, the corresponding sum must be replaced by 0.

Despite the complicated appearance of the fundamental identity the proof of it is, indeed, very simple. Consider first the sum

$$S = \sum_{(a)} F(\delta - 2i, d + i, 2d + 2i - \delta)$$

and split it into three parts S_1, S_2, S_3 , which correspond, respectively, to the solutions of the equation

$$(a) \quad n = \lambda i^2 + \mu(d + i) + \lambda d \delta,$$

in which $2i + d - \delta > 0$, $2i + d - \delta = 0$, $2i + d - \delta < 0$. To every solution i, d, δ of (a) in which $2i + d - \delta > 0$ the formulas

$$i' = \delta - i, \quad d' = 2i + d - \delta, \quad \delta' = \delta$$

give a corresponding solution of the same kind, for we have conversely

$$i = \delta' - i', \quad d = 2i' + d' - \delta', \quad \delta = \delta'.$$

Notice besides that

$$\begin{aligned} \delta' - 2i' &= -\delta + 2i, & d' + i' &= d + i, \\ 2d' + 2i' - \delta' &= 2d + 2i - \delta. \end{aligned}$$

When i, d, δ run through solutions of the first kind, i', d', δ' run through the same solutions. Consequently

$$\begin{aligned} S_1 &= \Sigma F(\delta - 2i, d + i, 2d + 2i - \delta) \\ &= \Sigma F(\delta' - 2i', d' + i', 2d' + 2i' - \delta'); \end{aligned}$$

but

$$\begin{aligned} F(\delta' - 2i', d' + i', 2d' + 2i' - \delta') &= \\ F(-\delta + 2i, d + i, 2d + 2i - \delta) &= \\ -F(\delta - 2i, d + i, 2d + 2i - \delta), \end{aligned}$$

and so

$$S_1 = -S_1,$$

whence $S_1 = 0$.

We turn now to the sum S_2 corresponding to solutions of equation (a) in which $2i + d - \delta < 0$. To each such solution the formulas

$$h = d + i, \quad \Delta = d, \quad \Delta' = \delta - d - 2i$$

give a corresponding solution h, Δ, Δ' of the equation

$$(c) \quad n = \lambda h^2 + \mu h + \lambda \Delta \Delta',$$

in which

$$\Delta' - \Delta + 2h > 0.$$

Conversely, to each solution of this nature corresponds a solution

$$i = h - \Delta, \quad d = \Delta, \quad \delta = \Delta' - \Delta + 2h$$

of equation (a) in which $2i + d - \delta < 0$. Consequently

$$S_3 = \Sigma F(\Delta + \Delta', h, \Delta - \Delta'),$$

where the summation extends over all solutions of (c) satisfying the inequality

$$\Delta' - \Delta + 2h > 0.$$

It remains to consider the sum S_2 corresponding to solutions of (a) in which $2i + d - \delta = 0$, or

$$i = \frac{\delta - d}{2}.$$

For this value of i equation (a) becomes

$$n = \lambda \left(\frac{d + \delta}{2} \right)^2 + \mu \frac{d + \delta}{2}.$$

Unless, therefore,

$$n = \lambda s^2 + \mu s$$

with positive integer s , the sum S_2 reduces to 0. Otherwise,

$$\begin{aligned} d + \delta = 2s, \quad \delta - 2i = 2s - \delta, \quad d + i = s, \\ 2d + 2i - \delta = 2s - \delta, \end{aligned}$$

and δ can assume all values $1, 2, 3, \dots, 2s - 1$, so that

$$S_2 = \Sigma F(2s - j, s, 2s - j),$$

j running through the values $1, 2, 3, \dots, 2s - 1$.

The sum

$$S' = \sum_{(b)} F(\delta - 2i, d + i, 2d + 2i - \delta)$$

can be split again into three parts S'_1, S'_2, S'_3 , corresponding to solutions of the equation

$$(b) \quad n = \lambda i^2 - \mu(i + d) + \lambda d\delta,$$

in which $2i + d - \delta > 0$, $2i + d - \delta = 0$, $2i + d - \delta < 0$, respectively. Exactly the same discussion as before shows that

$$S'_1 = 0$$

and

$$S'_2 = \sum F(\Delta + \Delta', h, \Delta - \Delta'),$$

the summation extending over all partitions

$$n = \lambda h^2 - \mu h + \lambda \Delta \Delta',$$

in which $\Delta - \Delta + 2h > 0$. But as $-h, \Delta', \Delta$ run through the same set of values as h, Δ, Δ' in equation (c) we have also

$$S'_2 = \sum F(\Delta + \Delta', -h, \Delta' - \Delta),$$

or because $F(x, y, z)$ is even with regard to y, z

$$S'_2 = \sum F(\Delta + \Delta', h, \Delta - \Delta'),$$

where the summation extends over all solutions of (c) in which $\Delta' - \Delta + 2h < 0$. Finally, $S'_2 = 0$ unless

$$n = \lambda s^2 - \mu s$$

with s a positive integer, in which case

$$S'_2 = \sum F(2s - j, s, 2s - j); \quad j = 1, 2, 3, \dots, 2s - 1.$$

From this discussion it follows that the left-hand side of the fundamental identity reduces to

$$S_3 + S'_2 + S_2 + S'_2.$$

But

$$S_3 + S'_2$$

differs from

$$\sum_{(c)} F(\Delta + \Delta', h, \Delta - \Delta')$$

only by terms in which $\Delta' - \Delta + 2h = 0$, and these terms combine to give U ; also it is clear that

$$S_2 + S'_2 = T,$$

and so the first fundamental identity is proved.

4. The Second Fundamental Identity. If we suppose that $F(x, y, z)$ satisfies the conditions

$$F(-x, y, z) = -F(x, y, z), \quad F(x, -y, -z) = -F(x, y, z), \\ F(0, y, z) = 0$$

and repeat exactly the same reasoning as above, paying attention to the fact that now $F(x, y, z)$ is odd with regard to the pair y, z , we get the second fundamental identity

$$\sum_{(a)} F(\delta - 2i, d + i, 2d + 2i - \delta) - \\ \sum_{(b)} F(\delta - 2i, d + i, 2d + 2i - \delta) = \\ \sum_{(c)} F(\Delta + \Delta', h, \Delta - \Delta') + T_1 - T_2 - U$$

where the extent of the summations indicated by (a), (b), (c) and the expression for U is exactly the same as in the first fundamental identity, while $T_1 = 0$ unless

$$n = \lambda s^2 + \mu s$$

with s a positive integer, in which case

$$T_1 = \Sigma F(2s - j, s, 2s - j); \quad j = 1, 2, 3, \dots, 2s - 1.$$

Similarly $T_2 = 0$ unless

$$n = \lambda s^2 - \mu s$$

with a positive integer s , in which case

$$T_2 = \Sigma F(2s - j, s, 2s - j); \quad j = 1, 2, 3, \dots, 2s - 1.$$

5. Euler's Recurrence Formula. The famous recurrence formula for the sum of divisors discovered by Euler has already been mentioned in Sec. 9, Chap. IV. Now we can prove it very simply by using the fundamental identities in which $F(x, y, z)$ is specialized in a proper way. Let

$$F(x, y, z) = 0 \text{ if either } x \text{ or } z \text{ is even;}$$

$$F(x, y, z) = (-1)^{\frac{x+z}{2}+y} \text{ if both } x \text{ and } z \text{ are odd.}$$

Then

$$F(-x, y, z) = -F(x, y, z), \quad F(x, -y, -z) = -F(x, y, z), \\ F(0, y, z) = 0,$$

and we can use this function in the second fundamental identity in which, besides, we shall take $\lambda = \frac{3}{2}i$, $\mu = \frac{1}{2}$.

Noticing that $U = 0$ with this definition of $F(x, y, z)$, we shall have

$$\sum_{(a)} (-1)^i - \sum_{(b)} (-1)^i = \sum_{(c)} (-1)^{h+\Delta} + T_1 - T_2,$$

where the summations indicated by (a), (b), (c) refer to the partitions

$$(a) \quad n = \frac{3i^2 + i}{2} + \frac{3\delta + 1}{2}d, \quad \delta \text{ odd.}$$

$$(b) \quad n = \frac{3i^2 - i}{2} + \frac{3\delta - 1}{2}d, \quad \delta \text{ odd.}$$

$$(c) \quad n = \frac{3h^2 + h}{2} + \frac{3}{2}\Delta\Delta', \quad \Delta' + \Delta \text{ odd.}$$

As to $T_1 - T_2$, considering that only one integer t positive or negative can satisfy the equation

$$n = \frac{3t^2 + t}{2},$$

we easily find that in all cases

$T_1 - T_2 = 0$ if n is not a pentagonal number;

$$T_1 - T_2 = (-1)^{s-1}s \quad \text{if} \quad n = \frac{3s^2 + s}{2}, \quad s \geq 0.$$

In the sum

$$\sum_{(c)} (-1)^{h+\Delta}$$

to each term

$$(-1)^{h+\Delta}$$

corresponds a term

$$(-1)^{h+\Delta'}$$

obtained by interchanging Δ and Δ' . Since Δ and Δ' are of different parity, the contribution due to such corresponding terms

$$(-1)^{h+\Delta} + (-1)^{h+\Delta'} = 0,$$

whence it follows that

$$\sum_{(c)} (-1)^{h+\Delta} = 0.$$

Thus we have the following result:

$$\begin{aligned} \sum_{(a)} (-1)^i - \sum_{(b)} (-1)^i &= 0 \text{ if } n \text{ is not a pentagonal number,} \\ &= (-1)^{s-1}s \quad \text{if} \quad n = \frac{3s^2 + s}{2}, \quad s \geq 0, \quad (A) \end{aligned}$$

the arithmetical interpretation of which will be given later.

In the first fundamental identity we are entitled to take

$F(x, y, z) = 0$ if either x or z is even,

$F(x, y, z) = (-1)^{\frac{x+z}{2}+y} (2y - z)$ if both x and z are odd,

for then

$$F(-x, y, z) = -F(x, y, z), \quad F(x, -y, -z) = F(x, y, z), \\ F(0, y, z) = 0.$$

The result will be

$$\sum_{(a)} (-1)^i \delta + \sum_{(b)} (-1)^i \delta = \sum_{(c)} (-1)^{h+\Delta} (2h + \Delta' - \Delta) + T,$$

where

$$T = 0 \text{ if } n \text{ is not a pentagonal number,} \\ T = (-1)^{s-1} s^2 \quad \text{if} \quad n = \frac{3s^2 + s}{2}, \quad s \geq 0.$$

For the same reason as before

$$\sum_{(c)} (-1)^{h+\Delta} h = 0,$$

so that the preceding relation can be simplified and put into the form

$$\sum_{(a)} (-1)^i \delta + \sum_{(b)} (-1)^i \delta = \sum_{(c)} (-1)^{h+\Delta} (\Delta' - \Delta) + T.$$

From this and (A) it follows that

$$\sum_{(a)} (-1)^i \frac{3\delta + 1}{2} + \sum_{(b)} (-1)^i \frac{3\delta - 1}{2} \\ = \frac{3}{2} \sum_{(c)} (-1)^{h+\Delta} (\Delta' - \Delta) + V, \quad (B)$$

where

$$V = 0 \text{ if } n \text{ is not a pentagonal number,} \\ V = (-1)^{s-1} \frac{3s^2 + s}{2} \quad \text{if} \quad n = \frac{3s^2 + s}{2}, \quad s \geq 0.$$

Since δ is odd, we can set $\delta = 2k - 1$ in (a) and $\delta = 2k + 1$ in (b); then (a) and (b) can be written thus:

$$(a) \quad n = \frac{3i^2 + i}{2} + (3k - 1)d,$$

$$(b) \quad n = \frac{3i^2 - i}{2} + (3k + 1)d,$$

or, changing i into $-i$,

$$(b) \quad n = \frac{3i^2 + i}{2} + (3k + 1)d.$$

Denote now by $\sigma_0(m)$, $\sigma_1(m)$, $\sigma_2(m)$ sums of the divisors of m which are $\equiv 0, 1, -1 \pmod{3}$, respectively; then

$$\sum_{(a)} (-1)^i \frac{3\delta + 1}{2} = \sum (-1)^i \sigma_2 \left(n - \frac{3i^2 + i}{2} \right),$$

$$\sum_{(b)} (-1)^i \frac{3\delta - 1}{2} = \sum (-1)^i \sigma_1 \left(n - \frac{3i^2 + i}{2} \right),$$

where the summations on the right extend over all positive, 0, and negative values of i for which

$$\frac{3i^2 + i}{2} < n.$$

It remains now to transform the sum

$$\frac{3}{2} \sum_{(c)} (-1)^{h+\Delta} (\Delta' - \Delta).$$

In the equation

$$n = \frac{3h^2 + h}{2} + \frac{3}{2} \Delta \Delta'$$

$\Delta \Delta'$ is an even number $= 2^{\alpha+1} M$. Taking the sum

$$\Sigma(-1)^{\Delta}(\Delta' - \Delta)$$

for h fixed, we find easily that its value is

$$-2(2^{\alpha+1} - 1)\sigma(M),$$

and consequently

$$\frac{2}{3}\Sigma(-1)^{\Delta}(\Delta' - \Delta)$$

is the sum, taken negatively, of all the divisors of $n - \frac{3h^2 + h}{2}$ which are divisible by 3. Hence

$$\frac{2}{3}\sum_{(c)}(-1)^{\Delta+\Delta}(\Delta' - \Delta) = -\sum\sigma_0\left(n - \frac{3h^2 + h}{2}\right),$$

where the summation extends over all integers h for which

$$\frac{3h^2 + h}{2} \leq n$$

Transferring the first term in the right-hand side of (B), changing h into i , and noticing that

$$\sigma_0(m) + \sigma_1(m) + \sigma_2(m) = \sigma(m),$$

we get

$$\sum(-1)^i\sigma\left(n - \frac{3i^2 + i}{2}\right) = 0 \text{ if } n \text{ is not a pentagonal number,}$$

$$\sum(-1)^i\sigma\left(n - \frac{3i^2 + i}{2}\right) = (-1)^s \frac{3s^2 + s}{2}$$

if

$$n = \frac{3s^2 + s}{2}, \quad s \geq 0,$$

and this is Euler's recurrence formula.

Equation (A) has also a simple arithmetical meaning. Denote by $\omega(m)$ the difference between the number of divisors of m of the form $3k + 1$ and the number of divisors of the form $3k - 1$. Then (A) is clearly equivalent to the recurrence formula

$$\sum (-1)^i \omega\left(n - \frac{3i^2 + i}{2}\right) = 0 \text{ if } n \text{ is not a pentagonal number,}$$

$$\sum (-1)^i \omega\left(n - \frac{3i^2 + i}{2}\right) = (-1)^s s$$

if

$$n = \frac{3s^2 + s}{2}, \quad s \geq 0.$$

Let us take, for example, $n = 10$; then since 10 is not a pentagonal number we must have

$$\omega(10) - \omega(9) + \omega(8) - \omega(5) + \omega(3) - \omega(1) = 0,$$

and indeed

$$\begin{aligned} \omega(10) = 0, \quad \omega(9) = 1, \quad \omega(8) = 0, \quad \omega(5) = 0, \\ \omega(3) = 1; \\ 0 - 1 + 0 + 0 + 1 = 0. \end{aligned}$$

Again, for $n = 12$

$$\begin{aligned} \omega(12) = 1, \quad \omega(11) = 0, \quad \omega(10) = 0, \quad \omega(7) = 2, \\ \omega(5) = 0 \end{aligned}$$

and

$$\begin{aligned} \omega(12) - \omega(11) - \omega(10) + \omega(7) + \omega(5) \\ = 1 - 0 - 0 + 2 + 0 = 3, \end{aligned}$$

as it should be, since

$$12 = \frac{3 \cdot (-3)^2 + (-3)}{2}.$$

6. **Specialization of the Fundamental Identities.** We take now $\lambda = 1, \alpha = 0$. Then the second fundamental identity degenerates into an insignificant and trivial equality, while the first becomes

$$2 \sum_{(a)} F(\delta - 2i, d + i, 2d + 2i - \delta) = \sum_{(b)} F(\Delta + \Delta', h, \Delta - \Delta') + 2T - U, \quad (A)$$

where the summations now indicated by (a) and (b) refer to the partitions

$$(a) \quad n = i^2 + d\delta$$

$$(b) \quad n = h^2 + \Delta\Delta',$$

and both T and U are = 0 unless $n = s^2 (s > 0)$, in which case

$$T = \sum_{j=1}^{2s-1} (2s-j, s, 2s-j),$$

$$U = \sum_{j=1}^{2s-1} (2s, j-s, 2j-2s),$$

The identity (A), though only a special case of the first fundamental identity, is still very important and will serve as a basis of all the subsequent deductions. We shall assume that

$$F(x, y, z) = 0 \text{ when } x \text{ or } z \text{ is even,}$$

$$F(x, y, z) = (-1)^{\frac{x+z}{2}+y} f(y) \text{ when } x \text{ and } z \text{ are odd,}$$

where $f(y)$ is an arbitrary odd function of y . With this definition we have

$$F(-x, y, z) = -F(x, y, z), \quad F(x, -y, -z) = F(x, y, z), \\ F(0, y, z) = 0,$$

as it should be. Considering that $F(x, y, z)$ is now an odd function of y , it is easy to see that

$$\sum_{(b)} F(\Delta + \Delta', h, \Delta - \Delta') = 0.$$

For h and $-h$ run through the same set of values, and so

$$\begin{aligned} \sum_{(b)} F(\Delta + \Delta', h, \Delta - \Delta') &= \sum_{(b)} F(\Delta + \Delta', -h, \Delta - \Delta') \\ &= -\sum_{(b)} F(\Delta + \Delta', h, \Delta - \Delta'), \end{aligned}$$

whence the statement follows. Moreover $U = 0$, and $T = 0$ unless n is a square $= s^2$, in which case

$$T = (-1)^{s-1} s f(s).$$

Thus

$$\sum_{(c)} (-1)^i f(d+i) = \{(-1)^{s-1} s f(s)\}, \quad (B)$$

where the summation refers to the partitions

$$(c) \quad n = i^2 + d\delta, \quad \delta \text{ odd},$$

and the symbol $\{(-1)^{s-1} s f(s)\}$, as in other formulas, stands for 0 in case n is not a square, and for the quantity

$$(-1)^{s-1} s f(s)$$

if $n = s^2$, $s > 0$. It must be remembered that $f(x)$ is an arbitrary odd function of x .

Suppose now that

$$F(x, y, z) = 0 \text{ when } x \text{ or } y \text{ is odd,}$$

and let n be an odd number. Then it suffices to take into consideration only those partitions (a) in which δ is even, i odd, and consequently d odd also, and only those partitions (b) in which h is even. When we replace δ by 2δ and h by $2h$, the summations in (A) will refer to the partitions

$$(e) \quad n = i^2 + 2d\delta, \quad d \text{ odd}$$

$$(f) \quad n = 4h^2 + \Delta\Delta'.$$

For even values of x and y the function $F(x, y, z)$ may be defined in any way whatsoever, observing only the usual conditions of parity. Denoting by $f(t)$ an arbitrary odd function of an integer t , we shall take one time

$$F(x, y, z) = f\left(\frac{x}{2}\right) \text{ for } x, y \text{ even,}$$

and another time

$$F(x, y, z) = (-1)^{\frac{y}{2}} f\left(\frac{x}{2}\right) \text{ for } x, y, \text{ even.}$$

This will lead to the identities

$$\sum_{(f)} f\left(\frac{\Delta + \Delta'}{2}\right) = 2 \sum_{(e)} f(\delta + i) + \{sf(s)\} \quad (C)$$

and

$$\sum_{(f)} (-1)^h f\left(\frac{\Delta + \Delta'}{2}\right) = 2 \sum_{(e)} (-1)^{\frac{\delta+i-1}{2}} f(\delta + i) + \{(-1)^{\frac{s-1}{2}} f(s)\}. \quad (D)$$

Finally, we need one more particular identity derived from (A). This time we set

$$F(x, y, z) = 0 \text{ when } x \text{ is odd or } y \text{ even,}$$

and suppose that n is an odd number $\equiv 1 \pmod{4}$. Then it suffices to consider only those partitions (a) in which δ is even, i odd, and d even, and those partitions (b) in which h is odd while Δ and Δ' are both even. When we replace correspondingly δ and d by 2δ and $2d$, and also Δ and Δ' by 2Δ and $2\Delta'$, the summations will refer to the partitions

$$\begin{aligned} (g) \quad n &= i^2 + 4d\delta \\ (k) \quad n &= h^2 + 4\Delta\Delta'. \end{aligned}$$

For even values of x and odd values of y the function $F(x, y, z)$ must satisfy only the conditions of parity. We may take

$$F(x, y, z) = f\left(\frac{x}{2}\right) \text{ for } x \text{ even, } y \text{ odd,}$$

the function $f(t)$ being odd. The resulting particular identity will be

$$2 \sum_{(g)} f(\delta + i) = \sum_{(k)} f(\Delta + \Delta') + \left\{ 2 \sum_{k=1}^{s-1} f(k) - (s-1)f(s) \right\} \quad (E)$$

7. An Application. The identities found in the preceding section, and many others of a similar nature, derived from the proper choice of the arbitrary functions, furnish a great many arithmetical results of interest. Here we shall consider only one application. We shall take in the identity (B), Sec. 6,

$$\sum_{(c)} (-1)^i i = 0.$$

Clearly,

$$\sum_{(c)} (-1)^i i = 0.$$

As to

$$\sum_{(c)} (-1)^i d$$

it can be evaluated by collecting first the terms corresponding to the same i . Let $T(M)$ denote the sum of the divisors of M whose conjugate divisors are odd; in other words, if $M = 2^\alpha m$, m odd, then

$$T(M) = 2^\alpha \sigma(m).$$

With this notation the result of the summation for a fixed i can be represented by

$$(-1)^i T(n - i^2).$$

Letting i take all integral values satisfying the inequality $i^2 < n$, the sum

$$\sum_{(c)} (-1)^i d$$

will be

$$T(n) - 2T(n - 1^2) + 2T(n - 2^2) - \dots$$

On the other hand, the right-hand side of (B) is

$$\{(-1)^{n-1}n\};$$

that is, 0 if n is not a square, and

$$(-1)^{n-1}n$$

if n is a square.

Thus we get a recurrence formula

$$T(n) - 2T(n - 1^2) + 2T(n - 2^2) - \dots = \{(-1)^{n-1}n\}, \quad (A)$$

which can serve to tabulate the functions $T(n)$ and $\sigma(n)$. But there is another interesting application of this formula. Let n be a prime $\equiv 1 \pmod{4}$; then

$$T(n) = n + 1, \quad \{(-1)^{n-1}n\} = 0$$

and

$$T(n - 1^2) - T(n - 2^2) + T(n - 3^2) - \dots = \frac{n + 1}{2}.$$

Now $\frac{1}{2}(n + 1)$ is odd; therefore among the terms of this sum there is at least one odd term. Clearly, $T(m)$ can be odd only if m is odd. Moreover $T(m)$ coincides with the sum of the divisors of m , if m is odd, and the sum of the divisors is odd if

and only if m is a square. Consequently, for some positive value of b we have $n - 4b^2$ an odd square a^2 , so that

$$n = a^2 + 4b^2$$

if n is a prime of the form $4k + 1$.

Thus we have another and extremely simple proof of this famous theorem. Moreover, we know that with positive a and b this representation is unique, a fact capable of direct proof in a very simple manner. Suppose that

$$n = a^2 + 4b^2 = a'^2 + 4b'^2,$$

where a' differs from a . Let $a' > a$, $b' < b$, and

$$a' = a + 2x, \quad 2b' = 2b - 2y.$$

On substituting and simplifying, we get

$$x(x + a) = y(2b - y).$$

Let the fraction x/y expressed in its simplest terms be t/u ; then

$$\begin{aligned} x &= rt, & y &= ru \\ x + a &= su, & 2b - y &= st, \end{aligned}$$

whence

$$a = su - rt, \quad 2b = ru + st$$

and

$$n = (su - rt)^2 + (ru + st)^2 = (r^2 + s^2)(t^2 + u^2).$$

Now r, s as well as t, u are positive integers, so that

$$r^2 + s^2 > 1, \quad t^2 + u^2 > 1,$$

but this contradicts the supposition that n is a prime number.

Replacing n by $n - i^2$ in the recurrence formula (A), we get

$$T(n - i^2) = 2 \sum (-1)^{i-1} T(n - i^2 - j^2) + (-1)^{n-i^2-1} \{n - i^2\};$$

$$j = 1, 2, 3, \dots,$$

and this expression being substituted back into (A), the result can be presented thus:

$$T(n) = 4 \sum (-1)^{i+j} T(n - i^2 - j^2) + (-1)^{n-1} \{n\} + 2(-1)^n \sum \{n - i^2\},$$

where the double summation extends over all positive integers i, j such that $i^2 + j^2 < n$, and the simple summation extends over the positive integers i such that $i^2 < n$. To each term of the double sum in which $i \neq j$ there corresponds an equal term obtained by interchanging i and j . Therefore, the sum of all terms in which $i \neq j$ is an even number and dropping multiples of 8 we get the congruence

$$T(n) \equiv 4 \sum T(n - 2i^2) + (-1)^{n-1} \{n\} + 2(-1)^n \sum \{n - i^2\} \pmod{8}.$$

Let now n be a prime number of the form $8k + 3$. Since such numbers cannot be the sums of two squares, we have

$$\{n - i^2\} = 0$$

for $i = 1, 2, 3, \dots$. Also $\{n\} = 0$ and $T(n) = 8k + 4$, so that

$$\sum T(n - 2i^2) \equiv 1 \pmod{2}.$$

This shows that $T(n - 2i^2)$ is odd for some i ; that is, $n - 2i^2$ is a square of an odd number j . In other words,

$$n = j^2 + 2i^2.$$

Let n now be a prime of the form $8k + 1$. Then $\{n\} = 0$ but in the sum

$$\sum \{n - i^2\}$$

there are exactly two terms different from 0. In fact, the prime n , by what has been proved before, can be represented in the form

$$n = k^2 + l^2$$

in one and only one way if k and l are positive and, besides, l is even. It is clear, then, that the sum

$$\Sigma\{n - i^2\}$$

reduces to two terms

$$\{n - k^2\} + \{n - l^2\} = k^2 + l^2 \equiv 1 \pmod{8},$$

so that

$$2(-1)^n \Sigma\{n - i^2\} \equiv -2 \pmod{8}.$$

Since $T(n) = 8k + 2$, we get again

$$\Sigma T(n - 2i^2) \equiv 1 \pmod{2},$$

whence it follows that for some integer j

$$n - 2i^2 = j^2,$$

or

$$n = j^2 + 2i^2.$$

It is thus proved again that primes of the form $8k + 1$ or $8k + 3$ are sums of a square and the double of a square.

8. Jacobi's Theorem. As another important application we shall give an elementary proof of Jacobi's result concerning the number of representations of integers by the sum of four squares. Admitting for the integers x, y, z, t positive, negative, or 0 values, we shall agree to consider two representations

$$n = x^2 + y^2 + z^2 + t^2; \quad n = x'^2 + y'^2 + z'^2 + t'^2$$

as distinct unless simultaneously

$$x' = x, \quad y' = y, \quad z' = z, \quad t' = t.$$

With this agreement let us denote by $N_4(n)$ the number of all representations of n by the sum of four squares; then Jacobi's theorem states that

$$\begin{aligned} N_4(n) &= 8\sigma(n) \text{ if } n \text{ is odd,} \\ N_4(n) &= 24\sigma(m) \text{ if } n \text{ is even} = 2^a m, m \text{ odd.} \end{aligned}$$

Thus, for instance, from one representation of $n = 3$:

$$\begin{aligned} 3 &= 1^2 + 1^2 + 1^2 + 0^2; \\ x &= 1, \quad y = 1, \quad z = 1, \quad t = 0 \end{aligned}$$

by changing the signs of x, y, z , and by permutations we find $8 \cdot 4 = 32$ different representations and $32 = 8\sigma(3)$. Again, from one representation of $n = 2$:

$$\begin{aligned} 2 &= 1^2 + 1^2 + 0^2 + 0^2; \\ x &= 1, \quad y = 1, \quad z = 0, \quad t = 0 \end{aligned}$$

by changing the signs of x, y , and by permutations we find $4 \cdot 6 = 24$ different representations; as in this case $m = 1$, we have $24\sigma(1) = 24$, in conformity with the theorem.

Various ways are open to prove Jacobi's theorem; one of the simplest is the following. It is easy to establish, by quite elementary considerations, the following relations:

$$\begin{aligned} N_4(2n) &= 3N_4(n) \text{ if } n \text{ is odd,} \\ N_4(2n) &= N_4(n) \text{ if } n \text{ is even.} \end{aligned}$$

Suppose at first that n is even; then in the equation

$$2n = x^2 + y^2 + z^2 + t^2 \quad (a)$$

x, y, z, t are all of the same parity. Correspondingly, the integers

$$\xi = \frac{x+y}{2}, \quad \eta = \frac{x-y}{2}, \quad \zeta = \frac{z+t}{2}, \quad \theta = \frac{z-t}{2}$$

satisfy the equation

$$n = \xi^2 + \eta^2 + \zeta^2 + \theta^2, \quad (b)$$

and, vice versa, from each solution of this equation, by means of the formulas

$$x = \xi + \eta, \quad y = \xi - \eta, \quad z = \zeta + \theta, \quad t = \zeta - \theta$$

a solution of equation (a) is derived. Thus, between the solutions of equations (a) and (b) there exists a one-to-one correspondence which shows that

$$N_4(2n) = N_4(n).$$

Suppose now that n is odd. Then in equation (b) either only one of the numbers ξ, η, ζ, θ is odd, or only one even, according as $n \equiv 1 \pmod{4}$ or $n \equiv 3 \pmod{4}$. Also in equation (a) among x, y, z, t there are two even and two odd numbers. Let us denote by P the number of solutions of (a) in which x, y are even and z, t odd; then, letting the even and odd squares occupy all possible places, out of every one of the P solutions we get six solutions, whence it follows that

$$N_4(2n) = 6P.$$

Again, if Q is the number of solutions of equation (b) such that ξ and η are of the same parity and ζ and θ of different parity, then it is easy to see that

$$N_4(n) = 2Q.$$

But the formulas

$$x = \xi + \eta, \quad y = \xi - \eta, \quad z = \zeta + \theta, \quad t = \zeta - \theta$$

establish a one-to-one correspondence between the solutions of (a) in which x and y are even, and the solutions of (b) in

which ξ and η are of the same parity, so that $P = Q$ and consequently

$$N_4(2n) = 3N_4(n).$$

Consider now the equation

$$n = x^2 + y^2 + z^2 + t^2 + u^2$$

with five unknown integers. It may not have any solutions. But if it has, then in case $n \equiv 3 \pmod{4}$ among the x, y, z, t, u there are three odd and two even numbers. Denote by R the number of solutions in which x is even and by S the number of those in which x is odd. It is easy to see that

$$R = \frac{2}{3}S.$$

But on the other hand R and S are expressed by the sums

$$R = \sum N_4(n - 4h^2); \quad h = 0, \pm 1, \pm 2, \dots,$$

$$S = \sum N_4(n - i^2); \quad i = \pm 1, \pm 3, \pm 5, \dots$$

which are extended over all integers h and odd integers i , rendering the arguments nonnegative. Thus, for $n \equiv 3 \pmod{4}$

$$\sum N_4(n - 4h^2) = \frac{2}{3} \sum N_4(n - i^2), \quad (c)$$

and this holds when, hypothetically, the equation

$$n = x^2 + y^2 + z^2 + t^2 + u^2 \quad (d)$$

has no solution; for then both sums reduce to 0.

If $n \equiv 1 \pmod{4}$, then among the numbers x, y, z, t, u in (d) there are one odd number and four even, or else, but only in case $n \equiv 5 \pmod{8}$, all five are odd. Disregarding solutions in which all five numbers are odd, we see that the number of solutions of equation (d) with an even x is exactly four times the number of solutions with an odd x . This leads, in case $n \equiv 1 \pmod{4}$, to the relation

$$\sum N_4(n - 4h^2) = 4 \sum N_4\left(\frac{n - i^2}{4}\right), \quad (e)$$

where the summations extend over all integers h and all odd integers i , rendering the arguments nonnegative.

By resorting to the identities (C) and (E) in Sec. 6, it is easy to find a priori numerical functions satisfying the relations (c) and (e). In the identity (C)

$$\sum_{(\alpha)} f\left(\frac{\Delta + \Delta'}{2}\right) = 2 \sum_{(\beta)} f(\delta + i) + \{sf(s)\}$$

$(\alpha) \quad n = 4h^2 + \Delta\Delta'$
 $(\beta) \quad n = i^2 + 2d\delta, \quad d \text{ odd}$

we take $f(x) = x$. Then in case $n \equiv 3 \pmod{4}$, d and δ are both odd in (β) , and for i fixed

$$\frac{\Delta + \Delta'}{2}$$

is just one-third of the sum of the divisors of $n - i^2$, while for h fixed

$$\sum \frac{\Delta + \Delta'}{2}$$

is the sum of the divisors of $n - 4h^2$. Consequently, for $n \equiv 3 \pmod{4}$, we have

$$\Sigma\sigma(n - 4h^2) = \frac{2}{3}\Sigma\sigma(n - i^2).$$

In case $n \equiv 5 \pmod{8}$, δ is the double of an odd number, and for i fixed

$$\Sigma\delta$$

is double the sum of the divisors of

$$\frac{n - i^2}{4},$$

so that for $n \equiv 5 \pmod{8}$

$$\sum_{\sigma} \sigma(n - 4h^2) = 4 \sum_{\sigma} \sigma\left(\frac{n - i^2}{4}\right).$$

Finally, in case $n \equiv 1 \pmod{8}$, δ is divisible by 4; replacing therefore δ by 4δ , we shall have

$$\sum_{(\gamma)} \sigma(n - 4h^2) = 4 \sum_{(\gamma)} 2\delta + \{n\}, \quad (f)$$

where the sign (γ) indicates the partitions

$$(\gamma) \quad n = i^2 + 8d\delta, \quad d \text{ odd.}$$

This relation we combine with one following from the identity (E):

$$\sum_{(k)} f(\Delta' + \Delta') = 2 \sum_{(h)} f(\delta + i) + \left\{ (s-1)f(s) - 2 \sum_{k=1}^{s-1} f(k) \right\}$$

$(k) \quad n = h^2 + 4\Delta\Delta'$
 $(h) \quad n = i^2 + 4d\delta$

by taking in it

$$f(x) = (-1)^x x.$$

Considering that the partitions (k) and (h) are identical except for notation, the result can be presented thus:

$$\sum_{(k)} [(-1)^{d+\delta}(d + \delta) + 2(-1)^d \delta] = \{-n + 1\},$$

or

$$2 \sum_{(k)} (-1)^d \delta [(-1)^d + 1] = \{-n + 1\}.$$

Terms corresponding to odd values of d vanish; therefore when we change d into $2d$, the final result will be

$$4 \sum_{(\epsilon)} (-1)^\delta \delta = \{-n + 1\}, \quad (g)$$

where the summation refers to the partitions

$$(\epsilon) \quad n = i^2 + 8d\delta.$$

The relation (f) can also be written thus:

$$\sum \sigma(n - 4h^2) = 4 \sum_{(\epsilon)} [1 - (-1)^\alpha] \delta + \{n\},$$

which combined with (g) gives

$$\sum \sigma(n - 4h^2) = 4 \sum_{(\epsilon)} [1 - (-1)^\alpha - (-1)^\delta] \delta + \{1\}.$$

Now the sum

$$\sum [1 - (-1)^\alpha - (-1)^\delta] \delta$$

for a fixed i equals three times the sum of the odd divisors of $(n - i^2)/8$ or, what is the same, of $(n - i^2)/4$, as can be easily verified. Denoting, therefore, by $\bar{\sigma}(m)$ the sum of the odd divisors of m , we can present the preceding relation thus:

$$\sum \sigma(n - 4h^2) = 12 \sum \bar{\sigma}\left(\frac{n - i^2}{4}\right) + \{1\}.$$

In the right-hand side the summation extends over all odd integers such that $i^2 < n$.

The three formulas found for $n \equiv 3 \pmod{4}$, $n \equiv 5 \pmod{8}$, and $n \equiv 1 \pmod{8}$ can be replaced by two by introducing the function

$$\chi(n) = (2 + (-1)^n) \bar{\sigma}(n), \quad \chi(0) = \frac{1}{8}.$$

The formula corresponding to $n \equiv 3 \pmod{4}$ will be

$$\sum \chi(n - 4h^2) = \frac{2}{3} \sum \chi(n - i^2), \quad (c')$$

and the one for $n \equiv 1 \pmod{4}$ will be

$$\sum x(n - 4h^2) = 4 \sum x\left(\frac{n - i^2}{4}\right). \quad (e')$$

It must be noticed that the summation in the right-hand side of (e') refers to all odd values of i for which the argument is nonnegative. Setting

$$N_4(n) - 8\chi(n) = \omega(n)$$

and comparing (c) and (e'), (e) and (e'), we have

$$\sum \omega(n - 4h^2) = \frac{2}{3} \sum \omega(n - i^2), \quad n \equiv 3 \pmod{4} \quad (A)$$

$$\sum \omega(n - 4h^2) = 4 \sum \omega\left(\frac{n - i^2}{4}\right), \quad n \equiv 1 \pmod{4}. \quad (B)$$

The proof of Jacobi's theorem is now almost immediate. In the first place

$$N_4(0) = 1, \quad 8\chi(0) = 1, \quad \omega(0) = 0.$$

Suppose that for $m = 0, 1, 2, \dots, n - 1$ it happens that $\omega(m) = 0$. Then we can prove that $\omega(n) = 0$ in the following manner. Let n and $\frac{1}{2}n$ be even; then

$$N_4(n) = N_4\left(\frac{1}{2}n\right), \quad \chi(n) = \chi\left(\frac{1}{2}n\right),$$

and

$$\omega(n) = \omega\left(\frac{1}{2}n\right) = 0,$$

since by hypothesis $\omega\left(\frac{1}{2}n\right) = 0$. Let $\frac{1}{2}n$ be odd; then

$$N_4(n) = 3N_4\left(\frac{1}{2}n\right), \quad \chi(n) = 3\chi\left(\frac{1}{2}n\right)$$

and

$$\omega(n) = 3\omega\left(\frac{1}{2}n\right) = 0.$$

If n is an odd number $\equiv 3 \pmod{4}$, then it follows from (A) that $\omega(n) = 0$, and if $n \equiv 1 \pmod{4}$ the same conclusion follows from (B). Now $\omega(0) = 0$, and then necessarily $\omega(1) = 0$, $\omega(2) = 0$, . . . ; that is, for every positive integer n

$$\omega(n) = 0$$

or

$$N_4(n) = 8\chi(n) = 8(2 + (-1)^n)\bar{\sigma}(n),$$

which is Jacobi's theorem.

In particular, if $n = 4m$ and m is odd, the number of all representations

$$4m = x^2 + y^2 + z^2 + t^2$$

is $24\sigma(m)$. But x, y, z, t are either all even or all odd. The number of representations with even x, y, z, t is the same as the number of representations of m , that is, $8\sigma(m)$. Consequently, there are $16\sigma(m)$ representations of $4m$ by the sum of four odd squares; if the roots of these squares are taken positively, the number of representations reduces to $\sigma(m)$. In other words, the number of representations of $4m$ by the sum of squares of four positive odd numbers is the same as the sum of divisors of m .

9. Additional Identities. When we come to the problem of the representation of integers by sums of three squares, we shall need identities of a character quite different from those in Sec. 6. Yet remarkably enough they can be derived from them in a simple and elegant manner. Our starting point will be the identity (B) in Sec. 6, which we shall present here in the form

$$\sum_{(c)} (-1)^i \phi(d' + i) = \{(-1)^{s-1} s \phi(s)\}, \quad (B)$$

denoting by (c) the partitions

$$(c) \quad n = i^2 + d'\delta', \quad \delta' \text{ odd,}$$

and by $\phi(x)$ an arbitrary odd function of x . Let d'' , δ'' be two positive integers satisfying the inequality

$$d''\delta'' < n$$

with δ'' odd. The function $f(x)$ being even,

$$\phi(x) = f(x - d'') - f(x + d'')$$

will be odd. Replacing n by $n - d''\delta''$ and choosing $\phi(x)$ as indicated, we shall have

$$\sum_{(c)} (-1)^i [f(d' - d'' + i) - f(d' + d'' + i)] \\ = \{(-1)^{s-1} s [f(s - d'') - f(s + d'')]\},$$

where the summation indicated by (c) refers to the partitions

$$(c) \quad n - d''\delta'' = i^2 + d''\delta', \quad \delta' \text{ odd,}$$

and the right-hand side is 0 unless

$$n - d''\delta'' = s^2, \quad s > 0,$$

in which case it is

$$(-1)^{s-1} s [f(s - d'') - f(s + d'')].$$

Letting d'' , δ'' run through all the values subject to the conditions

$$d''\delta'' < n, \quad \delta'' \text{ odd,}$$

and taking the sum of all the identities referring to each system d'' , δ'' , as a result we get

$$\sum_{(d)} (-1)^i [f(d' - d'' + i) - f(d' + d'' + i)] \\ = \sum_{(e)} (-1)^i f(i + d), \quad (P)$$

where the summations indicated by (d) and (e) refer to the partitions

$$(d) \quad n = i^2 + d'\delta' + d''\delta''; \quad \delta', \delta'' \text{ odd}$$

$$(e) \quad n = i^2 + d\delta, \quad \delta \text{ odd.}$$

The right-hand side of (P) can be transformed, by using the fundamental identity (A) of Sec. 6, in the following manner. Let

$$F(x, y, z) = 0 \text{ if } x \text{ or } z \text{ is even}$$

and otherwise either

$$F(x, y, z) = (-1)^{\frac{x-1}{2} + \frac{2y-z-1}{2}} (2y-z)f(y)$$

or

$$F(x, y, z) = (-1)^{\frac{x-1}{2} + \frac{2y-z-1}{2}} yf(y).$$

Then we get two identities

$$2 \sum_{(e)} (-1)^i \delta f(d+i) = \sum_{(f)} (-1)^{\Delta'-1+h} (2h + \Delta' - \Delta) f(h) + 2\{(-1)^{s-1} s^2 f(s)\}$$

$$2 \sum_{(e)} (-1)^i (d+i) f(d+i) = \sum_{(f)} (-1)^{\Delta'-1+h} h f(h) + 2\{(-1)^{s-1} s^2 f(s)\},$$

where the summations refer to the partitions

$$(e) \quad n = i^2 + d\delta, \quad \delta \text{ odd}$$

$$(f) \quad n = h^2 + \Delta\Delta', \quad \Delta + \Delta' \text{ odd.}$$

Since evidently

$$\sum_{(f)} (-1)^{\Delta'-1+h} h f(h) = 0$$

$$\sum_{(f)} (-1)^{\Delta'-1+h} (2h + \Delta' - \Delta) f(h) = -2 \sum_{(e)} (-1)^i (d - \delta) f(i),$$

by eliminating the terms in the braces we get

$$\sum_{(e)} (-1)^i i f(d + i) = \sum_{(e)} (-1)^i (\delta - d) f(d + i) + \sum_{(e)} (-1)^i (d - \delta) f(i),$$

and now (P) can be written as follows:

$$\begin{aligned} \sum_{(d)} (-1)^i [f(d' - d'' + i) - f(d' + d'' + i)] \\ = \sum_{(e)} (-1)^i [(\delta - d) f(d + i) + (d - \delta) f(i)]. \quad (Q) \end{aligned}$$

Let

$$\psi_i(x) = f(x + i) + f(x - i).$$

This function, for a given i , is even with regard to x . Denote by $\omega_i(n)$ the difference

$$\begin{aligned} \omega_i(n) = \sum_{(a)} [\psi_i(d' - d'') - \psi_i(d' + d'')] \\ - \sum_{(h)} (\delta - d) [\psi_i(d) - \psi_i(0)], \end{aligned}$$

where the summations are extended over the partitions

$$(g) \quad n = d' \delta' + d'' \delta''; \quad \delta', \delta'' \text{ odd}$$

$$(h) \quad n = d \delta, \quad \delta \text{ odd.}$$

Then (Q) is equivalent to

$$\omega_0(n) + 2 \sum (-1)^i \omega_i(n - i^2) = 0,$$

and in the summation i runs through positive integers such that $i^2 < n$. Since this identity holds for any $n \geq 1$, it implies necessarily that

$$\omega_0(n) = 0.$$

This amounts to the remarkable identity

$$\sum_{(g)} [f(d' - d'') - f(d' + d'')] = \sum_{(h)} (\delta - d)[f(d) - f(0)], \quad (R)$$

holding for any even function $f(x)$.

Suppose now that n is an even number $= 2m$, and that $f(x) = 0$ whenever x is odd. Then, in the partitions (g),

$$(g) \quad 2m = d'\delta' + d''\delta''; \quad \delta', \delta'' \text{ odd,}$$

either d', d'' are both odd or both are even; similarly in (h)

$$(h) \quad 2m = d\delta, \quad \delta \text{ odd,}$$

d must be even. If d is replaced by $2d$, the partitions (h) will be replaced by

$$(k) \quad m = d\delta, \quad \delta \text{ odd.}$$

If d', d'' are even, we can replace them by $2d', 2d''$; the corresponding part of the sum in the left side of (R) will be

$$\sum [f(2d' - 2d'') - f(2d' + 2d'')]$$

extended over the partitions

$$m = d'\delta' + d''\delta''; \quad \delta', \delta'' \text{ odd.}$$

But by the formula (R) itself, in which $f(x)$ is replaced by $f(2x)$, we have

$$\sum [f(2d' - 2d'') - f(2d' + 2d'')] = \sum_{(k)} (\delta - d)[f(2d) - f(0)],$$

and subtracting this member by member from (R), we get a new identity

$$\sum_{(g)} [f(d' - d'') - f(d' + d'')] = \sum_{(k)} d[f(0) - f(2d)], \quad (S)$$

where the sign (l) indicates the partitions

$$(l) \quad 2m = d'\delta' + d''\delta''; \quad d', \delta'; \quad d'', \delta'' \text{ odd.}$$

Another formula similar to (S) can be derived as follows. Let $F(x)$ be an odd function and let two positive integers d'', δ'' of which δ'' is odd satisfy the inequality

$$d''\delta'' < n.$$

Take in (B) $n - d''\delta''$ instead of n and set

$$\phi(x) = F(x - d'') + F(x + d''),$$

which for a given d'' is an odd function of x . Multiply each of the resulting equations by

$$(-1)^{\frac{\delta''-1}{2}}$$

and sum varying d'', δ'' in all possible ways. As a result we get the following formula

$$\begin{aligned} \sum_{(d)} (-1)^{i+\frac{\delta''-1}{2}} [F(d' - d'' + i) + F(d' + d'' + i)] \\ = - \sum_{(e)} (-1)^{i+\frac{\delta''-1}{2}} iF(i + d), \quad (T) \end{aligned}$$

where the summations refer to the partitions (d) and (e) as before. The right-hand member can be transformed by means of the identity (A) in Sec. 6. To this end, take

$$F(x, y, z) = 0 \text{ if } x \text{ or } z \text{ is even;}$$

otherwise

$$F(x, y, z) = (-1)^{\frac{z-1}{2}} zF(y).$$

After some evident simplifications we shall have

$$\sum_{(e)} (-1)^{i+\frac{\delta-1}{2}} (2d - \delta + 2i) F(i + d) = \{(-1)^{s-1} s F(s)\}.$$

On the other hand,

$$\sum_{(e)} (-1)^i F(i + d) = \{(-1)^{s-1} s F(s)\},$$

and so

$$\begin{aligned} \sum_{(e)} (-1)^{i-1+\frac{\delta-1}{2}} i F(i + d) &= \sum_{(e)} (d - \frac{1}{2}\delta) (-1)^{i+\frac{\delta-1}{2}} F(i + d) \\ &\quad - \frac{1}{2} \sum_{(e)} (-1)^i F(i + d), \end{aligned}$$

whereby (T) becomes

$$\begin{aligned} \sum_{(d)} (-1)^i [F(d' - d'' + i) + F(d' + d'' + i)] (-1)^{\frac{\delta''-1}{2}} \\ = \sum_{(e)} (-1)^i \left[(-1)^{\frac{\delta-1}{2}} d - \frac{1 + (-1)^{\frac{\delta-1}{2}} \delta}{2} \right] F(i + d). \quad (U) \end{aligned}$$

In the same way as we passed from (Q) to (R) we pass from (U) to

$$\begin{aligned} \sum_{(g)} (-1)^{\frac{\delta''-1}{2}} [F(d' - d'') + F(d' + d'')] = \\ \sum_{(h)} (-1)^{\frac{\delta-1}{2}} d F(d) - \sum_{(h)} \frac{1 + (-1)^{\frac{\delta-1}{2}} \delta}{2} F(d), \quad (V) \end{aligned}$$

the extent of the summations indicated by (g) and (h) being the same as in (R). Finally, as we passed from (R) to (S),

we pass from (V) to

$$\sum_{(l)} (-1)^{\frac{\delta''-1}{2}} [F(d' - d'') + F(d' + d'')] = \sum_{(k)} (-1)^{\frac{\delta-1}{2}} dF(2d), \quad (W)$$

the extent of the summations indicated by (l) and (k) being the same as in (S).

10. Representations by the Sums of Three Squares. We turn now to the identities (C) and (D) in Sec. 6. Supposing $n \equiv 3 \pmod{4}$, they can be presented as follows:

$$\sum_{(a)} F\left(\frac{d + \delta}{2}\right) = 2 \sum_{(b)} F(d' + i) \quad (C)$$

$$\sum_{(a)} (-1)^{\lambda} F\left(\frac{d + \delta}{2}\right) = 2 \sum_{(b)} (-1)^{\lambda} F(d' + i). \quad (D)$$

Here $F(x)$ is an arbitrary odd function, and the summation refers to the partitions

$$(a) \quad n = 4h^2 + d\delta$$

$$(b) \quad n = i^2 + 2d'\delta'.$$

Replace n by

$$4n + 1 - 2d''\delta'',$$

where d'' , δ'' are both odd and

$$2d''\delta'' < 4n + 1.$$

Denoting by $f(x)$ an even function, take also

$$F(x) = f(x - d'') - f(x + d'').$$

The results will be

$$\sum_{(a)} \left[f\left(\frac{d+\delta}{2} - d''\right) - f\left(\frac{d+\delta}{2} + d''\right) \right]$$

$$= 2 \sum_{(b)} [f(d' + i - d'') - f(d' + i + d'')]$$

$$\sum_{(a)} (-1)^h \left[f\left(\frac{d+\delta}{2} - d''\right) - f\left(\frac{d+\delta}{2} + d''\right) \right]$$

$$= 2 \sum_{(b)} (-1)^{\frac{i-1}{2} + \frac{\delta'-1}{2}} [f(d' + i - d'') - f(d' + i + d'')],$$

where

$$(a) \quad 4n + 1 - 2d''\delta'' = 4h^2 + d\delta$$

$$(b) \quad 4n + 1 - 2d''\delta'' = i^2 + 2d'\delta'.$$

Take the sum of all such equations varying in all possible ways d'' , δ'' ; the result of the summation clearly can be written thus:

$$\sum_{(c)} \left[f\left(\frac{d+\delta}{2} - d''\right) - f\left(\frac{d+\delta}{2} + d''\right) \right]$$

$$= 2 \sum_{(d)} [f(d' + i - d'') - f(d' + i + d'')]$$

$$\sum_{(c)} (-1)^h \left[f\left(\frac{d+\delta}{2} - d''\right) - f\left(\frac{d+\delta}{2} + d''\right) \right]$$

$$= 2 \sum_{(d)} (-1)^{\frac{i-1}{2} + \frac{\delta'-1}{2}} [f(d' + i - d'') - f(d' + i + d'')],$$

where (c) and (d) indicate the partitions

$$(c) \quad 4n + 1 = 4h^2 + d\delta + 2d''\delta''; \quad d'', \delta'' \text{ odd}$$

$$(d) \quad 4n + 1 = i^2 + 2d'\delta' + 2d''\delta''; \quad d', \delta', d'', \delta'' \text{ odd.}$$

Noticing that i and $-i$ run through the same set of numbers, we have

$$2 \sum_{(d)} [f(d' - d'' + i) - f(d' + d'' + i)] \\ = \sum_{(d)} [\psi_i(d' - d'') - \psi_i(d' + d'')],$$

where for a given i

$$\psi_i(x) = f(x + i) + f(x - i)$$

is an even function. Performing the summation for a given i by formula (S) in Sec. 9, we get at once

$$\sum_{(d)} [\psi_i(d' - d'') - \psi_i(d' + d'')] = 2 \sum_{(e)} d [f(i) - f(i - 2d)],$$

where (e) indicates the partitions

$$(e) \quad 4n + 1 = i^2 + 4d\delta, \quad \delta \text{ odd},$$

and at the same time

$$\sum_{(e)} \left[f\left(\frac{d + \delta}{2} - d''\right) - f\left(\frac{d + \delta}{2} + d''\right) \right] \\ = 2 \sum_{(e)} d [f(i) - f(i - 2d)]. \quad (A)$$

In a similar manner we find

$$2 \sum_{(d)} (-1)^{\frac{i-1}{2} + \frac{\delta-1}{2}} [f(d' - d'' + i) - f(d' + d'' + i)] \\ = \sum_{(d)} (-1)^{\frac{i-1}{2} + \frac{\delta-1}{2}} [\phi_i(d' - d'') - \phi_i(d' + d'')],$$

where

$$\phi_i(x) = f(x + i) - f(x - i)$$

for a fixed i is an odd function. Performing the summation for i fixed by formula (W), Sec. 9, we get

$$\sum_{(d)} (-1)^{\frac{i-1}{2} + \frac{\delta-1}{2}} [\phi_i(d' - d'') - \phi_i(d' + d'')] \\ = 2 \sum_{(e)} (-1)^{\frac{i-1}{2} + \frac{\delta-1}{2}} df(i - 2d),$$

and at the same time

$$\sum_{(e)} (-1)^h \left[f\left(\frac{d + \delta}{2} - d''\right) - f\left(\frac{d + \delta}{2} + d''\right) \right] \\ = 2 \sum_{(e)} (-1)^{\frac{i-1}{2} + \frac{\delta-1}{2}} df(i - 2d), \quad (B)$$

sign (e) indicating the same partitions as before.

Formulas (A) and (B) are very remarkable transformations of complicated sums into much simpler ones. For our purpose we shall define $f(x)$ as follows:

$$f(x) = 0 \quad \text{if} \quad x^2 > 1 \\ f(+1) = f(-1) = 1.$$

Then among the partitions (c) we retain only those in which

$$d'' = \frac{d + \delta}{2} \pm 1.$$

Correspondingly, if we denote by $T(n)$ the total number of solutions of both equations

$$4n + 1 = d\delta + (d + \delta - 2)\delta'' \\ 4n + 1 = d\delta + (d + \delta + 2)\delta''$$

in positive odd integers d, δ, δ'' such that $d + \delta \equiv 0 \pmod{4}$, the left-hand side of (A) and (B) will be represented by the sums

$$\Sigma T(n - h^2) \quad \text{and} \quad \Sigma (-1)^h T(n - h^2)$$

extended over integers h which make $n - h^2$ positive. As to the right-hand sides of the same equations, we shall evaluate them, for the sake of simplicity, only for $n = 2m, 4m$, where m is an odd number. In the right-hand side of (A) we have first the term

$$2 \sum_{(e)} df(i),$$

which reduces to the sum

$$4 \sum d$$

taken over representations of n in the form

$$n = d\delta, \quad \delta \text{ odd.}$$

Now if $n = 2m$, this sum is equal to

$$8\sigma(m),$$

and for $n = 4m$ it is

$$16\sigma(m).$$

Again we have the term

$$-2 \sum df(i - 2d),$$

but here we must take $i = 2d \pm 1$. From (e) it follows that

$$n = d(d + \delta \pm 1),$$

and both factors are of the same parity. Such representation is impossible if $n = 2m$, so that in this case

$$-2 \sum df(i - 2d) = 0.$$

The same will be true for the sum

$$\sum_{(e)} (-1)^{\frac{\delta-1}{2} + \frac{i-1}{2}} df(i - 2d).$$

Thus for $n = 2m$ we have

$$\sum T(2m - h^2) = 8\sigma(m), \quad \sum (-1)^h T(2m - h^2) = 0,$$

whence

$$T(2m) + 2T(2m - 2^2) + 2T(2m - 4^2) + \dots = 4\sigma(m) \quad (E)$$

$$T(2m - 1^2) + T(2m - 3^2) + T(2m - 5^2) + \dots = 2\sigma(m) \quad (F)$$

In case $n = 4m$, the equation

$$4m = d(d + \delta \pm 1)$$

is possible only if d is even; when we set $d = 2\Delta$, the sum

$$-2\sum df(d - 2i)$$

reduces to

$$-4\sum\Delta,$$

where the summation extends over all representations of m in the form

$$m = \Delta\left(\Delta + \frac{\delta \pm 1}{2}\right).$$

Similarly the sum

$$2\sum_{(e)} (-1)^{\frac{i-1}{2} + \frac{\delta-1}{2}} df(i - 2d)$$

reduces to

$$4\sum (-1)^{\Delta + \frac{\delta \pm 1}{2}} \Delta,$$

or, since

$$\Delta + \frac{\delta \pm 1}{2}$$

is odd, to

$$-4\sum\Delta,$$

with the extent of the summation as before. Taking, therefore, the difference of (A) and (B), we shall have

$$T(4m - 1^2) + T(4m - 3^2) + T(4m - 5^2) + \dots = 4\sigma(m). \quad (G)$$

Equations (E), (F), and (G) will lead very quickly to the fundamental results concerning the representation of numbers by sums of three squares. But first we shall prove that the numerical function $T(n)$, defined as the total number of solutions of both equations

$$\begin{aligned} 4n + 1 &= d\delta + (d + \delta + 2)\delta'' \\ 4n + 1 &= d\delta + (d + \delta + 2)\delta'' \end{aligned}$$

in positive odd numbers such that $d + \delta \equiv 0 \pmod{4}$, has always a positive value. In fact

$$d = 2n + 1, \quad \delta = 1, \quad \delta'' = 1$$

is a solution of the first equation satisfying the condition $d + \delta \equiv 0 \pmod{4}$ if n is odd, while $d = 2n - 1, \delta = 1, \delta'' = 1$ satisfy the second equation and the condition $d + \delta \equiv 0 \pmod{4}$ if n is even.

By Jacobi's theorem 16 $\sigma(m)$ is the number of solutions of the equation

$$4m = i^2 + j^2 + k^2 + l^2$$

in odd numbers. Denote in general by $N_3(n)$ the number of representations of n by the sum of three squares. Since numbers $\equiv 3 \pmod{4}$ may be represented by the sums of three odd squares only we have

$$8\sigma(m) = N_3(4m - 1^2) + N_3(4m - 3^2) + N_3(4m - 5^2) + \dots$$

and, comparing this with (G),

$$2[T(4m - 1^2) + T(4m - 3^2) + \dots] = N_3(4m - 1^2) + N_3(4m - 3^2) + \dots$$

This equation holding for all odd values of m , we must have

$$N_3(4m - 1) = 2T(4m - 1).$$

Now $4m - 1$ represents any number of the form $8N + 3$; consequently

$$N_3(8N + 3) = 2T(8N + 3).$$

It is thus proved that the equation

$$8N + 3 = i^2 + i'^2 + i''^2$$

can be satisfied by positive odd numbers i, i', i'' , and the number of solutions is

$$\frac{1}{4}T(8N + 3).$$

Setting

$$i = 2x + 1, \quad i' = 2y + 1, \quad i'' = 2z + 1,$$

we conclude that

$$N = \frac{x(x+1)}{2} + \frac{y(y+1)}{2} + \frac{z(z+1)}{2};$$

that is, every integer is the sum of three triangular numbers, as Fermat asserted without revealing his proof.

The equation

$$2m = x^2 + y^2 + z^2 + t^2$$

in case $m \equiv 1 \pmod{2}$, by Jacobi's theorem, has exactly $6\sigma(m)$ solutions with positive odd t . Hence

$$6\sigma(m) = N_3(2m - 1^2) + N_3(2m - 3^2) + \dots,$$

and on comparing with (F)

$$3T(2m - 1^2) + 3T(2m - 3^2) + \dots = N_3(2m - 1^2) + N_3(2m - 3^2) + \dots$$

Since this holds for any odd m , we must have

$$N_3(2m - 1) = 3T(2m - 1).$$

But $2m - 1$ represents any number of the form $4N + 1$; consequently

$$N_3(4N + 1) = 3T(4N + 1).$$

This means that every number of the form $4N + 1$ can be represented as the sum of three squares, and the number of representations is

$$3T(4N + 1).$$

By Jacobi's theorem the equation

$$2m = x^2 + y^2 + z^2 + t^2$$

has exactly $12\sigma(m)$ solutions in which x is even, so that

$$12\sigma(m) = N_3(2m) + 2N_3(2m - 2^2) + 2N_3(2m - 4^2) + \dots$$

Comparing this with (E), we have

$$3T(2m) + 6T(2m - 2^2) + \dots = N_3(2m) + 2N_3(2m - 2^2) + \dots,$$

and since this holds for every odd m we must have

$$N_3(2m) = 3T(2m).$$

Thus, twice an odd number can be represented as the sum of three squares, and the number of representations is

$$3T(2m).$$

It remains to consider numbers of the form $8N + 7$ and $4N$. The equation

$$8N + 7 = x^2 + y^2 + z^2$$

can hold only if x, y, z are odd; but then

$$x^2 + y^2 + z^2 \equiv 3 \pmod{8}.$$

Hence numbers of the form $8N + 7$ cannot be represented as the sum of three squares. Again the equation

$$4N = x^2 + y^2 + z^2$$

can hold only if x, y, z are even. It is clear then that this equation has exactly the same number of solutions as the equation

$$N = x^2 + y^2 + z^2.$$

Consequently, all integers except those of the form

$$4^k(8N + 7); \quad k \geq 0$$

can be represented by the sum of three squares. This famous theorem was first proved by Gauss. The proof given in this chapter may be a little long but it is truly elementary. The idea of this proof is due to Kronecker, who was led to it by deep investigations of elliptic functions with complex multiplication.

www.dbraulibrary.org.in

Downloaded from www.dbraulibrary.org.in

TABLE OF PRIMES LESS THAN 5000

2	227	509	829	1171	1823	1879
3	229	521	839	1181	1531	1889
5	233	523	853	1187	1543	1901
7	239	541	857	1193	1649	1907
11	241	547	859	1201	1553	1913
13	251	557	863	1213	1559	1931
17	257	563	877	1217	1567	1933
19	263	569	881	1223	1571	1949
23	269	571	883	1229	1579	1951
29	271	577	887	1231	1583	1973
31	277	587	907	1237	1697	1979
37	281	593	911	1249	1601	1987
41	283	599	919	1259	1607	1993
43	293	601	929	1277	1609	1997
47	307	607	937	1279	1613	1999
53	311	613	941	1283	1619	2003
59	313	617	947	1289	1621	2011
61	317	619	953	1291	1627	2017
67	331	631	967	1297	1637	2027
71	337	641	971	1301	1657	2029
73	347	643	977	1303	1663	2039
79	349	647	983	1307	1667	2053
83	353	653	991	1319	1669	2063
89	359	659	997	1321	1693	2069
97	367	661	1009	1327	1697	2081
101	373	673	1013	1361	1699	2083
103	379	677	1019	1367	1709	2087
107	383	683	1021	1373	1721	2089
109	389	691	1031	1381	1723	2099
113	397	701	1033	1399	1733	2111
127	401	709	1039	1409	1741	2113
131	409	719	1049	1423	1747	2129
137	419	727	1051	1427	1753	2131
139	421	733	1061	1429	1759	2137
149	431	739	1063	1433	1777	2141
151	433	743	1069	1439	1783	2143
157	439	751	1087	1447	1787	2153
163	443	757	1091	1451	1789	2161
167	449	761	1093	1453	1801	2179
173	457	769	1097	1459	1811	2203
179	461	773	1103	1471	1823	2207
181	463	787	1109	1481	1831	2213
191	467	797	1117	1483	1847	2221
193	479	809	1123	1487	1861	2237
197	487	811	1129	1489	1867	2239
199	491	821	1151	1493	1871	2243
211	499	823	1163	1499	1873	2251
223	503	827	1163	1511	1877	2267

TABLE OF PRIMES LESS THAN 5000.—(Continued)

2269	2659	3019	3435	3803	4217	4637
2273	2663	3023	3449	3821	4219	4639
2281	2671	3037	3457	3823	4229	4643
2287	2677	3041	3461	3833	4231	4649
2293	2683	3049	3463	3847	4241	4651
2297	2687	3061	3467	3851	4243	4657
2309	2689	3067	3469	3853	4253	4662
2311	2693	3079	3491	3863	4259	4675
2333	2699	3083	3499	3877	4261	4679
2339	2707	3089	3511	3881	4271	4691
2341	2711	3109	3517	3889	4273	4703
2347	2713	3119	3527	3907	4283	4721
2351	2719	3121	3529	3911	4289	4723
2357	2729	3137	3533	3917	4297	4729
2371	2731	3163	3539	3919	4327	4733
2377	2741	3167	3541	3923	4337	4731
2381	2749	3169	3547	3929	4339	4759
2383	2753	3181	3557	3931	4349	4783
2389	2767	3187	3559	3943	4357	4787
2393	2777	3191	3571	3947	4363	4789
2399	2789	3203	3581	3967	4373	4793
2411	2791	3209	3583	3989	4391	4799
2417	2797	3217	3593	4001	4397	4801
2423	2801	3221	3607	4003	4409	4813
2437	2803	3229	3613	4007	4421	4817
2441	2819	3251	3617	4013	4423	4831
2447	2833	3253	3623	4019	4441	4861
2459	2837	3257	3631	4021	4447	4871
2467	2843	3259	3637	4027	4451	4877
2473	2851	3271	3643	4049	4457	4883
2477	2857	3299	3659	4051	4463	4903
2503	2861	3301	3671	4057	4481	4909
2521	2879	3307	3673	4073	4483	4919
2531	2887	3313	3677	4079	4493	4931
2539	2897	3319	3691	4091	4507	4933
2543	2903	3323	3697	4093	4513	4937
2549	2909	3329	3701	4099	4517	4943
2551	2917	3331	3709	4111	4519	4951
2557	2927	3343	3719	4127	4523	4957
2579	2939	3347	3727	4129	4547	4967
2591	2953	3359	3733	4133	4549	4969
2593	2957	3361	3739	4139	4561	4973
2609	2963	3371	3761	4153	4567	4987
2617	2969	3373	3767	4157	4583	4993
2621	2971	3389	3769	4159	4591	4999
2633	2999	3391	3779	4177	4597	
2647	3001	3407	3793	4201	4603	
2657	3011	3413	3797	4211	4621	

TABLE OF INDICES.—(Continued)

p	Numbers															
	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49
37	8	19	18													
41	19	21	2	32	35	6	20									
43	23	18	14	7	4	33	22	6	21							
47	34	33	30	42	17	31	9	15	24	13	43	41	23			
53	11	9	36	30	38	41	50	45	32	22	8	29	40	44	21	26
59	41	24	44	55	39	37	9	14	11	33	27	48	16	23	54	56
61	48	11	14	39	27	46	25	54	56	43	17	34	58	20	10	35
67	65	38	14	22	11	58	18	53	63	9	61	27	29	50	43	46
71	55	29	64	20	22	65	48	25	33	48	43	10	21	9	50	2
73	29	34	28	64	70	65	25	4	47	51	71	13	54	31	38	66
79	25	37	10	19	36	35	74	75	58	49	76	64	30	59	17	28
83	57	35	64	20	48	67	30	40	81	71	26	7	61	23	76	16
89	22	63	34	11	51	24	30	21	10	29	28	72	73	54	65	74
97	27	32	16	91	19	95	7	85	39	4	58	45	15	84	14	62
p	Numbers															
	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65
53	43	27	26													
59	13	32	47	22	35	31	21	30	29							
61	45	53	42	33	19	37	52	32	36	31	30					
67	31	37	21	67	52	8	26	49	45	36	56	7	48	35	6	34
71	62	5	51	23	14	59	19	42	4	3	66	69	17	53	36	67
73	10	27	3	53	26	56	57	68	43	5	23	58	19	45	48	60
79	50	22	42	77	7	52	65	33	15	31	71	45	60	55	24	32
83	55	46	79	59	53	51	11	37	13	34	19	66	39	70	6	22
89	68	7	55	78	19	68	41	36	75	43	15	69	47	83	8	5
97	36	63	93	10	52	87	37	55	47	67	43	64	80	75	12	35
p	Numbers															
	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81
67	33															
71	63	47	61	41	35											
73	69	50	37	52	42	44	36									
79	73	48	29	27	41	51	14	44	23	47	40	45	39			
83	15	45	53	50	36	33	65	69	21	44	49	32	68	43	31	42
89	13	56	38	58	79	62	50	20	27	53	67	77	40	42	46	4
97	94	57	61	51	66	11	50	28	29	72	53	21	33	30	41	38
p	Numbers															
	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	
83	41															
89	37	61	26	76	45	60	44									
97	23	17	73	90	38	83	92	54	79	56	49	20	22	82	48	
p	Indices															
	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	
83	41															
89	37	61	26	76	45	60	44									
97	23	17	73	90	38	83	92	54	79	56	49	20	22	82	48	

TABLE OF INDICES.—(Continued)

Indices																
<i>p</i>	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49
27	28	19	1													
41	20	38	23	15	8	7	1									
43	31	7	21	20	17	8	24									
47	34	29	4	20	6	30	29	1								
53	9	18	36	19	38	23	46	39	25	50	47	41	29	5	10	20
59	27	54	49	39	19	38	17	34	9	18	36	13	26	52	46	31
61	45	29	58	55	49	37	13	26	52	43	25	50	39	17	34	7
67	65	63	59	51	35	3	8	12	24	48	29	58	49	31	62	57
71	10	70	64	22	12	13	20	69	57	44	24	26	40	67	43	17
73	35	29	72	68	48	21	32	14	70	58	71	63	23	42	64	28
79	13	39	38	35	26	78	76	70	52	77	73	61	25	75	67	43
83	59	35	70	57	31	62	41	82	81	79	75	67	51	19	38	76
89	36	19	57	82	68	26	78	56	79	59	88	86	80	62	8	24
97	2	10	50	56	86	42	16	80	12	60	9	45	31	58	96	92
Indices																
<i>p</i>	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65
53	40	27	1													
59	3	6	12	24	48	37	15	30	1							
61	14	28	56	51	41	21	42	23	46	31	1					
67	47	27	54	41	15	30	60	53	39	11	22	44	21	42	17	34
71	48	52	9	63	15	34	25	33	18	55	30	68	50	66	36	39
73	67	43	69	53	46	11	55	86	61	13	65	33	19	22	37	39
79	50	71	55	7	21	63	31	14	42	47	62	28	5	15	46	56
83	69	55	27	54	25	50	17	34	68	53	23	46	9	18	36	72
89	72	38	25	75	47	52	67	23	69	29	87	83	71	35	16	48
97	72	69	54	76	89	57	91	67	44	26	33	68	49	51	61	14
Indices																
<i>p</i>	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81
67	1															
71	60	65	29	61	1											
73	49	26	57	66	38	44	1									
79	10	30	11	33	20	60	22	66	40	41	44	53	1			
83	61	39	78	73	63	43	3	6	12	24	48	13	26	52	21	42
89	55	76	50	61	5	15	45	46	49	58	85	77	53	70	32	7
97	70	59	4	20	3	15	75	84	32	63	24	23	18	90	62	19
Indices																
<i>p</i>	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	
83	1															
89	21	63	11	33	10	30	1									
97	95	87	47	41	11	55	81	17	85	37	88	52	66	39	1	

INDEX

A

- Adams, J. C., 261
 Addition, 3
 associative law for, 3
 commutative law for, 3
 Algorithm, 26
 Euclid's, 26
 least remainder, 45
 Al Khowarizmi, 26
 Amicable numbers, 83
 Associate numbers, 154
 Associative law, for addition, 3
 for multiplication, 4

B

- Base, 13
 Bernoullian numbers, 249-269, 407
 Binary system of notation, 15, 22
 Biquadrate, 5, 21
 Bonse's inequality, 87
 Brauer, A., 399

C

- Calendar problems, 206-221
 Cauchy, 380
 Chinese method, 191
 Combinatorial theorem, 105
 Commutative law, for addition, 3
 for multiplication, 3
 Composite numbers, 5, 68
 successive, 90
 Congruences, definition, 126

- Congruences, degree of, 174
 of first degree, 176
 methods for solving, 177
 of higher degree, 192, 193
 in one unknown, 173
 quadratic, 315
 simple properties, 126
 system of, 184
 Congruent numbers, 419
 Cube, 5, 21

D

- Decimal system, 13
 Delaunay, 406
 Dickson, L. E., 380
 Diophantine equations, 55
 (See also Indeterminate equations)
 Diophantine problems, 388-428
 Diophantus, 55, 379
 Dirichlet, P. G., 93, 276, 407
 Distributive law, 4
 Divisibility, 24
 criterion of, 73, 131
 Division, 12, 24
 Divisors, 24, 74
 common, 25
 theorems concerning, 29
 greatest common, 26
 of several numbers, 28, 75
 number of, 76
 product of, 83
 sum of, 76, 80
 sum of r th powers of, 83

E

- $E(x)$, 94
 Epact, 213
 Eratosthenes, 69
 sieve of, 69
 Exclusion method, 317, 360
 Euclid, 2, 85
 algorithm of, 26
 rule for perfect numbers, 81
 Euler, L., 79, 130, 225, 284, 337,
 380, 407
 φ -function of, 107, 113, 143
 recurrence formula of, 79, 437
 Euler's criterion, 204, 274
 Euler's theorem, 146, 177, 227
 Even integer, 5

F

- Factorable numerical functions, 77
 inversion formula for, 114
 Factorial, power of prime in, 99
 Factorization, unique, theorem of,
 71
 Fermat, Pierre de, 2, 20, 25, 130,
 337, 339, 342, 379, 399, 401,
 407, 413.
 Fermat's equation, 346
 Fermat's last theorem, 407
 Fermat's little theorem, 146, 276
 Fermat's quotient, 151
 Fibonacci series, 41, 44
 Figurate numbers, 9
 Fractions mod m , 262
 Friendly numbers, 83
 Fundamental theorem of arith-
 metic, 32

G

- Gauss, K. F., 20, 21, 126, 153, 154,
 219, 286, 380, 474

Goldbach, 94

Greatest common divisor, 26
 of several numbers, 28

H

Hexagonal numbers, 10, 22
 Hindu-Arabic notation, 13

I

Indeterminate linear equations,
 52-67
 nonnegative solutions of, 59
 in several unknowns, 62
 systems of, 62
 Indices, 237
 Integral logarithm, 90
 Integral part, 94
 properties of, 95
 Inversion formula, 114

J

Jacobi, C. G. J., 295, 341
 Jacobi's symbol, 295
 Jacobi's theorem, 450

K

Kronecker, Leopold, 47, 156, 411,
 474
 Kronecker's theorem, 50
 Kummer, E. E., 20, 264, 375, 407
 Kummer's congruences, 262

L

Lagrange, J. L., 153, 335, 380
 Lagrange's theorem, 197
 $\lambda(n)$, 112

Lamé, Gabriel, 43, 407
 Lamé's theorem, 43
 Least common multiple, 35
 of several numbers, 36, 75
 Least-remainder algorithm, 45
 Lebesgue, V. A., 407
 Legendre, A. M., 277, 285, 311,
 407
 Legendre's symbol, 276
 Lehmer, D. H., 82, 322
 Lehmer, D. N., 70
 Liouville's function, 112
 Liouville's methods, 429-474

M

Magic squares, 159-172
 Meissel's formula, 120
 Mersenne, 25, 337, 413
 Mersenne's numbers, 82
 Metonic cycle, 212
 Modulus, 126
 Moebius's function, 109
 fundamental property of, 111
 $\mu(n)$, 109
 Multiple, common, 35
 least common, 35
 of several numbers, 36
 Multiplication, 3
 associative law for, 4
 commutative law for, 3

N

Nim, 16
 Nonresidues, 202
 Numerical functions, factorable, 77
 inversion formula for, 114

O

Octagonal number, 11
 Odd integer, 5

P

Pellian equation, 335
 (See also Fermat's equation)
 Pentagonal numbers, 10, 21
 generalized, 79
 Perfect numbers, 80
 Euclid's rule for, 81
 $\varphi(n)$, 107, 113, 143
 $\pi(x)$, 90, 117, 118, 120
 Polygonal numbers, 9, 21, 379
 table of, 11
 Powers, sums of, 139, 151, 199, 232,
 249, 253
 Prime numbers, 5, 21, 68-104
 contained in factorial, 99
 distribution of, 90
 infinite number of, 85
 in progressions, 92
 twin, 90
 Primitive roots, 229
 Primitive solutions, 38
 Pythagoras, 2
 Pythagorean equation, 37

Q

Quadratic congruences, 315
 solution by exclusion method,
 317
 Quadratic forms, 325-387
 Quadratic reciprocity law, 284
 Quadratic residue, 156, 270
 Quaternary system of notation, 15
 Quotient, 12

R

Radix, 13
 Reciprocity law, 284, 375
 Relatively prime numbers, 31

- Remainder, 12
 Residues, 134
 complete systems of, 134
 generation of systems of, 137,
 138
 of e th power, 202
 of powers, 222
 quadratic, 270
 reduced system of, 143
 various complete systems of, 135
- S
- Scales of notation, 13
 binary, 15, 22
 decimal, 13
 quaternary, 15
 ternary, 15, 22
- Series, summation of, 5
 $\sigma(n)$, 76, 80
 Sociable numbers, 83
 Square numbers, 5, 10, 21
 Staudt, Chr. von, 143
- Staudt's theorems, 143, 153, 257
 Subtraction, 12
- T
- $\tau(n)$, 76
 Triangular numbers, 10, 21
 Tshebysheff, 86
 Twin primes, 90
- V
- Vandiver, H. S., 408
 Vinogradov, 94
 Voronoi, G., 184, 261
 Voronoi's theorem, 261
- W
- Waring's theorem, 21
 Wilson's theorem, 153, 197, 199,
 231, 275
- Z
- Zeller's rule, 210