KARPAGAM ACADEMY OF HIGHER EDUCATION

(Deemed to be University Established Under Section 3 of UGC Act 1956)

Coimbatore – 641 021.

SYLLABUS

Semester – V

		L	T	P	C
16MMU502A	**NUMBER THEORY**	**6**	**2**	**0**	**6**

Scope: On successful completion of course the learners gain about the numbers , functions and its properties.

Objectives: To enable the students to learn and gain knowledge about linear Diophantine equation, Fermat's Little theorem and Inversion formula

UNIT I

Linear Diophantine equation, prime counting function, statement of prime number theorem, Goldbach conjecture, linear congruences, complete set of residues, Chinese Remainder theorem.

UNIT II

Fermat's Little theorem, Wilson's theorem. Number theoretic functions, sum and number of divisors, Totally multiplicative functions , Definition and properties of the Dirichlet product.

UNIT III

The Mobius Inversion formula, the greatest integer function, Euler's phi-function, Euler's theorem reduced set of residues-some properties of Euler's phi-function.

UNIT IV

Order of an integer modulo n, primitive roots for primes, composite numbers having primitive roots, Euler's criterion, the Legendre symbol and its properties.

UNIT V

Quadratic reciprocity-quadratic congruences with composite moduli. Public key encryption, RSA encryption and decryption, the equation $x^2 + y^2 = z^2$, Fermat's Last theorem.

SUGGESTED READINGS

TEXT BOOK

1. David M. Burton, (2007). Elementary Number Theory, Sixth Edition, Tata McGraw-Hill, Delhi.

REFERENCES

1. Neville Robinns, (2007). Beginning Number Theory, 2nd Ed., Narosa Publishing House Pvt. Ltd., Delhi.
2. Neal Koblitz., (2006).A course in Number theory and cryptography,Second Edition, Hindustan Book Agency, New Delhi.

KARPAGAM ACADEMY OF HIGHER EDUCATION

(Deemed to be University Established Under Section 3 of UGC Act 1956)

Coimbatore – 641 021.

LECTURE PLAN
DEPARTMENT OF MATHEMATICS

Staff name: U. R. Ramakrishnan
Subject Name: Number Theory **Sub.Code:16MMU502A**
Semester: V **Class: III B.Sc Mathematics**

S.No	Lecture Duration Period	Topics to be Covered	Support Material/Page Nos
		UNIT-I	
1.	1	Linear Diophantine equation	T_1:Chap2 P.No:38-39
2.	1	Theorem on Diophantine equation	T_1:Chap2 P.No:40
3.	1	Problems on Diophantine equation	T_1:Chap2 P.No:41-44
4.	1	Tutorial-1	
5.	1	Prime counting function	T_1:Chap3 P.No:51-56
6.	1	Statement of prime number theorem	T_1:Appendix P.No:344-350
7.	1	Goldbach conjecture	T_1:Chap3 P.No:58-61
8.	1	Tutorial-2	
9.	1	Theorem and Problems on Goldbach Conjecture	T_1:Chap3 P.No:61-65
10.	1	Linear congruences	T_1:Chap 4 P.No: 72-73
11.	1	Theorem and Problems on linear congruences	T_1:Chap 4 P.No: 73-74
12.	1	Tutorial-3	
13.	1	Complete set of residues	T_1:Chap 4 P.No:70-71
14.	1	Theorem on complete set of residues	T_1:Chap 4 P.No:71-72
15.	1	Chinese Remainder theorem	T_1:Chap 4 P.No:87-88
16.	1	Tutorial-4	

17.	1	Problems based on Chinese Remainder theorem	T_1:Chap 4 P.No:88-90
18.	1	Recapitulation and Discussion of possible questions	
Total No of Hours Planned For Unit I=18			
UNIT-II			
1.	1	Fermat's Little theorem	T_1:Chap 5 P.No:97-98
2.	1	Corollary and problems on Fermat's Little theorem	T_1:Chap 5 P.No:98-102
3.	1	Wilson's theorem	T_1:Chap 5 P.No:102-104
4.	1	Tutorial-1	
5.	1	Theorems and problems on Wilson's theorem	T_1:Chap 5 P.No:104-107
6.	1	Number theoretic functions	T_1:Chap 6 P.No:110-111
7.	1	Theorems on Number theoretic functions	T_1:Chap 6 P.No:111-114
8.	1	Tutorial-2	
9.	1	Problems on Number theoretic functions	T_1:Chap 6 P.No:114-115
10.	1	Multiplicative functions definition and theorems	T_1:Chap 6 P.No:115-117
11.	1	Continuation of theorems on Multiplicative functions	T_1:Chap 6 P.No:117-118
12.	1	Tutorial-3	
13.	1	Corollary and Problems on Multiplicative functions	T_1:Chap 6 P.No:118-120
14.	1	Dirichelet Product	R_1:Chap 5 P.No:119-120
15.	1	Theorems on Dirichelet Product	R_1:Chap 5 P.No:120-123
16.	1	Tutorial-4	
17.	1	Continuation of theorems on Dirichelet Product	R_1:Chap 5 P.No:123-124
18.	1	Continuation of theorems on Dirichelet Product	R_1:Chap 5 P.No:124-125
19.	1	Recapitulation and Discussion of possible questions	
Total No of Hours Planned For Unit II=19			
UNIT-III			

1.	1	The Mobius Inversion formula-Definition and theorem	T_1:Chap 6 P.No:120-122
2.	1	Continuation of theorems and Problems on Mobius Inversion formula	T_1:Chap 6 P.No:122-125
3.	1	Tutorial-1	
4.	1	The greatest integer function-Definition with example	T_1:Chap 6 P.No:126
5.	1	Theorems on the greatest integer function	T_1:Chap 6 P.No:126-130
6.	1	Problems on The greatest integer function	T_1:Chap 6 P.No:130-132
7.	1	Tutorial-2	
8.	1	Euler's phi-function-Definition with example	T_1:Chap 7 P.No:136-137
9.	1	Theorems on Euler's phi-function	T_1:Chap 7 P.No:137-138
10.	1	Continuation of theorems on Euler's phi-function	T_1:Chap 7 P.No:138-140
11.	1	Tutorial-3	
12.	1	Euler's theorem reduced set of residues	T_1:Chap 7 P.No:142-144
13.	1	Some related theorems for Euler's theorem	T_1:Chap 7 P.No:144-147
14.	1	Properties of Euler's phi-function - Theorem and examples	T_1:Chap 7 P.No:148-149
15.	1	Tutorial-4	
16.	1	Continuation of theorem on Properties of Euler's phi-function	T_1:Chap 7 P.No:149-150
17.	1	Problems on properties of Euler's phi-function	T_1:Chap 7 P.No:150-152
18.	1	Tutorial-5	
19.	1	Recapitulation and Discussion of possible questions	
Total No of Hours Planned For Unit III=19			
UNIT-IV			
1.	1	Order of an integer modulo n-Definition with example	T_1:Chap 8 P.No:156
2.	1	Theorems on Order of an integer modulo n	T_1:Chap 8 P.No:156-160
3.	1	Problems on Order of an integer modulo n	T_1:Chap 8 P.No:160-162

4.	1	Tutorial-1	
5.	1	Theorems on Primitive roots for primes	T_1:Chap 8 P.No:162-164
6.	1	Continuation of theorem on Primitive roots for primes	T_1:Chap 8 P.No:164-168
7.	1	Problems on Primitive roots for primes	T_1:Chap 8 P.No:168-169
8.	1	Tutorial-2	
9.	1	Theorems on primitive roots for composite numbers	T_1:Chap 8 P.No:170-172
10.	1	Continuation of theorems and problems on primitive roots for composite numbers	T_1:Chap 8 P.No:173-175
11.	1	Euler criterion	T_1:Chap 9 P.No:184-187
12.	1	Tutorial-3	
13.	1	Problems on Euler criterion	T_1:Chap 9 P.No:187-190
14.	1	Definition and theorems on Legendre symbol and its properties	T_1:Chap 9 P.No:190-193
15.	1	Continuation of theorem on Legendre symbol and its properties	T_1:Chap 9 P.No:194-197
16.	1	Tutorial-4	
17.	1	Continuation of theorem on Legendre symbol and its properties	T_1:Chap 9 P.No:197-201
18.	1	Problems on Legendre symbol and its properties	T_1:Chap 9 P.No:201-203
19.	1	Tutorial-5	
20.	1	Recapitulation and Discussion of possible questions	
Total No of Hours Planned For Unit IV=20			
UNIT-V			
1.	1	Quadratic reciprocity-Introduction and theorems	T_1:Chap 9 P.No:203-206
2.	1	Continuation of theorem and problems on Quadratic reciprocity	T_1:Chap 9 P.No:206-210
3.	1	Theorems on quadratic congruences with composite moduli	T_1:Chap 9 P.No:210-214
4.	1	Tutorial-1	
5.	1	Problems on quadratic congruences with composite moduli	T_1:Chap 9 P.No:215

6.	1	The idea of public key crptography	R_2:Chap 4 P.No:83-85
7.	1	Continuation of the idea of public key Crptography	R_2:Chap 4 P.No:86-88
8.	1	Tutorial-2	
9.	1	Classical vesus public key and Authentication	R_2:Chap 4 P.No:88-89
10.	1	Hash functions, key exchange and Probabilistic Encryption	R_2:Chap 4 P.No:89
11.	1	RSA encryption and decryption	R_2:Chap 4 P.No:92-95
12.	1	Tutorial-3	
13.	1	Theorems on Fermat's Last theorem	T_1:Chap 11 P.No:250-254
14.	1	Continuation of theorems on Fermat's Last theorem	T_1:Chap 11 P.No:254-256
15.	1	Problems on Fermat's Last theorem	T_1:Chap 11 P.No:257-258
16.	1	Tutorial-4	
17.	1	Recapitulation and Discussion of possible questions	
18.	1	Discuss on Previous ESE Question Papers	
19.	1	Discuss on Previous ESE Question Papers	
20.	1	Discuss on Previous ESE Question Papers	
Total No of Hours Planned for unit V=20			
Total Planned Hours			**96**

SUGGESTED READINGS

TEXT BOOK

1. David M. Burton, (2007). Elementary Number Theory, Sixth Edition, Tata McGraw-Hill, Delhi.

REFERENCES

1. Neville Robinns, (2007). Beginning Number Theory, 2nd Ed., Narosa Publishing House Pvt. Ltd., Delhi.
2. Neal Koblitz., (2006).A course in Number theory and cryptography,Second Edition, Hindustan Book Agency, New Delhi.

UNIT-I

SYLLABUS

Linear Diophantine equation, prime counting function, statement of prime number theorem, Goldbach conjecture, linear congruences, complete set of residues, Chinese Remainder theorem.

THE GREATEST COMMON DIVISOR

DEFINITION 2-1. An integer b is said to be *divisible* by an integer $a \neq 0$, in symbols $a \mid b$, if there exists some integer c such that $b = ac$. We write $a \nmid b$ to indicate that b is not divisible by a.

Thus, for example, -12 is divisible by 4, since $-12 = 4(-3)$. However, 10 is not divisible by 3; for there is no integer c which makes the statement $10 = 3c$ true.

There is other language for expressing the divisibility relation $a \mid b$. One could say that a is a *divisor* of b, that a is a *factor* of b or that b is a *multiple* of a. Notice that, in Definition 2-1, there is a restriction on the divisor a: whenever the notation $a \mid b$ is employed, it is understood that a is different from zero.

If a is a divisor of b, then b is also divisible by $-a$ (indeed, $b = ac$ implies that $b = (-a)(-c)$), so that the divisors of an integer always occur in pairs. In order to find all the divisors of a given integer, it is sufficient to obtain the positive divisors and then adjoin to them the corresponding negative integers. For this reason, we shall usually limit ourselves to a consideration of positive divisors.

THEOREM 2-2. *For integers a, b, c, the following hold:*

(1) $a \mid 0$, $1 \mid a$, $a \mid a$.
(2) $a \mid 1$ *if and only if* $a = \pm 1$.
(3) *If* $a \mid b$ *and* $c \mid d$, *then* $ac \mid bd$.
(4) *If* $a \mid b$ *and* $b \mid c$, *then* $a \mid c$.
(5) $a \mid b$ *and* $b \mid a$ *if and only if* $a = \pm b$.
(6) *If* $a \mid b$ *and* $b \neq 0$, *then* $|a| \leq |b|$.
(7) *If* $a \mid b$ *and* $a \mid c$, *then* $a \mid (bx + cy)$ *for arbitrary integers* x *and* y.

DEFINITION 2-2. Let a and b be given integers, with at least one of them different from zero. The *greatest common divisor* of a and b, denoted by $\gcd(a, b)$, is the positive integer d satisfying

(1) $d \mid a$ and $d \mid b$,
(2) if $c \mid a$ and $c \mid b$, then $c \leq d$.

Example 2-1

The positive divisors of -12 are 1, 2, 3, 4, 6, 12, while those of 30 are 1, 2, 3, 5, 6, 10, 15, 30; hence, the positive common divisors of -12 and 30 are 1, 2, 3, 6. Since 6 is the largest of these integers, it follows that $\gcd(-12, 30) = 6$. In the same way, one can show that

$$\gcd(-5, 5) = 5, \quad \gcd(8, 17) = 1, \quad \text{and} \quad \gcd(-8, -36) = 4.$$

Note

The next theorem indicates that $\gcd(a, b)$ can be represented as a linear combination of a and b (by a *linear combination* of a and b, we mean an expression of the form $ax + by$, where x and y are integers). This is illustrated by, say,

$$\gcd(-12, 30) = 6 = (-12)2 + 30 \cdot 1$$

or

$$\gcd(-8, -36) = 4 = (-8)4 + (-36)(-1).$$

THEOREM 2-3. *Given integers a and b, not both of which are zero, there exist integers x and y such that*

$$\gcd(a, b) = ax + by.$$

Proof: Consider the set S of all positive linear combinations of a and b:

$$S = \{au + bv \mid au + bv > 0;\ u, v \text{ integers}\}.$$

Notice first that S is not empty. For example, if $a \neq 0$, then the integer $|a| = au + b \cdot 0$ will lie in S, where we choose $u = 1$ or $u = -1$ according as a is positive or negative. By virtue of the Well-Ordering Principle, S must contain a smallest element d. Thus, from the very definition of S, there exist integers x and y for which $d = ax + by$. We claim that $d = \gcd(a, b)$.

Taking stock of the Division Algorithm, one can obtain integers q and r such that $a = qd + r$, where $0 \leq r < d$. Then r can be written in the form

$$\begin{aligned} r = a - qd &= a - q(ax + by) \\ &= a(1 - qx) + b(-qy). \end{aligned}$$

Were $r > 0$, this representation would imply that r is a member of S, contradicting the fact that d is the least integer in S (recall that $r < d$). Therefore, $r = 0$ and so $a = qd$, or equivalently, $d \mid a$. By similar reasoning $d \mid b$, the effect of which is to make d a common divisor of both a and b.

Now if c is an arbitrary positive common divisor of the integers a and b, then part (7) of Theorem 2-2 allows us to conclude that $c \mid (ax + by)$; in other words, $c \mid d$. By (6) of the same theorem, $c = |c| \leq |d| = d$, so that d is greater than every positive common divisor of a and b. Piecing the bits of information together, we see that $d = \gcd(a, b)$.

COROLLARY. *If a and b are given integers, not both zero, then the set*

$$T = \{ax + by \mid x, y \text{ are integers}\}$$

is precisely the set of all multiples of $d = \gcd(a, b)$.

Proof: Since $d \mid a$ and $d \mid b$, we know that $d \mid (ax + by)$ for all integers x, y. Thus, every member of T is a multiple of d. On the other hand, d may be written as $d = ax_0 + by_0$ for suitable integers x_0 and y_0, so that any multiple nd of d is of the form

$$nd = n(ax_0 + by_0) = a(nx_0) + b(ny_0).$$

Hence, nd is a linear combination of a and b, and, by definition, lies in T.

It may happen that 1 and -1 are the only common divisors of a given pair of integers a and b, whence $\gcd(a, b) = 1$. For example:

$$\gcd(2, 5) = \gcd(-9, 16) = \gcd(-27, -35) = 1.$$

DEFINITION 2-3. Two integers a and b, not both of which are zero, are said to be *relatively prime* whenever $\gcd(a, b) = 1$.

THEOREM 2-4. *Let a and b be integers, not both zero. Then a and b are relatively prime if and only if there exist integers x and y such that* $1 = ax + by$.

Proof: If a and b are relatively prime so that $\gcd(a, b) = 1$, then Theorem 2-3 guarantees the existence of integers x and y satisfying $1 = ax + by$. As for the converse, suppose that $1 = ax + by$ for some choice of x and y, and that $d = \gcd(a, b)$. Since $d \mid a$ and $d \mid b$, Theorem 2-2 yields $d \mid (ax + by)$, or $d \mid 1$. Inasmuch as d is a positive integer, this last divisibility condition forces $d = 1$ (part (2) of Theorem 2-2 plays a role here) and the desired conclusion follows.

COROLLARY 1. *If* $\gcd(a, b) = d$, *then* $\gcd(a/d, b/d) = 1$.

Proof: Before starting with the proof proper, we should observe that while a/d and b/d have the appearance of fractions, they are in fact integers since d is a divisor both of a and of b. Now, knowing that $\gcd(a, b) = d$, it is possible to find integers x and y such that $d = ax + by$. Upon dividing each side of this equation by d, one obtains the expression

$$1 = (a/d)x + (b/d)y.$$

Because a/d and b/d are integers, an appeal to the theorem is legitimate. The upshot is that a/d and b/d are relatively prime.

For an illustration of the last corollary, let us observe that $\gcd(-12, 30) = 6$ and

$$\gcd(-12/6, 30/6) = \gcd(-2, 5) = 1,$$

COROLLARY 2. *If* $a \mid c$ *and* $b \mid c$, *with* $\gcd(a, b) = 1$, *then* $ab \mid c$.

Proof: Inasmuch as $a \mid c$ and $b \mid c$, integers r and s can be found such that $c = ar = bs$. Now the relation $\gcd(a, b) = 1$ allows us to write $1 = ax + by$ for some choice of integers x and y. Multiplying the last equation by c, it appears that

$$c = c \cdot 1 = c(ax + by) = acx + bcy.$$

If the appropriate substitutions are now made on the right-hand side, then

$$c = a(bs)x + b(ar)y = ab(sx + ry)$$

or, as a divisibility statement, $ab \mid c$.

THEOREM 2-5 (Euclid's Lemma). *If* $a \mid bc$, *with* $\gcd(a, b) = 1$, *then* $a \mid c$.

Proof: We start again from Theorem 2-3, writing $1 = ax + by$ where x and y are integers. Multiplication of this equation by c produces

$$c = 1 \cdot c = (ax + by)c = acx + bcy.$$

Since $a \mid ac$ and $a \mid bc$, it follows that $a \mid (acx + bcy)$, which can be recast as $a \mid c$.

If a and b are not relatively prime, then the conclusion of Euclid's Lemma may fail to hold. A specific example: $12 \mid 9 \cdot 8$, but $12 \nmid 9$ and $12 \nmid 8$.

THEOREM 2-6. *Let* a, b *be integers, not both zero. For a positive integer* d, $d = \gcd(a, b)$ *if and only if*

(1) $d \mid a$ *and* $d \mid b$,
(2) *whenever* $c \mid a$ *and* $c \mid b$, *then* $c \mid d$.

THE DIOPHANTINE EQUATION $ax + by = c$

It is customary to apply the term *Diophantine equation* to any equation in one or more unknowns which is to be solved in the integers. The simplest type of Diophantine equation that we shall consider is the linear Diophantine equation in two unknowns:

$$ax + by = c,$$

where a, b, c are given integers and a, b not both zero. A solution of this equation is a pair of integers x_0, y_0 which, when substituted into the equation, satisfy it; that is, we ask that $ax_0 + by_0 = c$. Curiously enough,

A given linear Diophantine equation can have a number of solutions, as with $3x + 6y = 18$, where

$$3\cdot 4 + 6\cdot 1 = 18,$$
$$3(-6) + 6\cdot 6 = 18,$$
$$3\cdot 10 + 6(-2) = 18.$$

By contrast, there is no solution to the equation $2x + 10y = 17$. Indeed, the left-hand side is an even integer whatever the choice of x and y, while the right-hand side is not.

THEOREM 2-9. *The linear Diophantine equation $ax + by = c$ has a solution if and only if $d \mid c$, where $d = \gcd(a, b)$. If x_0, y_0 is any particular solution of this equation, then all other solutions are given by*

$$x = x_0 + (b/d)t, \qquad y = y_0 - (a/d)t$$

for varying integers t.

Proof: To establish the second assertion of the theorem, let us suppose that a solution x_0, y_0 of the given equation is known. If x', y' is any other solution, then

$$ax_0 + by_0 = c = ax' + by',$$

which is equivalent to

$$a(x' - x_0) = b(y_0 - y').$$

By the Corollary to Theorem 2-4, there exist relatively prime integers r and s such that $a = dr$, $b = ds$. Substituting these values into the last-written equation and cancelling the common factor d, we find that

$$r(x' - x_0) = s(y_0 - y').$$

The situation is now this: $r \mid s(y_0 - y')$, with $\gcd(r, s) = 1$. Using Euclid's Lemma, it must be the case that $r \mid (y_0 - y')$; or, in other words, $y_0 - y' = rt$ for some integer t. Substituting, we obtain

$$x' - x_0 = st.$$

This leads us to the formulas

$$x' = x_0 + st = x_0 + (b/d)t,$$
$$y' = y_0 - rt = y_0 - (a/d)t.$$

It is easy to see that these values satisfy the Diophantine equation, regardless of the choice of the integer t; for,

$$\begin{aligned} ax' + by' &= a[x_0 + (b/d)t] + b[y_0 - (a/d)t] \\ &= (ax_0 + by_0) + (ab/d - ab/d)t \\ &= c + 0 \cdot t = c. \end{aligned}$$

Thus there are an infinite number of solutions of the given equation, one for each value of t.

Example 2-3

Consider the linear Diophantine equation

$$172x + 20y = 1000.$$

Applying Euclid's Algorithm to the evaluation of gcd (172, 20), we find that

$$172 = 8 \cdot 20 + 12,$$
$$20 = 1 \cdot 12 + 8,$$

$$12 = 1 \cdot 8 + 4,$$
$$8 = 2 \cdot 4,$$

whence $\gcd(172, 20) = 4$. Since $4 \mid 1000$, a solution to this equation exists. To obtain the integer 4 as a linear combination of 172 and 20, we work backwards through the above calculations, as follows:

$$\begin{aligned} 4 &= 12 - 8 \\ &= 12 - (20 - 12) \\ &= 2 \cdot 12 - 20 \\ &= 2(172 - 8 \cdot 20) - 20 \\ &= 2 \cdot 172 + (-17)20. \end{aligned}$$

Upon multiplying this relation by 250, one arrives at

$$\begin{aligned} 1000 &= 250 \cdot 4 - 250[2 \cdot 172 + (-17)20] \\ &= 500 \cdot 172 + (-4250)20, \end{aligned}$$

so that $x = 500$ and $y = -4250$ provides one solution to the Diophantine equation in question. All other solutions are expressed by

$$x = 500 + (20/4)t = 500 + 5t,$$
$$y = -4250 - (172/4)t = -4250 - 43t$$

for some integer t.

A little further effort produces the solutions in the positive integers, if any happen to exist. For this, t must be chosen so as to satisfy simultaneously the inequalities

$$5t + 500 > 0, \qquad -43t - 4250 > 0$$

or, what amounts to the same thing,

$$-98\tfrac{36}{43} > t > -100.$$

Since t must be an integer, we are forced to conclude that $t = -99$. Thus our Diophantine equation has a unique positive solution $x = 5$, $y = 7$ corresponding to the value $t = -99$.

COROLLARY. *If* $\gcd(a, b) = 1$ *and if* x_0, y_0 *is a particular solution of the linear Diophantine equation* $ax + by = c$, *then all solutions are given by*

$$x = x_0 + bt, \qquad y = y_0 - at$$

for integral values of t.

Example 2-4

A customer bought a dozen pieces of fruit, apples and oranges, for \$1.32. If an apple costs 3 cents more than an orange and more apples than oranges were purchased, how many pieces of each kind were bought?

To set up this problem as a Diophantine equation, let x be the number of apples and y the number of oranges purchased; also, let z represent the cost (in cents) of an orange. Then the conditions of the problem lead to

$$(z + 3)x + zy = 132$$

or equivalently

$$3x + (x + y)z = 132.$$

Since $x + y = 12$, the above equation may be replaced by

$$3x + 12z = 132,$$

which in turn simplifies to $x + 4z = 44$.

Stripped of inessentials, the object is to find integers x and z satisfying the Diophantine equation

(*) $$x + 4z = 44.$$

Inasmuch as $\gcd(1, 4) = 1$ is a divisor of 44, there is a solution to this equation. Upon multiplying the relation $1 = 1(-3) + 4 \cdot 1$ by 44 to get

$$44 = 1(-132) + 4 \cdot 44,$$

it follows that $x_0 = -132$, $z_0 = 44$ serves as one solution. All other solutions of $(*)$ are of the form

$$x = -132 + 4t,$$
$$z = 44 - t,$$

where t is an integer.

Not all of the infinite set of values of t furnish solutions to the original problem. Only values of t should be considered which will ensure that $12 \geq x > 6$. This requires obtaining those t such that

$$12 \geq -132 + 4t > 6.$$

Now, $12 \geq -132 + 4t$ implies that $t \leq 36$, while $-132 + 4t > 6$ gives $t > 34\frac{1}{2}$. The only integral values of t to satisfy both inequalities are $t = 35$ and $t = 36$. Thus there are two possible purchases: a dozen apples costing 11 cents apiece (the case where $t = 36$), or else 8 apples at 12 cents each and 4 oranges at 9 cents each (the case where $t = 35$).

DEFINITION 3-1. An integer $p > 1$ is called a *prime number*, or simply a *prime*, if its only positive divisors are 1 and p. An integer greater than 1 which is not a prime is termed *composite*.

THE GOLDBACH CONJECTURE

While there is an infinitude of primes, their distribution within the positive integers is most mystifying. Repeatedly in their distribution one finds hints or, as it were, shadows of a pattern; yet an actual pattern amenable to precise description remains unfound. The difference between consecutive primes can be small as with the pairs 11 and 13, 17 and 19, or for that matter 1,000,000,000,061 and 1,000,000,000,063. At the same

time there exist arbitrarily long intervals in the sequence of integers which are totally devoid of any primes.

It is an unanswered question whether there are infinitely many pairs of *twin primes*; that is, pairs of successive odd integers p and $p+2$ which are both primes. Numerical evidence leads us to suspect an affirmative conclusion. Electronic computers have discovered 152,892 pairs of twin primes less than 30,000,000 and twenty pairs between 10^{12} and $10^{12}+10{,}000$, which hints at their growing scarcity as the positive integers increase in magnitude.

Consecutive primes can not only be close together, but also be far apart; that is, arbitrarily large gaps can occur between consecutive primes. Stated precisely: Given any positive integer n, there exist n consecutive integers, all of which are composite. To prove this, we need simply consider the integers

$$(n+1)!+2,\ (n+1)!+3,\ \ldots,\ (n+1)!+(n+1),$$

where $(n+1)!=(n+1)\cdot n\cdots 3\cdot 2\cdot 1$. Clearly there are n integers listed and they are consecutive. What is important is that each integer is composite; for, $(n+1)!+2$ is divisible by 2, $(n+1)!+3$ is divisible by 3, and so on.

For instance, if a sequence of four consecutive composite integers is desired, then the argument above produces 122, 123, 124, and 125:

$$5!+2=122=2\cdot 61,$$
$$5!+3=123=3\cdot 41,$$
$$5!+4=124=4\cdot 31,$$
$$5!+5=125=5\cdot 25.$$

Of course, one can find other sets of four consecutive composites, such as 24, 25, 26, 27 or 32, 33, 34, 35.

This brings us to another unsolved problem concerning primes, the Goldbach Conjecture. In a letter to Euler (1742), Christian Goldbach hazarded the guess that every even integer is the sum of two numbers that are either primes or 1. A somewhat more general formulation is that every even integer greater than 4 can be written as a sum of two odd prime numbers. This is easy to confirm for the first few even integers:

$$
\begin{aligned}
2 &= 1 + 1 \\
4 &= 2 + 2 = 1 + 3 \\
6 &= 3 + 3 = 1 + 5 \\
8 &= 3 + 5 = 1 + 7 \\
10 &= 3 + 7 = 5 + 5 \\
12 &= 5 + 7 = 1 + 11 \\
14 &= 3 + 11 = 7 + 7 = 1 + 13 \\
16 &= 3 + 13 = 5 + 11 \\
18 &= 5 + 13 = 7 + 11 = 1 + 17 \\
20 &= 3 + 17 = 7 + 13 = 1 + 19 \\
22 &= 3 + 19 = 5 + 17 = 11 + 11 \\
24 &= 5 + 19 = 7 + 17 = 11 + 13 = 1 + 23 \\
26 &= 3 + 23 = 7 + 19 = 13 + 13 \\
28 &= 5 + 23 = 11 + 17 \\
30 &= 7 + 23 = 11 + 19 = 13 + 17 = 1 + 29.
\end{aligned}
$$

It seems that Euler never tried to prove the result, but, writing to Goldbach at a later date he countered with a conjecture of his own: any even integer (≥ 6) of the form $4n+2$ is a sum of two numbers each being either primes of the form $4n+1$ or 1.

The numerical evidence for the truth of these conjectures is overwhelming (indeed Goldbach's Conjecture has been verified for all even integers up to 100,000), but a general proof or counterexample is still awaited. The nearest approach of modern number theorists to Goldbach's Conjecture is the result of the Russian mathematician Vinogradov, which states: Almost all even integers are the sum of two primes. The technical meaning of the term "almost all" is that if $A(n)$ denotes the number of even integers $m \leq n$ which are not representable as the sum of two primes, then

$$\lim_{n \to \infty} A(n)/n = 0.$$

As Landau so aptly put it, "The Goldbach conjecture is false for at most 0% of all even integers; this at most 0% does not exclude, of course, the possibility that there are infinitely many exceptions."

We remark that if the conjecture of Goldbach is true, then each odd number larger than 7 must be the sum of three odd primes. For, take n to be an odd integer greater than 7, so that $n-3$ is even and greater than 4; if $n-3$ could be expressed as the sum of two odd primes, then n would be the sum of three. In 1937, Vinogradov showed that this does indeed hold for every sufficiently large odd integer, say greater than N. Thus, it is enough to answer the question for every odd integer n in the range $9 \leq n \leq N$, which for a given integer becomes a matter of tedious computation (unfortunately, N is so large that this exceeds the capabilities of the most modern electronic computers).

Vinogradov's result implies that every sufficiently large even integer is the sum of not more than four odd primes. Thus, there is a number N such that every even integer beyond N is the sum of either two or four odd primes.

Having digressed somewhat, let us observe that according to the Division Algorithm, every positive integer can be written uniquely in one of the forms

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

for some suitable $n \geq 0$. Clearly, the integers $4n$ and $4n+2=2(2n+1)$ are both even. Thus, all odd integers fall into two progressions: one containing integers of the form $4n+1$,

$$1, 5, 9, 13, 17, 21, \ldots$$

and the other containing integers of the form $4n+3$,

$$3, 7, 11, 15, 19, 23, \ldots .$$

While each of these progressions includes some obviously prime numbers, the question arises as to whether each of them contains infinitely many primes. This provides a pleasant opportunity for a repeat performance of Euclid's method for proving the existence of an infinitude of primes. A slight modification of his argument reveals that there are an infinite number of primes of the form $4n+3$. We approach the proof through a simple lemma.

LEMMA. *The product of two or more integers of the form* $4n+1$ *is of the same form.*

Proof: It is sufficient to consider the product of just two integers. Let $k=4n+1$ and $k'=4m+1$. Multiplying these together, we obtain

$$\begin{aligned} kk' &= (4n+1)(4m+1) \\ &= 16nm+4n+4m+1 = 4(4nm+n+m)+1, \end{aligned}$$

which is of the desired form.

This paves the way for:

THEOREM 3-6. *There is an infinite number of primes of the form* $4n + 3$.

Proof: In anticipation of a contradiction, let us assume that there exist only finitely many primes of the form $4n + 3$; call them q_1, $q_2, \ldots, q_s$. Consider the positive integer

$$N = 4q_1 q_2 \cdots q_s - 1 = 4(q_1 q_2 \cdots q_s - 1) + 3$$

and let $N = r_1 r_2 \cdots r_t$ be its prime factorization. Since N is an odd integer, we have $r_k \neq 2$ for all k, so that each r_k is either of the form $4n + 1$ or $4n + 3$. By the Lemma, the product of any number of primes of the form $4n + 1$ is again an integer of this type. For N to take the form $4n + 3$, as it clearly does, N must contain at least one prime factor r_i of the form $4n + 3$. But r_i cannot be found among the listing $q_1, q_2, \ldots, q_s$, for this would lead to the contradiction that $r_i \mid 1$. The only possible conclusion is that there are infinitely many primes of the form $4n + 3$.

Having just seen that there are infinitely many primes of the form $4n + 3$, one might reasonably ask: Is the number of primes of the form $4n + 1$ also infinite? This answer is likewise in the affirmative, but a demonstration must await the development of the necessary mathematical machinery. Both these results are special cases of a remarkable theorem by Dirichlet on primes in arithmetic progressions, established in 1837. The proof is much too difficult for inclusion here, so that we content ourselves with the mere statement.

THEOREM 3-7 (Dirichlet). *If a and b are relatively prime positive integers, then the arithmetic progression*

$$a, a+b, a+2b, a+3b, \ldots$$

contains infinitely many primes.

There is no arithmetic progression $a, a+b, a+2b, \ldots$ that consists solely of prime numbers. To see this, suppose that $a+nb=p$, where p is a prime. If we put $n_k = n \mid kp$ for $k=1, 2, 3, \ldots$, then the n_kth term in the progression is

$$a+n_k b = a+(n+kp)b = (a+nb)+kpb = p+kpb.$$

Since each term on the right-hand side is divisible by p, so is $a+n_k b$. In other words, the progression must contain infinitely many composite numbers.

It has been conjectured that there exist arithmetic progressions of finite (but otherwise arbitrary) length, composed of consecutive prime numbers. Examples of such progressions consisting of three and four primes, respectively, are 41, 47, 53 and 251, 257, 263, 269. Not long ago, a computer search revealed progressions of five and six consecutive primes, the terms having a common difference of 30; these begin with the primes

9,843,019 and 121,174,811.

We are not able to discover, at least for the time being, an arithmetic progression consisting of seven consecutive primes. When the restriction that the prime numbers involved be consecutive is removed, then it is possible to find infinitely many sets of seven primes in an arithmetic progression; one such is 7, 157, 307, 457, 607, 757, 907.

In interests of completeness, we might mention another famous problem that so far has resisted the most determined attack. For centuries, mathematicians have sought a simple formula that would yield every prime number or, failing this, a formula that would produce nothing but primes. At first glance, the request seems modest enough: find a function $f(n)$ whose domain is, say, the nonnegative integers and whose range is some infinite subset of the set of all primes. It was widely believed in the Middle Ages that the quadratic polynomial

$$f(n) = n^2 + n + 41$$

assumed only prime values. As evidenced by the following table, the claim is a correct one for $n = 0, 1, 2, \ldots, 39$.

n	$f(n)$	n	$f(n)$	n	$f(n)$
0	41	14	251	28	853
1	43	15	281	29	911
2	47	16	313	30	971
3	53	17	347	31	1033
4	61	18	383	32	1097
5	71	19	421	33	1163
6	83	20	461	34	1231
7	97	21	503	35	1301
8	113	22	547	36	1373
9	131	23	593	37	1447
10	151	24	641	38	1523
11	173	25	691	39	1601
12	197	26	743		
13	223	27	797		

However, this provocative conjecture is shattered in the cases $n = 40$ and $n = 41$, where there is a factor of 41:

$$f(40) = 40 \cdot 41 + 41 = 41^2$$

and

$$f(41) = 41 \cdot 42 + 41 = 41 \cdot 43.$$

The next value $f(42) = 1747$ turns out to be prime once again. It is not presently known whether $f(n) = n^2 + n + 41$ assumes infinitely many prime values for integral n.

The failure of the above function to be prime-producing is no accident, for it is easy to prove that there is no nonconstant polynomial $f(n)$ with integral coefficients which takes on just prime values for integral n. We assume that such a polynomial $f(n)$ actually does exist and argue until a contradiction is reached. Let

$$f(n) = a_k n^k + a_{k-1} n^{k-1} + \cdots + a_2 n^2 + a_1 n + a_0,$$

where the coefficients $a_0, a_1, \ldots, a_k$ are all integers and $a_k \neq 0$. For a fixed value of n, say $n = n_0$, $p = f(n_0)$ is a prime number. Now, for any integer t, we consider the expression $f(n_0 + tp)$:

$$\begin{aligned} f(n_0 + tp) &= a_k(n_0 + tp)^k + \cdots + a_1(n_0 + tp) + a_0 \\ &= (a_k n_0^k + \cdots + a_1 n_0 + a_0) + pQ(t) \\ &= f(n_0) + pQ(t) \\ &= p + pQ(t) = p(1 + Q(t)), \end{aligned}$$

where $Q(t)$ is a polynomial in t having integral coefficients. Our reasoning shows that $p \mid f(n_0 + tp)$; hence, from our own assumption that $f(n)$ takes on only prime values, $f(n_0 + tp) = p$ for any integer t. Since a polynomial of degree k cannot assume the same value more than k times, we have obtained the required contradiction.

Recent years have seen a measure of success in the search for prime-producing functions. W. H. Mills proved (1947) that there exists a positive real number r such that the expression $f(n) = [r^{3^n}]$ is prime for $n = 1, 2, 3, \ldots$ (the bracket indicates the greatest integer function). Needless to say, this is strictly an existence theorem and nothing is known about the actual value of r.

BASIC PROPERTIES OF CONGRUENCE

DEFINITION 4-1. Let n be a fixed positive integer. Two integers a and b are said to be *congruent modulo n*, symbolized by

$$a \equiv b \pmod{n}$$

if n divides the difference $a - b$; that is, provided that $a - b = kn$ for some integer k.

To fix the idea, consider $n = 7$. It is routine to check that

$$3 \equiv 24 \pmod 7, \quad -31 \equiv 11 \pmod 7, \quad -15 \equiv -64 \pmod 7,$$

since $3 - 24 = (-3)7$, $-31 - 11 = (-6)7$, and $-15 - (-64) = 7 \cdot 7$. If $n \nmid (a - b)$, then we say that a is *incongruent to b modulo n* and in this case we write $a \not\equiv b \pmod{n}$. For example: $25 \not\equiv 12 \pmod 7$, since 7 fails to divide $25 - 12 = 13$.

Complete Set Residue

Given an integer a, let q and r be its quotient and remainder upon division by n, so that

$$a = qn + r, \qquad 0 \leq r < n.$$

Then, by definition of congruence, $a \equiv r \pmod{n}$. Since there are n choices for r, we see that every integer is congruent modulo n to exactly one of the values $0, 1, 2, \ldots, n-1$; in particular, $a \equiv 0 \pmod{n}$ if and only if $n \mid a$. The set of n integers $0, 1, 2, \ldots, n-1$ is called the set of *least positive residues modulo n.*

In general, a collection of n integers $a_1, a_2, \ldots, a_n$ is said to form a *complete set of residues* (or a *complete system of residues*) *modulo n* if every integer is congruent modulo n to one and only one of the a_k; to put it another way, $a_1, a_2, \ldots, a_n$ are congruent modulo n to $0, 1, 2, \ldots, n-1$, taken in some order. For instance,

$$-12, -4, 11, 13, 22, 82, 91$$

constitute a complete set of residues modulo 7; here, we have

$$-12 \equiv 2, \; -4 \equiv 3, \; 11 \equiv 4, \; 13 \equiv 6, \; 22 \equiv 1, \; 82 \equiv 5, \; 91 \equiv 0,$$

all modulo 7. An observation of some importance is that any n integers form a complete set of residues modulo n if and only if no two of the integers are congruent modulo n.

THEOREM 4-1. *For arbitrary integers a and b, $a \equiv b \pmod{n}$ if and only if a and b leave the same nonnegative remainder when divided by n.*

Proof: First, take $a \equiv b \pmod{n}$, so that $a - b + kn$ for some integer k. Upon division by n, b leaves a certain remainder r: $b = qn + r$, where $0 \leq r < n$. Therefore,

$$a = b + kn = (qn + r) + kn = (q + k)n + r,$$

which indicates that a has the same remainder as b.

On the other hand, suppose we can write $a = q_1 n + r$ and $b = q_2 n + r$, with the same remainder r $(0 \leq r < n)$. Then

$$a - b = (q_1 n + r) - (q_2 n + r) = (q_1 - q_2)n,$$

whence $n \mid a - b$. In the language of congruences, this says that $a \equiv b \pmod{n}$.

Example 4-1

Since the integers -56 and -11 can be expressed in the form

$$-56 = (-7)9 + 7, \quad -11 = (-2)9 + 7$$

with the same remainder 7, Theorem 4-1 tells us that $-56 \equiv -11 \pmod{9}$. Going in the other direction, the congruence $-31 \equiv 11 \pmod{7}$ implies that -31 and 11 have the same remainder when divided by 7; this is clear from the relations

$$-31 = (-5)7 + 4, \quad 11 = 1 \cdot 7 + 4.$$

THEOREM 4-2. *Let $n > 0$ be fixed and a, b, c, d be arbitrary integers. Then the following properties hold:*

(1) $a \equiv a \pmod{n}$.
(2) *If* $a \equiv b \pmod{n}$, *then* $b \equiv a \pmod{n}$.
(3) *If* $a \equiv b \pmod{n}$ *and* $b \equiv c \pmod{n}$, *then* $a \equiv c \pmod{n}$.
(4) *If* $a \equiv b \pmod{n}$ *and* $c \equiv d \pmod{n}$, *then* $a + c \equiv b + d \pmod{n}$ and $ac \equiv bd \pmod{n}$.
(5) *If* $a \equiv b \pmod{n}$, *then* $a + c \equiv b + c \pmod{n}$ *and* $ac \equiv bc \pmod{n}$.
(6) *If* $a \equiv b \pmod{n}$, *then* $a^k \equiv b^k \pmod{n}$ *for any positive integer* k.

Proof: For any integer a, we have $a - a = 0 \cdot n$, so that $a \equiv a \pmod{n}$. Now if $a \equiv b \pmod{n}$, then $a - b = kn$ for some integer k. Hence, $b - a = -(kn) = (-k)n$ and, since $-k$ is an integer, this yields (2).

Property (3) is slightly less obvious: Suppose that $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$. Then there exist integers h and k satisfying $a - b = hn$ and $b - c = kn$. It follows that

$$a - c = (a - b) + (b - c) = hn + kn = (h + k)n,$$

in consequence of which $a \equiv c \pmod{n}$.

In the same vein, if $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then we are assured that $a - b = k_1 n$ and $c - d = k_2 n$ for some choice of k_1 and k_2. Adding these equations, one gets

$$\begin{aligned}(a + c) - (b + d) &= (a - b) + (c - d) \\ &= k_1 n + k_2 n = (k_1 + k_2)n\end{aligned}$$

or, as a congruence statement, $a + c \equiv b + d \pmod{n}$. As regards the second assertion of (4), note that

$$ac = (b + k_1 n)(d + k_2 n) = bd + (bk_2 + dk_1 + k_1 k_2 n)n.$$

Since $bk_2 + dk_1 + k_1 k_2 n$ is an integer, this says that $ac - bd$ is divisible by n, whence $ac \equiv bd \pmod{n}$.

The proof of property (5) is covered by (4) and the fact that $c \equiv c \pmod{n}$. Finally, we obtain (6) by making an induction argument. The statement certainly holds for $k = 1$, and we will assume it is true for some fixed k. From (4), we know that $a \equiv b \pmod{n}$ and $a^k \equiv b^k \pmod{n}$ together imply that $aa^k \equiv bb^k \pmod{n}$, or equivalently, $a^{k+1} \equiv b^{k+1} \pmod{n}$. This is the form the statement should take for $k + 1$, so the induction step is complete.

Example 4-2

Let us endeavor to show that 41 divides $2^{20} - 1$. We begin by noting that $2^5 \equiv -9 \pmod{41}$, whence $(2^5)^4 \equiv (-9)^4 \pmod{41}$ by Theorem 4-2(6); in other words, $2^{20} \equiv 81 \cdot 81 \pmod{41}$. But $81 \equiv -1 \pmod{41}$ and so $81 \cdot 81 \equiv 1 \pmod{41}$. Using parts (2) and (5) of Theorem 4-2, we finally arrive at

$$2^{20} - 1 \equiv 81 \cdot 81 - 1 \equiv 1 - 1 \equiv 0 \pmod{41}.$$

Thus $41 \mid 2^{20} - 1$, as desired.

THEOREM 4-3. *If* $ca \equiv cb \pmod{n}$, *then* $a \equiv b \pmod{n/d}$, *where* $d = \gcd(c, n)$.

Proof: By hypothesis, we can write

$$c(a - b) = ca - cb = kn$$

for some integer k. Knowing that $\gcd(c, n) = d$, there exist relatively prime integers r and s satisfying $c = dr$, $n = ds$. When these values are substituted in the displayed equation and the common factor d cancelled, the net result is

$$r(a - b) = ks.$$

Hence, $s \mid r(a - b)$ and $\gcd(r, s) = 1$. Euclid's Lemma implies that $s \mid a - b$, which may be recast as $a \equiv b \pmod{s}$; in other words, $a \equiv b \pmod{n/d}$.

COROLLARY 1. *If* $ca \equiv cb \pmod{n}$ *and* $\gcd(c, n) = 1$, *then* $a \equiv b \pmod{n}$.

COROLLARY 2. *If* $ca \equiv cb \pmod{p}$ *and* $p \nmid c$, *where* p *is a prime number, then* $a \equiv b \pmod{p}$.

Proof: The conditions $p \nmid c$ and p a prime imply that $\gcd(c, p) = 1$.

Example 4-4

Consider the congruence $33 \equiv 15 \pmod 9$ or, if one prefers, $3 \cdot 11 \equiv 3 \cdot 5 \pmod 9$. Since $\gcd(3, 9) = 3$, Theorem 4-3 leads to the conclusion that $11 \equiv 5 \pmod 3$. A further illustration is furnished by the congruence $-35 \equiv 45 \pmod 8$, which is the same as $5 \cdot (-7) \equiv 5 \cdot 9 \pmod 8$. The integers 5 and 8 being relatively prime, we may cancel to obtain a correct congruence $-7 \equiv 9 \pmod 8$.

LINEAR CONGRUENCES

An equation of the form $ax \equiv b \pmod n$ is called a *linear congruence*, and by a solution of such an equation we mean an integer x_0 for which $ax_0 \equiv b \pmod n$. By definition, $ax_0 \equiv b \pmod n$ if and only if $n \mid ax_0 - b$ or, what amounts to the same thing, if and only if $ax_0 - b = ny_0$ for some integer y_0. Thus, the problem of finding all integers satisfying the linear congruence $ax \equiv b \pmod n$ is identical with that of obtaining all solutions of the linear Diophantine equation $ax - ny = b$.

It is convenient to treat two solutions of $ax \equiv b \pmod n$ which are congruent modulo n as being "equal" even though they are not equal in the usual sense. For instance, $x = 3$ and $x = -9$ both satisfy the congruence $3x \equiv 9 \pmod{12}$; since $3 \equiv -9 \pmod{12}$, they are not counted as different solutions. In short: When we refer to the number of solutions of $ax \equiv b \pmod n$, we mean the number of incongruent integers satisfying this congruence.

THEOREM 4-7. *The linear congruence* $ax \equiv b \pmod{n}$ *has a solution if and only if* $d \mid b$, *where* $d = \gcd(a, n)$. *If* $d \mid b$, *then it has* d *mutually incongruent solutions modulo* n.

Proof: We have already observed that the given congruence is equivalent to the linear Diophantine equation $ax - ny = b$. From Theorem 2-9, it is known that the latter equation can be solved if and only if $d \mid b$; moreover, if it is solvable and x_0, y_0 is one specific solution, then any other solution has the form

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

for some choice of t.

Among the various integers satisfying the first of these formulas, consider those which occur when t takes on the successive values $t = 0, 1, 2, \ldots, d-1$:

$$x_0, x_0 + \frac{n}{d}, x_0 + \frac{2n}{d}, \ldots, x_0 + \frac{(d-1)n}{d}.$$

We claim that these integers are incongruent modulo n, while all other such integers x are congruent to some one of them. If it happened that

$$x_0 + \frac{n}{d}t_1 \equiv x_0 + \frac{n}{d}t_2 \pmod{n},$$

where $0 \leq t_1 < t_2 \leq d-1$, then one would have

$$\frac{n}{d}t_1 \equiv \frac{n}{d}t_2 \pmod{n}.$$

Now $\gcd(n/d, n) = n/d$ and so, by Theorem 4-3, the factor n/d could be cancelled to arrive at the congruence

$$t_1 \equiv t_2 \pmod{d},$$

which is to say that $d \mid t_2 - t_1$. But this is impossible, in view of the inequality $0 < t_2 - t_1 < d$.

It remains to argue that any other solution $x_0 + (n/d)t$ is congruent modulo n to one of the d integers listed above. The Division Algorithm permits us to write t as $t = qd + r$, where $0 \leq r \leq d - 1$. Hence

$$\begin{aligned} x_0 + \frac{n}{d}t &= x_0 + \frac{n}{d}(qd + r) \\ &= x_0 + nq + \frac{n}{d}r \\ &\equiv x_0 + \frac{n}{d}r \pmod{n}, \end{aligned}$$

with $x_0 + (n/d)r$ being one of our d selected solutions. This ends the proof.

The argument that we gave in Theorem 4-7 brings out a point worth stating explicitly: If x_0 is any solution of $ax \equiv b \pmod{n}$, then the $d = \gcd(a, n)$ incongruent solutions are given by

$$x_0, x_0 + n/d, x_0 + 2(n/d), \ldots, x_0 + (d-1)(n/d).$$

COROLLARY. *If* $\gcd(a, n) = 1$, *then the linear congruence* $ax \equiv b \pmod{n}$ *has a unique solution modulo n.*

Example 4-6

Consider the linear congruence $18x \equiv 30 \pmod{42}$. Since gcd (18, 42) = 6 and 6 surely divides 30, Theorem 4-7 guarantees the existence of exactly six solutions, which are incongruent modulo 42. By inspection, one solution is found to be $x = 4$. Our analysis tells us that the six solutions are as follows:

$$x \equiv 4 + (42/6)t \equiv 4 + 7t \pmod{42}, \qquad t = 0, 1, \ldots, 5$$

or, plainly enumerated,

$$x \equiv 4, 11, 18, 25, 32, 39 \pmod{42}.$$

Example 4-7

Let us solve the linear congruence $9x \equiv 21 \pmod{30}$. At the outset, since gcd (9, 30) = 3 and $3 \mid 21$, we know that there must be three incongruent solutions.

One way to find these solutions is to divide the given congruence through by 3, thereby replacing it by the equivalent congruence $3x \equiv 7 \pmod{10}$. The relative primeness of 3 and 10 implies that the latter congruence admits a unique solution modulo 10. Although it is not the most efficient method, we could test the integers 0, 1, 2, ..., 9 in turn until the solution is obtained. A better way is this: multiply both sides of the congruence $3x \equiv 7 \pmod{10}$ by 7 to get

$$21x \equiv 49 \pmod{10},$$

which reduces to $x \equiv 9 \pmod{10}$. (This simplification is no accident, for the multiples $0 \cdot 3, 1 \cdot 3, 2 \cdot 3, \ldots, 9 \cdot 3$ form a complete set of residues modulo 10; hence, one of them is necessarily congruent to 1 modulo 10.) But the original congruence was given modulo 30, so that its incongruent solutions are sought among the integers 0, 1, 2, ..., 29. Taking $t = 0, 1, 2$, in the formula

$$x = 9 + 10t,$$

one gets 9, 19, 29, whence

$$x \equiv 9 \pmod{30}, \quad x \equiv 19 \pmod{30}, \quad x \equiv 29 \pmod{30}$$

are the required three solutions of $9x \equiv 21 \pmod{30}$.

A different approach to the problem would be to use the method that is suggested in the proof of Theorem 4-7. Since the congruence $9x \equiv 21 \pmod{30}$ is equivalent to the linear Diophantine equation

$$9x - 30y = 21,$$

we begin by expressing $3 = \gcd(9, 30)$ as a linear combination of 9 and 30. It is found, either by inspection or by the Euclidean Algorithm, that $3 = 9(-3) + 30 \cdot 1$, so that

$$21 = 7 \cdot 3 = 9(-21) - 30(-7).$$

Thus, $x = -21$, $y = -7$ satisfy the Diophantine equation and, in consequence, all solutions of the congruence in question are to be found from the formula

$$x = -21 + \tfrac{30}{3}t = -21 + 10t.$$

The integers $x = -21 + 10t$, where $t = 0, 1, 2$ are incongruent modulo 30 (but all are congruent modulo 10); thus, we end up with the incongruent solutions

$$x \equiv -21 \pmod{30}, \quad x \equiv -11 \pmod{30}, \quad x \equiv -1 \pmod{30}$$

or, if one prefers positive numbers, $x \equiv 9, 19, 29 \pmod{30}$.

Having considered a single linear congruence, it is natural to turn to the problem of solving a system

$$a_1 x \equiv b_1 \pmod{m_1}, a_2 x \equiv b_2 \pmod{m_2}, \ldots, a_r x \equiv b_r \pmod{m_r}$$

of simultaneous linear congruences. We shall assume that the moduli m_k are relatively prime in pairs. Evidently, the system will admit no solution unless each individual congruence is solvable; that is, unless $d_k \mid b_k$ for each k, where $d_k = \gcd(a_k, m_k)$. When these conditions are satisfied, the factor d_k can be cancelled in the kth congruence to produce a new system (having the same set of solutions as the original one),

$$a_1' x \equiv b_1' \pmod{n_1}, a_2' x \equiv b_2' \pmod{n_2}, \ldots, a_r' x \equiv b_r' \pmod{n_r},$$

where $n_k = m_k/d_k$ and $\gcd(n_i, n_j) = 1$ for $i \neq j$; also, $\gcd(a_i', n_i) = 1$. The solutions of the individual congruences assume the form

$$x \equiv c_1 \pmod{n_1}, \; x \equiv c_2 \pmod{n_2}, \ldots, x \equiv c_r \pmod{n_r}.$$

Thus, the problem is reduced to one of finding a simultaneous solution of a system of congruences of this simpler type.

The kind of problem that can be solved by simultaneous congruences has a long history, appearing in the Chinese literature as early as the first century A.D. Sun-Tsu asked: Find a number which leaves the remainders 2, 3, 2 when divided by 3, 5, 7, respectively. (Such mathematical puzzles are by no means confined to a single cultural sphere; indeed, the same problem occurs in the *Introductio Arithmeticae* of the Greek mathematician Nicomachus, circa 100 A.D.) In honor of their early contributions, the rule for obtaining a solution usually goes by the name of the Chinese Remainder Theorem.

THEOREM 4-8 (Chinese Remainder Theorem). *Let $n_1, n_2, \ldots, n_r$ be positive integers such that* $\gcd(n_i, n_j) = 1$ *for* $i \neq j$. *Then the system of linear congruences*

$$\begin{aligned} x &\equiv a_1 \pmod{n_1}, \\ x &\equiv a_2 \pmod{n_2}, \\ &\vdots \\ x &\equiv a_r \pmod{n_r} \end{aligned}$$

has a simultaneous solution, which is unique modulo $n_1 n_2 \cdots n_r$.

Proof: We start by forming the product $n = n_1 n_2 \cdots n_r$. For each $k = 1, 2, \ldots, r$, let

$$N_k = n/n_k = n_1 \cdots n_{k-1} n_{k+1} \cdots n_r;$$

in other words, N_k is the product of all the integers n_i with the factor n_k omitted. By hypothesis, the n_i are relatively prime in pairs, so that $\gcd(N_k, n_k) = 1$. According to the theory of a single linear congruence, it is therefore possible to solve the congruence $N_k x \equiv 1 \pmod{n_k}$; call the unique solution x_k. Our aim is to prove that the integer

$$\bar{x} = a_1 N_1 x_1 + a_2 N_2 x_2 + \cdots + a_r N_r x_r$$

is a simultaneous solution of the given system.

First, it is to be observed that $N_i \equiv 0 \pmod{n_k}$ for $i \neq k$, since $n_k \mid N_i$ in this case. The result is that

$$\bar{x} = a_1 N_1 x_1 + \cdots + a_r N_r x_r \equiv a_k N_k x_k \pmod{n_k}.$$

But the integer x_k was chosen to satisfy the congruence $N_k x \equiv 1 \pmod{n_k}$, which forces

$$\bar{x} \equiv a_k \cdot 1 \equiv a_k \pmod{n_k}.$$

This shows that a solution to the given system of congruences exists.

As for the uniqueness assertion, suppose that x' is any other integer which satisfies these congruences. Then

$$\bar{x} \equiv a_k \equiv x' \pmod{n_k}, \qquad k = 1, 2, \ldots, r$$

and so $n_k \mid \bar{x} - x'$ for each value of k. Because $\gcd(n_i, n_j) = 1$, Corollary 2 to Theorem 2-5 supplies us with the crucial point that $n_1 n_2 \cdots n_r \mid \bar{x} - x'$; hence, $\bar{x} \equiv x' \pmod{n}$. With this, the Chinese Remainder Theorem is proven.

Example 4-8

The problem posed by Sun-Tsu corresponds to the system of three congruences

$$x \equiv 2 \pmod 3,$$
$$x \equiv 3 \pmod 5,$$
$$x \equiv 2 \pmod 7.$$

In the notation of Theorem 4-8, we have $n = 3 \cdot 5 \cdot 7 = 105$ and

$$N_1 = n/3 = 35, \quad N_2 = n/5 = 21, \quad N_3 = n/7 = 15.$$

Now the linear congruences

$$35x \equiv 1 \pmod 3, \quad 21x \equiv 1 \pmod 5, \quad 15x \equiv 1 \pmod 7$$

are satisfied by $x_1 = 2$, $x_2 = 1$, $x_3 = 1$, respectively. Thus, a solution of the system is given by

$$\bar{x} = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233.$$

Modulo 105, we get the unique solution $\bar{x} = 233 \equiv 23 \pmod{105}$.

Example 4-9

For a second illustration, let us solve the linear congruence

$$17x \equiv 9 \pmod{276}.$$

Since $276 = 3 \cdot 4 \cdot 23$, this is equivalent to finding a solution of the system of congruences

$$\begin{array}{lll} 17x \equiv 9 \pmod 3 & \text{or} & x \equiv 0 \pmod 3 \\ 17x \equiv 9 \pmod 4 & & x \equiv 1 \pmod 4 \\ 17x \equiv 9 \pmod{23} & & 17x \equiv 9 \pmod{23} \end{array}$$

Note that if $x \equiv 0 \pmod 3$, then $x = 3k$ for any integer k. We substitute into the second congruence of the system and obtain

$$3k \equiv 1 \pmod 4.$$

Multiplication of both sides of this congruence by 3 gives us

$$k \equiv 9k \equiv 3 \pmod 4,$$

so that $k = 3 + 4j$, where j is an integer. Then

$$x = 3(3 + 4j) = 9 + 12j.$$

For x to satisfy the last congruence, we must have

$$17(9 + 12j) \equiv 9 \pmod{23}$$

or $204j \equiv -144 \pmod{23}$, which reduces to $3j \equiv 6 \pmod{23}$; that is, $j \equiv 2 \pmod{23}$. This yields $j = 2 + 23t$, t an integer, whence

$$x = 9 + 12(2 + 23t) = 33 + 276t.$$

All in all, $x \equiv 33 \pmod{276}$ provides a solution to the system of congruences and, in turn, a solution to $17x \equiv 9 \pmod{276}$.

PROBLEMS

1. Solve the following linear congruences:
   (a) $25x \equiv 15 \pmod{29}$.
   (b) $5x \equiv 2 \pmod{26}$.
   (c) $6x \equiv 15 \pmod{21}$.
   (d) $36x \equiv 8 \pmod{102}$.
   (e) $34x \equiv 60 \pmod{98}$.
   (f) $140x \equiv 133 \pmod{301}$. [*Hint:* gcd (140, 301) = 7.]
2. Using congruences, solve the Diophantine equations below:
   (a) $4x + 51y = 9$. [*Hint:* $4x \equiv 9 \pmod{51}$ gives $x = 15 + 51t$, while $51y \equiv 9 \pmod{4}$ gives $y = 3 + 4s$. Find the relation between s and t.]
   (b) $12x + 25y = 331$.
   (c) $5x - 53y = 17$.
3. Find all solutions of the linear congruence $3x - 7y \equiv 11 \pmod{13}$.
4. Solve each of the following sets of simultaneous congruences:
   (a) $x \equiv 1 \pmod{3}$, $x \equiv 2 \pmod{5}$, $x \equiv 3 \pmod{7}$
   (b) $x \equiv 5 \pmod{11}$, $x \equiv 14 \pmod{29}$, $x \equiv 15 \pmod{31}$
   (c) $x \equiv 5 \pmod{6}$, $x \equiv 4 \pmod{11}$, $x \equiv 3 \pmod{17}$
   (d) $2x \equiv 1 \pmod{5}$, $3x \equiv 9 \pmod{6}$, $4x \equiv 1 \pmod{7}$, $5x \equiv 9 \pmod{11}$.
5. Solve the linear congruence $17x \equiv 3 \pmod{2 \cdot 3 \cdot 5 \cdot 7}$ by solving the system

$17x \equiv 3 \pmod{2}$, $17x \equiv 3 \pmod{3}$, $17x \equiv 3 \pmod{5}$, $17x \equiv 3 \pmod{7}$.

Possible Questions

2 Mark Questions:

1. Define divisible with example.
2. Prove that if $a|b$ and $a|c$,then $a|(bx+cy)$ for arbitrary integers x and y.
3. Define greatest common divisor with example.
4. What is relatively prime.
5. Discuss about Diophantine equation.
6. Prove that if p is a prime and $p|ab,$ then $p|a$ or $p|b$.
7. State Euclid theorem.
8. Define Linear congruence.
9. Prove if $\gcd(a,n)=1,$ then the linear congruence $ax \equiv b(\mathrm{mod}\, n)$ has a unique solution modulo n.
10. State Chinese Remainder theorem.

8 Mark Questions:

1. Prove that the linear Diophantine equation $ax+by=c$ has a solution if and only if $d|c$,where $d=\gcd(a,b)$. If x_0, y_0 is any particular solution of this equation then all other solutions are given by

$$x = x_0 + (b/d)t, \quad y = y_0 - (a/d)t$$

for varying integers t.

2. Determine all the solutions in the integers of each of the following Diophantine equations:
   a) $56x+72y=40;$
   b) $24x+138y=18;$
   c) $221x+91y=117;$
   d) $84x-438y=156.$

3. Determine all the solutions in the Positive integers of each of the following Diophantine equations:

   a) $30x + 17y = 300;$

   b) $54x + 21y = 906;$

   c) $123x + 360y = 99;$

4. State and prove fundamental theorem of Arithmetic.

5. State and prove Euclid Lemma.

6. Prove that if p_n is the n[th] prime number, then $p_n \le 2^{2^{n-1}}$.

7. Prove that there are infinite number of primes of the form $4n+3$.

8. Prove that the linear congruence $ax \equiv b(\mathrm{mod}\, n)$ has a solution if and only if $d \mid b$, where $d = \gcd(a,n)$. if $d \mid b$, then it has d mutually in-congruent solutions modulo n.

9. State and Prove Chinese Remainder theorem.

10. Solve the following linear congruence:

    a) $25x \equiv 15(\mathrm{mod}\, 29)$ b) $5x \equiv 2(\mathrm{mod}\, 26)$

UNIT-II

SYLLABUS

Fermat's Little theorem, Wilson's theorem. Number theoretic functions, sum and number of divisors, Totally multiplicative functions , Definition and properties of the Dirichlet product.

FERMAT'S FACTORIZATION METHOD

In a fragment of a letter, written in all probability to Father Marin Mersenne in 1643, Fermat described a technique of his for factoring large numbers. This represented the first real improvement over the classical method of attempting to find a factor of n by dividing by all primes not exceeding $\sqrt{n}$. Fermat's factorization scheme has at its heart the observation that the search for factors of an odd integer n (since powers of 2 are easily recognizable and may be removed at the outset, there is no loss in assuming that n is odd) is equivalent to obtaining integral solutions x and y of the equation

$$n = x^2 - y^2.$$

If n is the difference of two squares, then it is apparent that n can be factored as

$$n = x^2 - y^2 = (x + y)(x - y).$$

Conversely, when n has the factorization $n = ab$, with $a \geq b \geq 1$, then we may write

$$n = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2.$$

Moreover, because n is taken to be an odd integer, a and b are themselves odd; hence, $(a + b)/2$ and $(a - b)/2$ will be nonnegative integers.

One begins the search for possible x and y satisfying the equation $n = x^2 - y^2$, or what is the same thing, the equation

$$x^2 - n = y^2$$

by first determining the smallest integer k for which $k^2 \geq n$. Now look successively at the numbers

$$k^2 - n, (k + 1)^2 - n, (k + 2)^2 - n, (k + 3)^2 - n, \ldots$$

until a value of $m \geq \sqrt{n}$ is found making $m^2 - n$ a square. The process cannot go on indefinitely, since we eventually arrive at

$$\left(\frac{n+1}{2}\right)^2 - n = \left(\frac{n-1}{2}\right)^2,$$

the representation of n corresponding to the trivial factorization $n = n \cdot 1$. If this point is reached without a square difference having been discovered earlier, then n has no factors other than n and 1, in which case it is a prime.

Fermat used the procedure just described to factor

$$2027651281 = 44021 \cdot 46061$$

in only 11 steps, as compared to making 4850 divisions by the odd primes up to 44021. This was probably a favorable case devised on purpose to show the chief virtue of his method: it does not require one to know all the primes less than $\sqrt{n}$ in order to find factors of n.

Example 5-1

To illustrate the application of Fermat's method, let us factor the integer $n = 119143$. From a table of squares, we find that $345^2 < 119143 < 346^2$; thus it suffices to consider values of $k^2 - 119143$ for k in the range $346 < k < (119143 + 1)/2 = 59572$. The calculations begin as follows:

$$346^2 - 119143 = 119716 - 119143 = 573,$$
$$347^2 - 119143 = 120409 - 119143 = 1266,$$
$$348^2 - 119143 = 121104 - 119143 = 1961,$$
$$349^2 - 119143 = 121801 - 119143 = 2658,$$
$$350^2 - 119143 = 122500 - 119143 = 3357,$$
$$351^2 - 119143 = 123201 - 119143 = 4058,$$
$$352^2 - 119143 = 123904 - 119143 = 4761 = 69^2.$$

This last line exhibits the factorization

$$119143 = 352^2 - 69^2 = (352 + 69)(352 - 69) = 421 \cdot 283,$$

the two factors themselves being prime. In only seven trials, we have obtained the prime factorization of the number 119143. Of course, one does not always fare so luckily; it may take many steps before a difference turns out to be a square.

Fermat's method is most effective when the two factors of n are of nearly the same magnitude, for in this case a suitable square will appear quickly. To illustrate, let us suppose that $n = 23449$ is to be factored. The smallest square exceeding n is 154^2, so that the sequence $k^2 - n$ starts with

$$154^2 - 23449 = 23716 - 23449 = 267,$$
$$155^2 - 23449 = 24025 - 23449 = 576 = 24^2.$$

Hence, factors of 23449 are

$$23449 = (155 + 24)(155 - 24) = 179 \cdot 131.$$

When examining the differences $k^2 - n$ as possible squares, many values can be immediately excluded by inspection of the final digits. We know, for instance, that a square must end in one of the six digits 0, 1, 4, 5, 6, 9 (Problem 1a, Section 4.3). This allows us to exclude all values in the above example, save for 1266, 1961, and 4761. By calculating the squares of the integers from 0 to 99 modulo 100, one sees further that, for a square, the last two digits are limited to the following twenty-two possibilities:

00	21	41	64	89
01	24	44	69	96
04	25	49	76	
09	29	56	81	
16	36	61	84	

The integer 1266 can be eliminated from consideration in this way. Since 61 is among the last two digits allowable in a square, it is only necessary to look at the numbers 1961 and 4761; the former is not a square, but $4761 = 69^2$.

PROBLEMS

1. Use Fermat's method to factor
   (a) 2279;
   (b) 10541;
   (c) 340663. [*Hint:* The smallest square just exceeding 340663 is 587^2.]
2. Prove that a perfect square must end in one of the following pairs of digits: 00, 01, 04, 09, 16, 21, 24, 25, 29, 36, 41, 44, 49, 56, 61, 64, 69, 76, 81, 84, 89, 96. [*Hint:* Since $x^2 \equiv (50 + x)^2 \pmod{100}$ and $x^2 \equiv (50 - x)^2 \pmod{100}$, it suffices to examine the final digits of x^2 for the 26 values $x = 0, 1, 2, \ldots, 25$.]

THE LITTLE THEOREM

The most significant of Fermat's correspondents in number theory was Bernhard Frénicle de Bessy (1605–1675), an official at the French mint who was renowned for his gift of manipulating large numbers. (Frénicle's facility in numerical calculation is revealed by the following incident: On hearing that Fermat had proposed the problem of finding cubes which when increased by their proper divisors become squares, as is the case with $7^3 + (1 + 7 + 7^2) = 20^2$, he immediately gave four different solutions; and supplied six more the next day.) Though in no way Fermat's equal as a mathematician, Frénicle alone among his contemporaries could challenge him in number theory and his challenges had the distinction of coaxing out of Fermat some of his carefully guarded secrets. One of the most striking is the theorem which states: If p is a prime and a is any integer not divisible by p, then p divides $a^{p-1} - 1$. Fermat communicated the result in a letter to Frénicle dated October 18, 1640, along with the comment, "I would send you the demonstration, if I did not fear its being too long." This theorem has since become known as "Fermat's Little Theorem" to distinguish it from Fermat's "Great" or "Last Theorem," which is the subject of Chapter 11. Almost 100 years were to elapse before Euler published the first proof of the Little Theorem in 1736. Leibniz, however, seems not to have received his share of recognition; for he left an identical argument in an unpublished manuscript sometime before 1683.

THEOREM 5-1 (Fermat's Little Theorem). *If p is a prime and $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.*

Proof: We begin by considering the first $p-1$ positive multiples of a; that is, the integers

$$a, 2a, 3a, \ldots, (p-1)a.$$

None of these numbers is congruent modulo p to any other, nor is any congruent to zero. Indeed, if it happened that

$$ra \equiv sa \pmod{p}, \qquad 1 \leq r < s \leq p-1$$

then a could be cancelled to give $r \equiv s \pmod{p}$, which is impossible. Therefore, the above set of integers must be congruent modulo p to 1, 2, 3, ..., $p-1$, taken in some order. Multiplying all these congruences together, we find that

$$a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p},$$

whence

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}.$$

Once $(p-1)!$ is cancelled from both sides of the preceding congruence (this is possible since $p \nmid (p-1)!$), our line of reasoning culminates in $a^{p-1} \equiv 1 \pmod{p}$, which is Fermat's Theorem.

This result can be stated in a slightly more general way in which the requirement that $p \nmid a$ is dropped.

COROLLARY. *If p is a prime, then $a^p \equiv a \pmod{p}$ for any integer a.*

Proof: When $p \mid a$, the statement obviously holds; for, in this setting, $a^p \equiv 0 \equiv a \pmod{p}$. If $p \nmid a$, then in accordance with Fermat's Theorem, $a^{p-1} \equiv 1 \pmod{p}$. When this congruence is multiplied by a, the conclusion $a^p \equiv a \pmod{p}$ follows.

There is a different proof of the fact that $a^p \equiv a \pmod{p}$, involving induction on a. If $a = 1$, the assertion is that $1^p \equiv 1 \pmod{p}$, which is clearly true, as is the case $a = 0$. Assuming that the result holds for a, we must confirm its validity for $a+1$. In light of the binomial theorem,

$$(a+1)^p = a^p + \binom{p}{1}a^{p-1} + \cdots + \binom{p}{k}a^{p-k} + \cdots + \binom{p}{p-1}a + 1,$$

where the coefficient $\binom{p}{k}$ is given by

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{p(p-1)\cdots(p-k+1)}{1 \cdot 2 \cdot 3 \cdots k}.$$

Our argument hinges on the observation that $\binom{p}{k} \equiv 0 \pmod{p}$ for $1 \leq k \leq p-1$. To see this, note that

$$k!\binom{p}{k} = p(p-1)\cdots(p-k+1) \equiv 0 \pmod{p},$$

by virtue of which $p \mid k!$ or $p \mid \binom{p}{k}$. But $p \mid k!$ implies that $p \mid j$ for some j satisfying $1 \leq j \leq k \leq p-1$, an absurdity. Therefore, $p \mid \binom{p}{k}$ or, converting to a congruence statement,

$$\binom{p}{k} \equiv 0 \pmod{p}.$$

The point which we wish to make is that

$$(a+1)^p \equiv a^p + 1 \equiv a + 1 \pmod{p},$$

where the right-most congruence uses our inductive assumption. Thus, the desired conclusion holds for $a+1$ and, in consequence, for all $a \geq 0$. If a is a negative integer, there is no problem: since $a \equiv r \pmod{p}$ for some r, where $0 \leq r \leq p-1$, we get $a^p \equiv r^p \equiv r \equiv a \pmod{p}$.

Fermat's Theorem has many applications and is central to much of what is done in number theory. On one hand, it can be a labor-saving device in certain calculations. If asked to verify that $5^{38} \equiv 4 \pmod{11}$, for instance, we would take the congruence $5^{10} \equiv 1 \pmod{11}$ as our starting point. Knowing this,

$$\begin{aligned} 5^{38} = 5^{10\cdot 3+8} &= (5^{10})^3(5^2)^4 \\ &\equiv 1^3 \cdot 3^4 \equiv 81 \equiv 4 \pmod{11}, \end{aligned}$$

as desired.

Another use of Fermat's Theorem is as a tool in testing the primality of a given integer n. For, if it could be shown that the congruence

$$a^n \equiv a \pmod{n}$$

fails to hold for some choice of a, then n is necessarily composite. As an example of this approach, let us look at $n = 117$. The computation is kept under control by selecting a small integer for a; say, $a = 2$. Since 2^{117} may we written as

$$2^{117} = 2^{7 \cdot 16 + 5} = (2^7)^{16} 2^5$$

and $2^7 = 128 \equiv 11 \pmod{117}$, we have

$$2^{117} \equiv 11^{16} \cdot 2^5 \equiv (121)^8 \, 2^5 \equiv 4^8 \cdot 2^5 \equiv 2^{21} \pmod{117}.$$

But $2^{21} = (2^7)^3$, which leads to

$$2^{21} \equiv 11^3 \equiv 121 \cdot 11 \equiv 4 \cdot 11 \equiv 44 \pmod{117}.$$

Combining these congruences, we finally obtain

$$2^{117} \equiv 44 \not\equiv 2 \pmod{117},$$

so that 117 must be composite; actually, $117 = 13 \cdot 9$.

It might be worthwhile to give an example illustrating the failure of the converse of Fermat's Theorem to hold; in other words, to show that if $a^{n-1} \equiv 1 \pmod{n}$ for some integer a, then n need not be prime. As a prelude we require a technical lemma:

LEMMA. *If p and q are distinct primes such that $a^p \equiv a \pmod{q}$ and $a^q \equiv a \pmod{p}$, then $a^{pq} \equiv a \pmod{pq}$.*

Proof: It is known from the last corollary that $(a^q)^p \equiv a^q \pmod{p}$, while $a^q \equiv a \pmod{p}$ by hypothesis. Combining these congruences, we obtain $a^{pq} \equiv a \pmod{p}$ or, in different terms, $p \mid a^{pq} - a$. In an entirely similar manner, $q \mid a^{pq} - a$. The corollary to Theorem 2-4 now yields $pq \mid a^{pq} - a$, which can be recast as $a^{pq} \equiv a \pmod{pq}$.

Our contention is that $2^{340} \equiv 1 \pmod{341}$ where $341 = 11 \cdot 31$. In working towards this end, notice that $2^{10} = 1024 = 31 \cdot 33 + 1$. Thus,

$$2^{11} = 2 \cdot 2^{10} \equiv 2 \cdot 1 \equiv 2 \pmod{31}$$

Exploiting the lemma,

$$2^{11 \cdot 31} \equiv 2 \pmod{11 \cdot 31}$$

or $2^{341} \equiv 2 \pmod{341}$. After cancelling a factor of 2, we pass to

$$2^{340} \equiv 1 \pmod{341},$$

so that the converse to Fermat's Theorem is false.

The historical interest in numbers of the form $2^n - 2$ resides in the claim made by the Chinese mathematicians over 25 centuries ago that n is prime if and only if $n \mid 2^n - 2$ (in point of fact, this criterion is reliable for all integers $n \leq 340$). Needless to say, our example, where $341 \mid 2^{341} - 2$ although $341 = 11 \cdot 31$, lays the conjecture to rest; this was discovered in the year 1819. The situation in which $n \mid 2^n - 2$ occurs often enough to merit a name though: call a composite integer n *pseudoprime* whenever $n \mid 2^n - 2$. It can be shown that there are infinitely many pseudoprimes, the smallest four being 341, 561, 645, and 1105.

PROBLEMS

1. Verify that $18^6 \equiv 1 \pmod{7^k}$ for $k = 1, 2, 3$.
2. (a) If $\gcd(a, 35) = 1$, show that $a^{12} \equiv 1 \pmod{35}$. [*Hint:* From Fermat's Theorem $a^6 \equiv 1 \pmod 7$ and $a^4 \equiv 1 \pmod 5$.]
   (b) If $\gcd(a, 42) = 1$, show that $168 = 3 \cdot 7 \cdot 8$ divides $a^6 - 1$.
   (c) If $\gcd(a, 133) = \gcd(b, 133) = 1$, show that $133 \mid a^{18} - b^{18}$.
3. Prove that there exist infinitely many composite numbers n for which $a^{n-1} \equiv a \pmod n$. [*Hint:* Take $n = 2p$, where p is an odd prime.]
4. Derive each of the following congruences:
   (a) $a^{21} \equiv a \pmod{15}$ for all a. [*Hint:* By Fermat's Theorem, $a^5 \equiv a \pmod 5$.]
   (b) $a^7 \equiv a \pmod{42}$ for all a.
   (c) $a^{13} \equiv a \pmod{3 \cdot 7 \cdot 13}$ for all a.

WILSON'S THEOREM

We now turn to another milestone in the development of number theory. In his *Meditationes Algebraicae* of 1770, the English mathematician Edward Waring (1741–1793) announced several new theorems. Foremost among these is an interesting property of primes reported to him by one of his former students, a certain John Wilson. The property is the following: if p is a prime number, then p divides $(p-1)!+1$. Wilson appears to have guessed this on the basis of numerical computations; at any rate, neither he nor Waring knew how to prove it. Confessing his inability to supply a demonstration, Waring added, "Theorems of this kind will be very hard to prove, because of the absence of a notation to express prime numbers." (Reading the passage, Gauss uttered his telling comment on "notationes versus notiones," implying that in questions of this nature it was the notion that really mattered, not the notation.) Despite Waring's pessimistic forecast, Lagrange soon afterwards (1771) gave a proof of what in the literature is called "Wilson's Theorem" and observed that the converse also holds. It would be perhaps more just to name the theorem after Leibniz, for there is evidence that he was aware of the result almost a century earlier, but published nothing upon the subject.

Now to a proof of Wilson's Theorem.

THEOREM 5-2 (Wilson). *If p is a prime, then* $(p-1)! \equiv -1 \pmod{p}$.

Proof: Dismissing the cases $p=2$ and $p=3$ as being evident, let us take $p>3$. Suppose that a is any one of the $p-1$ positive integers

$$1, 2, 3, \ldots, p-1$$

and consider the linear congruence $ax \equiv 1 \pmod{p}$. Then gcd $(a, p)=1$. By Theorem 4-7, this congruence admits a unique solution modulo p; hence, there is a unique integer a', with $1 \leq a' \leq p-1$, satisfying $aa' \equiv 1 \pmod{p}$.

Since p is prime, $a = a'$ if and only if $a = 1$ or $a = p - 1$. Indeed, the congruence $a^2 \equiv 1 \pmod{p}$ is equivalent to $(a - 1) \cdot (a + 1) \equiv 0 \pmod{p}$. Therefore, either $a - 1 \equiv 0 \pmod{p}$, in which case $a = 1$, or $a + 1 \equiv 0 \pmod{p}$, in which case $a = p - 1$.

If we omit the numbers 1 and $p - 1$, the effect is to group the remaining integers $2, 3, \ldots, p - 2$ into pairs a, a', where $a \neq a'$, such that $aa' \equiv 1 \pmod{p}$. When these $(p - 3)/2$ congruences are multiplied together and the factors rearranged, we get

$$2 \cdot 3 \cdots (p - 2) \equiv 1 \pmod{p}$$

or rather

$$(p - 2)! \equiv 1 \pmod{p}.$$

Now multiply by $p - 1$ to obtain the congruence

$$(p - 1)! \equiv p - 1 \equiv -1 \pmod{p},$$

as was to be proved.

A concrete example should help to clarify the proof of Wilson's Theorem. Specifically, let us take $p = 13$. It is possible to divide the integers $2, 3, \ldots, 11$ into $(p - 3)/2 = 5$ pairs each of whose products is congruent to 1 modulo 13. To write these congruences out explicitly:

$$2 \cdot 7 \equiv 1 \pmod{13},$$
$$3 \cdot 9 \equiv 1 \pmod{13},$$
$$4 \cdot 10 \equiv 1 \pmod{13},$$
$$5 \cdot 8 \equiv 1 \pmod{13},$$
$$6 \cdot 11 \equiv 1 \pmod{13}.$$

Multiplving the above congruences gives the result

$$11! = (2 \cdot 7)(3 \cdot 9)(4 \cdot 10)(5 \cdot 8)(6 \cdot 11) \equiv 1 \pmod{13}$$

and so

$$12! \equiv 12 \equiv -1 \pmod{13}.$$

Thus, $(p-1)! \equiv -1 \pmod{p}$, with $p = 13$.

The converse of Wilson's Theorem is also true: If $(n-1)! \equiv -1 \pmod{n}$, then n must be prime. For, if n is not a prime, then n has a divisor d, with $1 < d < n$. Furthermore, since $d \leq n-1$, d occurs as one of the factors in $(n-1)!$, whence $d \mid (n-1)!$. Now we are assuming that $n \mid (n-1)! + 1$, and so $d \mid (n-1)! + 1$ too. The conclusion is that $d \mid 1$, which is nonsense.

Taken together, Wilson's Theorem and its converse provide a necessary and sufficient condition for determining primality; namely, an integer $n > 1$ is prime if and only if $(n-1)! \equiv -1 \pmod{n}$. Unfortunately, this test is of more theoretical than practical interest since as n increases, $(n-1)!$ rapidly becomes unmanageable in size.

We would like to close this chapter with an application of Wilson's Theorem to the study of quadratic congruences. [It is understood that *quadratic congruence* means a congruence of the form $ax^2 + bx + c \equiv 0 \pmod{n}$, with $a \not\equiv 0 \pmod{n}$.]

THEOREM 5-3. *The quadratic congruence* $x^2 + 1 \equiv 0 \pmod{p}$, *where* p *is an odd prime, has a solution if and only if* $p \equiv 1 \pmod{4}$.

Proof: Let a be any solution of $x^2 + 1 \equiv 0 \pmod{p}$, so that $a^2 \equiv -1 \pmod{p}$. Since $p \nmid a$, the outcome of applying Fermat's Theorem is:

$$1 \equiv a^{p-1} \equiv (a^2)^{(p-1)/2} \equiv (-1)^{(p-1)/2} \pmod{p}.$$

The possibility that $p = 4k + 3$ for some k does not arise. If it did, we would have

$$(-1)^{(p-1)/2} = (-1)^{2k+1} = -1;$$

hence $1 \equiv -1 \pmod{p}$. The net result of this is that $p \mid 2$, which is patently false. Therefore, p must be of the form $4k + 1$.

Now for the opposite direction. In the product

$$(p-1)! = 1 \cdot 2 \cdots \frac{p-1}{2} \cdot \frac{p+1}{2} \cdots (p-2)(p-1),$$

we have the congruences

$$\begin{aligned} p - 1 &\equiv -1 \pmod{p}, \\ p - 2 &\equiv -2 \pmod{p}, \\ &\vdots \\ \frac{p+1}{2} &\equiv -\frac{p-1}{2} \pmod{p}. \end{aligned}$$

Rearranging the factors produces

$$\begin{aligned} (p-1)! &\equiv 1 \cdot (-1) \cdot 2 \cdot (-2) \cdots \frac{p-1}{2} \cdot \left(-\frac{p-1}{2}\right) \pmod{p} \\ &\equiv (-1)^{(p-1)/2} \left(1 \cdot 2 \cdots \frac{p-1}{2}\right)^2 \pmod{p}, \end{aligned}$$

since there are $(p-1)/2$ minus signs involved. It is at this point that Wilson's Theorem can be brought to bear; for, $(p-1)! \equiv -1 \pmod{p}$, whence

$$-1 \equiv (-1)^{(p-1)/2} \left[\left(\frac{p-1}{2}\right)!\right]^2 \pmod{p}.$$

If we assume that p is of the form $4k + 1$, then $(-1)^{(p-1)/2} = 1$, leaving us with the congruence

$$-1 \equiv \left[\left(\frac{p-1}{2}\right)!\right]^2 \pmod{p}.$$

The conclusion: $[(p-1)/2]!$ satisfies the quadratic congruence $x^2+1 \equiv 0 \pmod{p}$.

Let us take a look at an actual example; say, the case $p = 13$, which is a prime of the form $4k+1$. Here, we have $(p-1)/2 = 6$ and it is easy to see that

$$6! = 720 \equiv 5 \pmod{13},$$

while

$$5^2 + 1 = 26 \equiv 0 \pmod{13}.$$

Thus the assertion that $[(\frac{1}{2}(p-1))!]^2 + 1 \equiv 0 \pmod{p}$ is correct for $p = 13$.

Wilson's Theorem implies that there exists an infinitude of composite numbers of the form $n!+1$. On the other hand, it is an open question whether $n!+1$ is prime for infinitely many values of n. The only values of n in the range $1 \leq n \leq 100$ for which $n!+1$ is known to be a prime number are $n = 1, 2, 3, 11, 27, 37, 41, 73$, and 77.

PROBLEMS

1. (a) Find the remainder when 15! is divided by 17.
   (b) Find the remainder when 2(26!) is divided by 29. [*Hint:* By Wilson's Theorem, $2(p-3)! \equiv -1 \pmod{p}$ for any odd prime $p > 3$.]
2. Determine whether 17 is a prime by deciding whether or not $16! \equiv -1 \pmod{17}$.
3. Arrange the integers 2, 3, 4, ..., 21 in pairs a and b with the property that $ab \equiv 1 \pmod{23}$.
4. Show that $18! \equiv -1 \pmod{437}$.
5. (a) Prove that an integer $n > 1$ is prime if and only if $(n-2)! \equiv 1 \pmod{n}$.
   (b) If n is a composite integer, show that $(n-1)! \equiv 0 \pmod{n}$, except when $n = 4$.

Number-Theoretic Functions

THE FUNCTIONS τ AND σ

Certain functions are found to be of special importance in connection with the study of the divisors of an integer. Any function whose domain of definition is the set of positive integers is said to be a *number-theoretic (or arithmetic) function.* While the value of a number-theoretic function is not required to be a positive integer or, for that matter, even an integer, most of the number-theoretic functions that we shall encounter are integer-valued. Among the easiest to handle, as well as the most natural, are the functions τ and σ.

DEFINITION 6-1. Given a positive integer n, let $\tau(n)$ denote the number of positive divisors of n and $\sigma(n)$ denote the sum of these divisors.

For an example of these notions, consider $n = 12$. Since 12 has the positive divisors 1, 2, 3, 4, 6, 12, we find that

$$\tau(12) = 6 \quad \text{and} \quad \sigma(12) = 1 + 2 + 3 + 4 + 6 + 12 = 28.$$

For the first few integers,

$$\tau(1) = 1, \tau(2) = 2, \tau(3) = 2, \tau(4) = 3, \tau(5) = 2, \tau(6) = 4, \ldots$$

and

$$\sigma(1) = 1, \sigma(2) = 3, \sigma(3) = 4, \sigma(4) = 7, \sigma(5) = 6, \sigma(6) = 12, \ldots.$$

It is not difficult to see that $\tau(n) = 2$ if and only if n is a prime number; also, $\sigma(n) = n + 1$ and if only if n is a prime.

Before studying the functions τ and σ in more detail, we wish to introduce a notation that will clarify a number of situations later on. It is customary to interpret the symbol

$$\sum_{d|n} f(d)$$

to mean, "Sum the values $f(d)$ as d runs over all the positive divisors of the positive integer n." For instance, we have

$$\sum_{d|20} f(d) = f(1) + f(2) + f(4) + f(5) + f(10) + f(20).$$

With this understanding, τ and σ may be expressed in the form

$$\tau(n) = \sum_{d|n} 1, \quad \sigma(n) = \sum_{d|n} d.$$

The notation $\sum_{d|n} 1$, in particular, says that we are to add together as many 1's as there are positive divisors of n. To illustrate: the integer 10 has the four positive divisors 1, 2, 5, 10, whence

$$\tau(10) = \sum_{d|10} 1 = 1 + 1 + 1 + 1 = 4,$$

while

$$\sigma(10) = \sum_{d|10} d = 1 + 2 + 5 + 10 = 18.$$

Our first theorem makes it easy to obtain the positive divisors of a positive integer n once its prime factorization is known.

THEOREM 6-1. *If $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ is the prime factorization of $n > 1$, then the positive divisors of n are precisely those integers d of the form*

$$d = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r},$$

where $0 \leq a_i \leq k_i$ $(i = 1, 2, \ldots, r)$.

Proof: Note that the divisor $d = 1$ is obtained when $a_1 = a_2 = \cdots = a_r = 0$, and n itself occurs when $a_1 = k_1$, $a_2 = k_2$, $\ldots$, $a_r = k_r$. Suppose that d divides n nontrivially; say $n = dd'$, where $d > 1$, $d' > 1$. Express both d and d' as products of (not necessarily distinct) primes:

$$d = q_1 q_2 \cdots q_s, \qquad d' = t_1 t_2 \cdots t_u,$$

with q_i, t_j prime. Then

$$p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} = q_1 \cdots q_s t_1 \cdots t_u$$

are two prime factorizations of the positive integer n. By the uniqueness of the prime factorization, each prime q_i must be one of the p_j. Collecting the equal primes into a single integral power, we get

$$d = q_1 q_2 \cdots q_s = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r},$$

where the possibility that $a_i = 0$ is allowed.

Conversely, every number $d = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ $(0 \leq a_i \leq k_i)$ turns out to be a divisor of n. For we can write

$$\begin{aligned} n &= p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} \\ &= (p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r})(p_1^{k_1 - a_1} p_2^{k_2 - a_2} \cdots p_r^{k_r - a_r}) \\ &= dd', \end{aligned}$$

with $d' = p_1^{k_1 - a_1} p_2^{k_2 - a_2} \cdots p_r^{k_r - a_r}$ and $k_i - a_i \geq 0$ for each i. Then $d' > 0$ and $d \mid n$.

We put this theorem to work at once.

THEOREM 6-2. *If $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ is the prime factorization of $n > 1$, then*

(a) $\tau(n) = (k_1 + 1)(k_2 + 1) \cdots (k_r + 1)$, *and*

(b) $\sigma(n) = \dfrac{p_1^{k_1+1} - 1}{p_1 - 1} \dfrac{p_2^{k_2+1} - 1}{p_2 - 1} \cdots \dfrac{p_r^{k_r+1} - 1}{p_r - 1}.$

Proof: According to Theorem 6-1, the positive divisors of n are precisely those integers

$$d = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r},$$

where $0 \leq a_i \leq k_i$. There are $k_1 + 1$ choices for the exponent a_1; $k_2 + 1$ choices for a_2, ...; $k_r + 1$ choices for a_r; hence, there are

$$(k_1 + 1)(k_2 + 1) \cdots (k_r + 1)$$

possible divisors of n.

In order to evaluate $\sigma(n)$, consider the product

$$(1 + p_1 + p_1^2 + \cdots + p_1^{k_1})(1 + p_2 + p_2^2 + \cdots + p_2^{k_2}) \cdots (1 + p_r + p_r^2 + \cdots + p_r^{k_r}).$$

Each positive divisor of n appears once and only once as a term in the expansion of this product, so that

$$\sigma(n) = (1 + p_1 + p_1^2 + \cdots + p_1^{k_1}) \cdots (1 + p_r + p_r^2 + \cdots + p_r^{k_r}).$$

Applying the formula for the sum of a finite geometric series to the ith factor on the right-hand side, we get

$$1 + p_i + p_i^2 + \cdots + p_i^{k_i} = \frac{p_i^{k_i+1} - 1}{p_i - 1}.$$

It follows that

$$\sigma(n) = \frac{p_1^{k_1+1} - 1}{p_1 - 1} \frac{p_2^{k_2+1} - 1}{p_2 - 1} \cdots \frac{p_r^{k_r+1} - 1}{p_r - 1}.$$

Corresponding to the $\sum$ notation for sums, a notation for products may be defined using the Greek capital letter "pi." The restriction delimiting the numbers over which the product is to be made is usually put under the $\prod$-sign. Examples are

$$\prod_{1 \le d \le 5} f(d) = f(1)f(2)f(3)f(4)f(5),$$

$$\prod_{d|9} f(d) = f(1)f(3)f(9),$$

$$\prod_{\substack{p|30 \\ p \text{ prime}}} f(d) = f(2)f(3)f(5).$$

With this convention, the conclusion to Theorem 6-2 takes the compact form: if $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ is the prime factorization of $n > 1$, then

$$\tau(n) = \prod_{1 \le i \le r} (k_i + 1)$$

and

$$\sigma(n) = \prod_{1 \le i \le r} \frac{p_i^{k_i+1} - 1}{p_i - 1}$$

Example 6-1

The number $180 = 2^2 \cdot 3^2 \cdot 5$ has

$$\tau(180) = (2+1)(2+1)(1+1) = 18$$

positive divisors. These are integers of the form

$$2^{a_1} \cdot 3^{a_2} \cdot 5^{a_3},$$

where $a_1 = 0, 1, 2$; $a_2 = 0, 1, 2$; $a_3 = 0, 1$. Specifically, we obtain

1, 2, 3, 4, 5, 6, 9, 10, 12, 15, 18, 20, 30, 36, 45, 60, 90, 180.

The sum of these integers is

$$\sigma(180) = \frac{2^3 - 1}{2 - 1} \frac{3^3 - 1}{3 - 1} \frac{5^2 - 1}{5 - 1} = \frac{7}{1} \frac{26}{2} \frac{24}{4} = 7 \cdot 13 \cdot 6 = 546.$$

One of the more interesting properties of the divisor function τ is that the product of the positive divisors of an integer $n > 1$ is equal to $n^{\tau(n)/2}$. It is not difficult to get at this fact: Let d denote an arbitrary

positive divisor of n, so that $n = dd'$ for some d'. As d ranges over all $\tau(d)$ positive divisors of n, $\tau(d)$ such equations occur. Multiplying these together, we get

$$n^{\tau(n)} = \prod_{d|n} d \cdot \prod_{d'|n} d'.$$

But as d runs through the divisors of n, so does d'; hence, $\prod_{d|n} d = \prod_{d'|n} d'$. The situation is now this:

$$n^{\tau(n)} = \left(\prod_{d|n} d\right)^2$$

or equivalently,

$$n^{\tau(n)/2} = \prod_{d|n} d.$$

The reader might (or, at any rate, should) have one lingering doubt concerning this equation. For it is by no means obvious that the left-hand side is always an integer. If $\tau(n)$ is even, there is certainly no problem. When $\tau(n)$ is odd, n turns out to be a perfect square (Problem 7), say $n = m^2$; thus $n^{\tau(n)/2} = m^{\tau(n)}$, settling all suspicions.

For a numerical example, the product of the five divisors of 16 (namely, 1, 2, 4, 8, 16) is

$$\prod_{d|16} d = 16^{\tau(16)/2} = 16^{5/2} = 4^5 = 1024.$$

Multiplicative functions arise naturally in the study of the prime factorization of an integer. Before presenting the definition, we observe that

$$\tau(2 \cdot 10) = \tau(20) = 6 \neq 2 \cdot 4 = \tau(2) \cdot \tau(10).$$

At the same time

$$\sigma(2 \cdot 10) = \sigma(20) = 42 \neq 3 \cdot 18 = \sigma(2) \cdot \sigma(10).$$

These calculations bring out the nasty fact that, in general, it need not be true that

$$\tau(mn) = \tau(m)\tau(n) \quad \text{and} \quad \sigma(mn) = \sigma(m)\sigma(n).$$

On the positive side of the ledger, equality always holds provided we stick to relatively prime m and n. This circumstance is what prompts

DEFINITION 6-2. A number-theoretic function f is said to be *multiplicative* if

$$f(mn) = f(m)f(n)$$

whenever $\gcd(m, n) = 1$.

For simple illustrations of multiplicative functions, one need only consider the functions given by $f(n) = 1$ and $g(n) = n$ for all $n \geq 1$. It follows by induction that if f is multiplicative and $n_1, n_2, \ldots, n_r$ are positive integers which are pairwise relatively prime, then

$$f(n_1 n_2 \cdots n_r) = f(n_1)f(n_2)\cdots f(n_r).$$

Multiplicative functions have one big advantage for us: they are completely determined once their values at prime powers are known. Indeed, if $n > 1$ is a given positive integer, then we can write $n = p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$ in canonical form; since the $p_i^{k_i}$ are relatively prime in pairs, the multiplicative property ensures that

$$f(n) = f(p_1^{k_1})f(p_2^{k_2})\cdots f(p_r^{k_r}).$$

If f is a multiplicative function which does not vanish identically, then there exists an integer n such that $f(n) \neq 0$. But

$$f(n) = f(n \cdot 1) = f(n)f(1).$$

Being nonzero, $f(n)$ may be cancelled from both sides of this equation to give $f(1) = 1$. The point to which we wish to call attention is that $f(1) = 1$ for any multiplicative function not identically zero.

We now establish that τ and σ have the multiplicative property.

THEOREM 6-3. *The functions τ and σ are both multiplicative functions.*

Proof: Let m and n be relatively prime integers. Since the result is trivially true if either m or n is equal to 1, we may assume that $m > 1$ and $n > 1$. If

$$m = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} \quad \text{and} \quad n = q_1^{j_1} q_2^{j_2} \cdots q_s^{j_s}$$

are the prime factorizations of m and n, then, since $\gcd(m, n) = 1$, no p_i can occur among the q_j. It follows that the prime factorization of the product mn is given by

$$mn = p_1^{k_1} \cdots p_r^{k_r} q_1^{j_1} \cdots q_s^{j_s}.$$

Appealing to Theorem 6-2, we obtain

$$\begin{aligned}\tau(mn) &= [(k_1 + 1) \cdots (k_r + 1)][(j_1 + 1) \cdots (j_s + 1)] \\ &= \tau(m)\tau(n).\end{aligned}$$

In a similar fashion, Theorem 6-2 gives

$$\begin{aligned}\sigma(mn) &= \left[\frac{p_1^{k_1+1} - 1}{p_1 - 1} \cdots \frac{p_r^{k_r+1} - 1}{p_r - 1}\right]\left[\frac{q_1^{j_1+1} - 1}{q_1 - 1} \cdots \frac{q_s^{j_s+1} - 1}{q_s - 1}\right] \\ &= \sigma(m)\sigma(n).\end{aligned}$$

Thus, τ and σ are multiplicative functions.

We continue our program by proving a general result on multiplicative functions. This requires a preparatory lemma.

LEMMA. *If $\gcd(m, n) = 1$, then the set of positive divisors of mn consists of all products $d_1 d_2$, where $d_1 \mid n$, $d_2 \mid m$ and $\gcd(d_1, d_2) = 1$; furthermore, these products are all distinct.*

Proof: It is harmless to assume that $m > 1$ and $n > 1$; let $m = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ and $n = q_1^{j_1} q_2^{j_2} \cdots q_s^{j_s}$ be their respective prime factorizations. Inasmuch as the primes $p_1, \ldots, p_r, q_1, \ldots, q_s$ are

all distinct, the prime factorization of mn is

$$mn = p_1^{k_1} \cdots p_r^{k_r} q_1^{j_1} \cdots q_s^{j_s}.$$

Hence, any positive divisor d of mn will be uniquely representable in the form

$$d = p_1^{a_1} \cdots p_r^{a_r} q_1^{b_1} \cdots q_s^{b_s}, \qquad 0 \le a_i \le k_i,\ 0 \le b_i \le j_i.$$

This allows us to write d as $d = d_1 d_2$, where $d_1 = p_1^{a_1} \cdots p_r^{a_r}$ divides m and $d_2 = q_1^{b_1} \cdots q_s^{b_s}$ divides n. Since no p_i is equal to any q_j, we surely have $\gcd(d_1, d_2) = 1$.

A keystone in much of our subsequent work is

THEOREM 6-4. *If f is a multiplicative function and F is defined by*

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

then F is also multiplicative.

Proof: Let m and n be relatively prime positive integers. Then

$$F(mn) = \sum_{d|mn} f(d) = \sum_{\substack{d_1|m \\ d_2|n}} f(d_1 d_2),$$

since every divisor d of mn can be uniquely written as a product of a divisor d_1 of m and a divisor d_2 of n, where $\gcd(d_1, d_2) = 1$. By the definition of a multiplicative function,

$$f(d_1 d_2) = f(d_1) f(d_2).$$

It follows that

$$F(mn) = \sum_{\substack{d_1|m \\ d_2|n}} f(d_1) f(d_2)$$

$$= \left(\sum_{d_1|m} f(d_1)\right)\left(\sum_{d_2|n} f(d_2)\right) = F(m)F(n).$$

It might be helpful to take time out and run through the proof of Theorem 6-4 in a concrete case. Letting $m = 8$ and $n = 3$, we have

$$\begin{aligned}
F(8\cdot 3) &= \sum_{d|24} f(d) \\
&= f(1)+f(2)+f(3)+f(4)+f(6)+f(8)+f(12)+f(24) \\
&= f(1\cdot 1)+f(2\cdot 1)+f(1\cdot 3)+f(4\cdot 1)+f(2\cdot 3)+f(8\cdot 1) \\
&\qquad +f(4\cdot 3)+f(8\cdot 3) \\
&= f(1)f(1)+f(2)f(1)+f(1)f(3)+f(4)f(1)+f(2)f(3)+f(8)f(1) \\
&\qquad +f(4)f(3)+f(8)f(3) \\
&= [f(1)+f(2)+f(4)+f(8)][f(1)+f(3)] \\
&= \sum_{d|8} f(d)\cdot\sum_{d|3} f(d) = F(8)F(3).
\end{aligned}$$

Theorem 6-4 provides a deceptively short way of drawing the conclusion that τ and σ are multiplicative.

COROLLARY. *The functions τ and σ are multiplicative functions.*

Proof: We have mentioned before that the constant function $f(n) = 1$ is multiplicative, as is the identity function $f(n) = n$. Since τ and σ may be represented in the form

$$\tau(n) = \sum_{d|n} 1 \qquad \text{and} \qquad \sigma(n) = \sum_{d|n} d,$$

the stated result follows immediately from Theorem 6-4.

PROBLEMS

1. Let m and n be positive integers and $p_1, p_2, \ldots, p_r$ be the distinct primes which divide at least one of m or n. Then m and n may be written in the form

$$m = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}, \qquad \text{with } k_i \geq 0 \text{ for } i = 1, 2, \ldots, r$$

$$n = p_1^{j_1} p_2^{j_2} \cdots p_r^{j_r}, \qquad \text{with } j_i \geq 0 \text{ for } i = 1, 2, \ldots, r$$

Prove that

$$\gcd(m, n) = p_1^{u_1} p_2^{u_2} \cdots p_r^{u_r}, \quad \operatorname{lcm}(m, n) = p_1^{v_1} p_2^{v_2} \cdots p_r^{v_r},$$

where $u_i = \min\{k_i, j_i\}$, the smaller of k_i and j_i; and $v_i = \max\{k_i, j_i\}$, the larger of k_i and j_i.

2. Use Problem 1 to calculate gcd (12378, 3054) and lcm (12378, 3054).

3. Deduce from Problem 1 that $\gcd(m, n) \operatorname{lcm}(m, n) = mn$ for positive integers m and n.

4. In the notation of Problem 1, show that $\gcd(m, n) = 1$ if and only if $k_i j_i = 0$ for $i = 1, 2, \ldots, r$.

5. (a) Verify that $\tau(n) = \tau(n+1) = \tau(n+2) = \tau(n+3)$ holds for $n = 3655$ and 4503.

(b) When $n = 14$, 206, and 957, show that $\sigma(n) = \sigma(n+1)$.

Possible Questions

2 Mark Questions:

1. What is Fermat's Factorization method.
2. Prove that if p is a prime, then $a^p \equiv a(\text{mod } p)$ for any integer a.
3. Verify that $18^6 \equiv 1(\text{mod } 7^k)$ for $k = 1,2,3.$
4. Find the remainder when $15!$ is divided by 17.
5. Write about $\tau(n)$ and $\sigma(n)$ with example.
6. What is multiplicative function.
7. Prove that if f is a multiplicative function and F is defined by

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

then F is also multiplicative.

8. Define Dirichlet Product.
9. Find the remainder when 5^{11} is divided by 7.
10. Use Fermat's method to factor 23449.

8 Mark Questions:

1. State and prove Fermat's Little theorem.
2. Prove that if p and q are distinct primes such that $a^p \equiv a(\text{mod } q)$ and $a^q \equiv a(\text{mod } p)$, then $a^{pq} \equiv a(\text{mod } pq)$.
3. State and prove Wilson's theorem.
4. Prove that the quadratic congruence $x^2 + 1 \equiv 0(\text{mod } p)$, where p is an odd prime, has a solution if and only if $p \equiv 1(\text{mod } 4).$

5. Prove that if $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ is the prime factorization of $n > 1$, then the positive divisors of n are precisely those integers d of the form

$$d = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r},$$

where $0 \le a_i \le k_i (i = 1,2,\dots,r)$.

6. Prove that if $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ is the prime factorization of $n > 1$, then

a) $\tau(n) = (k_1 + 1)(k_2 + 1)\dots(k_r + 1)$, and

b) $\sigma(n) = \dfrac{p_1^{k_1+1} - 1}{p_1 - 1} \dfrac{p_2^{k_2+1} - 1}{p_2 - 1} \dots \dfrac{p_r^{k_r+1} - 1}{p_r - 1}$.

7. Prove that the function τ and σ are both multiplicative functions.

8. Prove that if $\gcd(m,n) = 1$, then the set of positive divisors of mn consists of all products $d_1 d_2$, where $d_1 | n, d_2 | m$ and $\gcd(d_1, d_2) = 1$; furthermore, these products are all distinct.

9. Discuss about Dirichlet Product.

10. Find the remainder when 72^{1001} is divisible by 31.

11. Prove that the quadratic congruence $x^2 \equiv -1 (\mathrm{mod}\, p)$, p is a prime, has a solution if and only if $p \equiv 1 (\mathrm{mod}\, 4)$.

UNIT-III

SYLLABUS

The Mobius Inversion formula, the greatest integer function, Euler's phi-function, Euler's theorem reduced set of residues-some properties of Euler's phi-function.

THE MÖBIUS INVERSION FORMULA

We introduce another naturally defined function on the positive integers, the Möbius μ-function.

DEFINITION 6-3. For a positive integer n, define μ by the rules

$$\mu(n) = \begin{cases} 1 \text{ if } n = 1 \\ 0 \text{ if } p^2 \mid n \text{ for some prime } p \\ (-1)^r \text{ if } n = p_1 p_2 \cdots p_r, \text{ where the } p_i \text{ are distinct primes} \end{cases}$$

Put somewhat differently, Definition 6-3 states that $\mu(n) = 0$ if n is not a square-free integer, while $\mu(n) = (-1)^r$ if n is square-free with r prime factors. For example: $\mu(30) = \mu(2 \cdot 3 \cdot 5) = (-1)^3 = -1$. The first few values of μ are

$$\mu(1) = 1, \mu(2) = -1, \mu(3) = -1, \mu(4) = 0, \mu(5) = -1, \mu(6) = 1, \ldots .$$

If p is a prime number, it is clear that $\mu(p) = -1$; also, $\mu(p^k) = 0$ for $k \geq 2$.

As the reader may have guessed already, the Möbius μ-function is multiplicative. This is the content of

THEOREM 6-5. *The function μ is a multiplicative function.*

Proof: We want to show that $\mu(mn) = \mu(m)\mu(n)$, whenever m and n are relatively prime. If either $p^2 \mid m$ or $p^2 \mid n$, p a prime, then $p^2 \mid mn$; hence, $\mu(mn) = 0 = \mu(m)\mu(n)$, and the formula holds trivially. We may therefore assume that both m and n are square-free integers. Say, $m = p_1 p_2 \cdots p_r$, $n = q_1 q_2 \cdots q_s$, the primes p_i and q_j being all distinct. Then

$$\begin{aligned} \mu(mn) = \mu(p_1 \cdots p_r q_1 \cdots q_s) &= (-1)^{r+s} \\ &= (-1)^r (-1)^s = \mu(m)\mu(n), \end{aligned}$$

which completes the proof.

Let us see what happens if $\mu(d)$ is evaluated for all the positive divisors d of an integer n and the results added. In case $n = 1$, the answer is easy; here,

$$\sum_{d|1} \mu(d) = \mu(1) = 1.$$

Suppose that $n > 1$ and put

$$F(n) = \sum_{d|n} \mu(d).$$

To prepare the ground, we first calculate $F(n)$ for the power of a prime, say, $n = p^k$. The positive divisors of p^k are just the $k+1$ integers $1, p, p^2, \ldots, p^k$, so that

$$\begin{aligned} F(p^k) = \sum_{d|p^k} \mu(d) &= \mu(1) + \mu(p) + \mu(p^2) + \cdots + \mu(p^k) \\ &= \mu(1) + \mu(p) = 1 + (-1) = 0. \end{aligned}$$

Since μ is known to be a multiplicative function, an appeal to Theorem 6-4 is legitimate; this result guarantees that F is multiplicative too. Thus, if the canonical factorization of n is $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, then $F(n)$ is the product of the values assigned to F for the prime powers in this representation:

$$F(n) = F(p_1^{k_1}) F(p_2^{k_2}) \cdots F(p_r^{k_r}) = 0.$$

THEOREM 6-6. *For each positive integer $n \geq 1$,*

$$\sum_{d|n} \mu(d) = \begin{cases} 1 \text{ if } n = 1 \\ 0 \text{ if } n > 1 \end{cases}$$

where d runs through the positive divisors of n.

For an illustration of this last theorem, consider $n = 10$. The divisors of 10 are 1, 2, 5, 10 and the desired sum is

$$\sum_{d|10} \mu(d) = \mu(1) + \mu(2) + \mu(5) + \mu(10)$$

$$= 1 + (-1) + (-1) + 1 = 0.$$

The full significance of Möbius' function should become apparent with the next theorem.

THEOREM 6-7 (Möbius Inversion Formula). *Let F and f be two number-theoretic functions related by the formula*

$$F(n) = \sum_{d|n} f(d).$$

Then

$$f(n) = \sum_{d|n} \mu(d)F(n/d) = \sum_{d|n} \mu(n/d)F(d).$$

Proof: The two sums mentioned in the conclusion of the theorem are seen to be the same upon replacing the dummy index d by $d' = n/d$; as d ranges over all positive divisors of n, so does d'.

Carrying out the required computation, we get

$$(1) \quad \sum_{d|n} \mu(d)F(n/d) = \sum_{d|n} \left(\mu(d) \sum_{c|(n/d)} f(c) \right) = \sum_{d|n} \left(\sum_{c|(n/d)} \mu(d)f(c) \right).$$

It is easily verified that $d \mid n$ and $c \mid (n/d)$ if and only if $c \mid n$ and $d \mid (n/c)$. Because of this, the last expression in (1) becomes

$$(2) \quad \sum_{d|n} \left(\sum_{c|(n/d)} \mu(d)f(c) \right) = \sum_{c|n} \left(\sum_{d|(n/c)} f(c)\mu(d) \right)$$
$$= \sum_{c|n} \left(f(c) \sum_{d|(n/c)} \mu(d) \right).$$

In compliance with Theorem 6-6, the sum $\sum_{d|(n/c)} \mu(d)$ must vanish except when $n/c = 1$ (that is, when $n = c$), in which case it is equal to 1; the upshot is that the right-hand side of (2) simplifies to

$$\sum_{c|n} \left(f(c) \sum_{d|(n/c)} \mu(d) \right) = \sum_{c=n} f(c) \cdot 1 = f(n),$$

giving us the stated result.

Let us use $n = 10$ again to illustrate how the double sum in (2) is turned around. In this instance, we find that

$$\begin{aligned}\sum_{d|10}\left(\sum_{c|(10/d)}\mu(d)f(c)\right) &= \mu(1)[f(1)+f(2)+f(5)+f(10)]\\ &\quad+\mu(2)[f(1)+f(5)]+\mu(5)[f(1)+f(2)]+\mu(10)f(1)\\ &= f(1)[\mu(1)+\mu(2)+\mu(5)+\mu(10)]\\ &\quad+f(2)[\mu(1)+\mu(5)]+f(5)[\mu(1)+\mu(2)]+f(10)\mu(1)\\ &= \sum_{c|10}\left(\sum_{d|(10/c)}f(c)\mu(d)\right).\end{aligned}$$

To see how Möbius inversion works in a particular case, we remind the reader that the functions τ and σ may both be described as "sum functions":

$$\tau(n) = \sum_{d|n} 1 \quad \text{and} \quad \sigma(n) = \sum_{d|n} d.$$

Theorem 6-7 tells us that these formulas may be inverted to give

$$1 = \sum_{d|n}\mu(n/d)\tau(d) \quad \text{and} \quad n = \sum_{d|n}\mu(n/d)\sigma(d),$$

valid for all $n \geq 1$.

Theorem 6-4 insures that if f is a multiplicative function, then so is $F(n) = \sum_{d|n} f(d)$. Turning the situation around, one might ask whether the multiplicative nature of F forces that of f. Surprisingly enough, this is exactly what happens.

THEOREM 6-8. *If F is a multiplicative function and*

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

then f is also multiplicative.

Proof: Let m and n be relatively prime positive integers. We recall that any divisor d of mn can be uniquely written as $d = d_1 d_2$, where $d_1 \mid m$, $d_2 \mid n$, and $\gcd(d_1, d_2) = 1$. Thus, using the inversion formula,

$$f(mn) = \sum_{d|mn} \mu(d)F\left(\frac{mn}{d}\right)$$

$$= \sum_{\substack{d_1|m \\ d_2|n}} \mu(d_1 d_2)F\left(\frac{mn}{d_1 d_2}\right)$$

$$= \sum_{\substack{d_1|m \\ d_2|n}} \mu(d_1)\mu(d_2)F\left(\frac{m}{d_1}\right) F\left(\frac{n}{d_2}\right)$$

$$= \sum_{d_1|m} \mu(d_1)F\left(\frac{m}{d_1}\right)\sum_{d_2|n} \mu(d_2)F\left(\frac{n}{d_2}\right) = f(m)f(n),$$

which is the assertion of the theorem. Needless to say, the multiplicative character of μ and of F is crucial to the above calculation.

PROBLEMS

1. (a) For each positive integer n, show that

$$\mu(n)\mu(n+1)\mu(n+2)\mu(n+3) = 0.$$

(b) For any integer $n \geq 3$, show that $\sum_{k=1}^{n} \mu(k!) = 1$.

2. The *Mangoldt function* Λ is defined by

$$\Lambda(n) = \begin{cases} \log p, \text{ if } n = p^k, \text{ where } p \text{ is a prime and } k \geq 1 \\ 0, \text{ otherwise} \end{cases}$$

Prove that $\Lambda(n) = \sum_{d|n} \mu(n/d) \log d = -\sum_{d|n} \mu(d) \log d$. [*Hint:* First show that $\sum_{d|n} \Lambda(d) = \log n$ and then apply the Möbius Inversion Formula.]

3. Let $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ be the prime factorization of the integer $n > 1$. If f is a multiplicative function, prove that

$$\sum_{d|n} \mu(d)f(d) = (1 - f(p_1))(1 - f(p_2)) \cdots (1 - f(p_r)).$$

[*Hint:* By Theorem 6-4, the function F defined by $F(n) = \sum_{d|n} \mu(d)f(d)$ is multiplicative; hence, $F(n)$ is the product of the values $F(p_i^{k_i})$.]

THE GREATEST INTEGER FUNCTION

The greatest integer or "bracket" function [ ] is especially suitable for treating divisibility problems. While not strictly a number-theoretic function, its study has a natural place in this chapter.

DEFINITION 6-4. For an arbitrary real number x, we denote by $[x]$ the largest integer less than or equal to x; that is, $[x]$ is the unique integer satisfying $x-1<[x]\leq x$.

By way of illustration, [ ] assumes the particular values

$$[-3/2]=-2,\ [\sqrt{2}]=1,\ [1/3]=0,\ [\pi]=3,\ [-\pi]=-4.$$

The important observation to be made here is that the equality $[x]=x$ holds if and only if x is an integer. Definition 6-4 also makes plain that any real number x can be written as

$$x=[x]+\theta$$

for a suitable choice of θ, with $0\leq\theta<1$.

We now plan to investigate the question of how many times a particular prime p appears in $n!$. For instance, if $p=3$ and $n=9$, then

$$\begin{aligned}9!&=1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6\cdot 7\cdot 8\cdot 9\\&=2^7\cdot 3^4\cdot 5\cdot 7,\end{aligned}$$

so that the exact power of 3 which divides 9! is 4. It is desirable to have a formula that will give this count, without the necessity of always writing $n!$ in canonical form.

THEOREM 6-9. *If n is a positive integer and p a prime, then the exponent of the highest power of p that divides $n!$ is*

$$\sum_{k=1}^{\infty}[n/p^k].$$

(This is not an infinite series, since $[n/p^k] = 0$ *for* $p^k > n$.)

Proof: Among the first n positive integers, those which are divisible by p are $p, 2p, \ldots, tp$, where t is the largest integer such that $tp \leq n$; in other words, t is the largest integer less than or equal to n/p (which is to say $t = [n/p]$). Thus, there are exactly $[n/p]$ multiples of p occurring in the product that defines $n!$, namely,

$$p, 2p, \ldots, [n/p]p. \tag{1}$$

The exponent of p in the prime factorization of $n!$ is obtained by adding to the number of integers in (1), the number of integers among $1, 2, \ldots, n$ which are divisible by p^2, and then the number divisible by p^3, and so on. Reasoning as in the first paragraph, the integers between 1 and n that are divisible by p^2 are

$$p^2, 2p^2, \ldots, [n/p^2]p^2, \tag{2}$$

which are $[n/p^2]$ in number. Of these, $[n/p^3]$ are again divisible by p:

$$p^3, 2p^3, \ldots, [n/p^3]p^3. \tag{3}$$

After a finite number of repetitions of this process, we are led to conclude that the total number of times p divides $n!$ is $\sum_{k=1}^{\infty} [n/p^k]$.

This result can be cast as the following equation, which usually appears under the name of Legendre's formula:

$$n! = \prod_{p \leq n} p^{\sum_{k=1}^{\infty} [n/p^k]}.$$

Example 6-2

We would like to find the number of zeroes with which the decimal representation of 50! terminates. In determining the number of times 10 enters into the product 50!, it is enough to find the exponents of

10 enters into the product 50!, it is enough to find the exponents of 2 and 5 in the prime factorization of 50!, and then to select the smaller figure.

By direct calculation we see that

$$[50/2] + [50/2^2] + [50/2^3] + [50/2^4] + [50/2^5]$$
$$= 25 + 12 + 6 + 3 + 1 = 47.$$

Theorem 6-9 tells us that 2^{47} divides 50!, but 2^{48} does not. Similarly,

$$[50/5] + [50/5^2] = 10 + 2 = 12$$

and so the highest power of 5 dividing 50! is 12. This means that 50! ends with 12 zeroes.

THEOREM 6-10. *If n and r are positive integers with $1 \leq r < n$, then the binomial coefficient*

$$\binom{n}{r} = \frac{n!}{r!(n-r)!}$$

is also an integer.

Proof: The argument rests on the observation that if a and b are arbitrary real numbers, then $[a+b] \geq [a] + [b]$. In particular, for each prime factor of p of $r!\,(n-r)!$,

$$[n/p^k] \geq [r/p^k] + [(n-r)/p^k], \qquad k = 1, 2, \ldots .$$

Adding these inequalities together, we obtain

$$(1) \qquad \sum_{k\geq 1} [n/p^k] \geq \sum_{k\geq 1} [r/p^k] + \sum_{k\geq 1} [(n-r)/p^k].$$

The left-hand side of (1) gives the exponent of the highest power of the prime p that divides $n!$, whereas the right-hand side equals the highest power of this prime contained in $r!(n-r)!$. Hence, p

appears in the numerator of $n!/r!(n-r)!$ at least as many times as it occurs in the denominator. Since this holds true for every prime divisor of the denominator, $r!(n-r)!$ must divide $n!$, making $n!/r!(n-r)!$ an integer.

COROLLARY. *For a positive integer r, the product of any r consecutive positive integers is divisible by $r!$.*

Proof: The product of r consecutive positive integers, the largest of which is n, is

$$n(n-1)(n-2)\cdots(n-r+1).$$

Now we have

$$n(n-1)\cdots(n-r+1)=\left(\frac{n!}{r!(n-r)!}\right)r!.$$

Since $n!/r!(n-r)!$ is an integer, it follows that $r!$ must divide the product $n(n-1)\cdots(n-r+1)$, as asserted.

We pick up a few loose threads. Having introduced the greatest integer function, let us see what it has to do with the study of number-theoretic functions. Their relationship is brought out by

THEOREM 6-11. *Let f and F be number-theoretic functions such that*

$$F(n)=\sum_{d|n} f(d).$$

Then, for any positive integer N,

$$\sum_{n=1}^{N} F(n)=\sum_{k=1}^{N} f(k)[N/k].$$

Proof: We begin by noting that

$$\sum_{n=1}^{N} F(n)=\sum_{n=1}^{N}\sum_{d|n} f(d). \tag{1}$$

The strategy is to collect terms with equal values of $f(d)$ in this double sum. For a fixed positive integer $k \leq N$, the term $f(k)$ appears in $\sum_{d|n} f(d)$ if and only if k is a divisor of n. (Since each integer has itself as a divisor, the right-hand side of (1) includes $f(k)$, at least once.) Now, in order to calculate the number of sums $\sum_{d|n} f(d)$ in which $f(k)$ occurs as a term, it is sufficient to find the number of integers among 1, 2, ..., N which are divisible by k. There are exactly $[N/k]$ of them:

$$k, 2k, 3k, \ldots, [N/k]k.$$

Thus, for each k such that $1 \leq k \leq N$, $f(k)$ is a term of the sum $\sum_{d|n} f(d)$ for $[N/k]$ different positive integers less than or equal to N. Knowing this, we may rewrite the double sum in (1) as

$$\sum_{n=1}^{N} \sum_{d|n} f(d) = \sum_{k=1}^{N} f(k)[N/k]$$

and our task is complete.

As an immediate application of Theorem 6-11, we deduce

COROLLARY 1. *If N is a positive integer, then*

$$\sum_{n=1}^{N} \tau(n) = \sum_{n=1}^{N} [N/n].$$

Proof: Noting that $\tau(n) = \sum_{d|n} 1$, we may write τ for F and take f to be the constant function $f(n) = 1$ for all n.

In the same way, the relation $\sigma(n) = \sum_{d|n} d$ yields

COROLLARY 2. *If N is a positive integer, then*

$$\sum_{n=1}^{N} \sigma(n) = \sum_{n=1}^{N} n[N/n].$$

Example 6-3

Consider the case $N = 6$. The results on page 110 tell us that

$$\sum_{n=1}^{6} \tau(n) = 14.$$

From Corollary 1,

$$\sum_{n=1}^{6} [6/n] = [6] + [3] + [2] + [3/2] + [6/5] + [1]$$
$$= 6 + 3 + 2 + 1 + 1 + 1 = 14,$$

as it should. In the present case, we also have

$$\sum_{n=1}^{6} \sigma(n) = 33,$$

while a simple calculation leads to

$$\sum_{n=1}^{6} n[6/n] = 1[6] + 2[3] + 3[2] + 4[3/2] + 5[6/5] + 6[1]$$
$$= 1 \cdot 6 + 2 \cdot 3 + 3 \cdot 2 + 4 \cdot 1 + 5 \cdot 1 + 6 \cdot 1 = 33.$$

PROBLEMS

1. Given integers a and $b > 0$, show that there exists a unique integer r with $0 \leq r < b$ satisfying $a = [a/b]b + r$.

2. Let x and y be real numbers. Prove that the greatest integer function satisfies the following properties:
   (a) $[x + n] = [x] + n$ for any integer n.
   (b) $[x] + [-x] = 0$ or -1, according as x is an integer or not. [*Hint:* Write $x = [x] + \theta$, with $0 \leq \theta < 1$, so $-x = -[x] - 1 + (1 - \theta)$.]
   (c) $[x] + [y] \leq [x + y]$ and, when x and y are positive, $[x][y] \leq [xy]$.
   (d) $[x/n] = [[x]/n]$ for any positive integer n. [*Hint:* Let $x/n = [x/n] + \theta$, where $0 \leq \theta < 1$; then $[x] = n[x/n] + [n\theta]$.]
   (e) $[nm/k] \geq n[m/k]$ for positive integers n, m, k.
   (f) $[x] + [y] + [x + y] \leq [2x] + [2y]$. [*Hint:* Let $x = [x] + \theta$, $0 \leq \theta < 1$, and $y = [y] + \theta'$, $0 \leq \theta' < 1$. Consider cases in which neither, one, or both of θ and θ' are greater than $\frac{1}{2}$.]

EULER'S PHI-FUNCTION

The present chapter deals with that part of the theory arising out of the result known as Euler's Generalization of Fermat's Theorem. In a nutshell, Euler extended Fermat's Theorem, which concerns congruences with prime moduli, to arbitrary moduli. While doing so, he introduced an important number-theoretic function, described as follows:

DEFINITION 7-1. For $n \geq 1$, let $\phi(n)$ denote the number of positive integers not exceeding n that are relatively prime to n.

As an illustration of the definition, we find that $\phi(30) = 8$; for, among the positive integers that do not exceed 30, there are eight which are relatively prime to 30; specifically

$$1, 7, 11, 13, 17, 19, 23, 29.$$

Similarly, for the first few positive integers, the reader may check that

$$\phi(1) = 1,\ \phi(2) = 1,\ \phi(3) = 2,\ \phi(4) = 2,\ \phi(5) = 4,\ \phi(6) = 2,\ \phi(7) = 6, \ldots.$$

Notice that $\phi(1) = 1$, since $\gcd(1, 1) = 1$. While if $n > 1$, then $\gcd(n, n) = n \neq 1$, so that $\phi(n)$ can be characterized as the number of integers less than n and relatively prime to it. The function ϕ is usually called the *Euler phi-function* (sometimes, the *indicator* or *totient*) after its originator; the functional notation $\phi(n)$, however, is credited to Gauss.

If n is a prime number, then every integer less than n is relatively prime to it; whence, $\phi(n) = n - 1$. On the other hand, if $n > 1$ is composite, then n has a divisor d such that $1 < d < n$. It follows that there are at least two integers among $1, 2, 3, \ldots, n$ which are not relatively prime to n, namely, d and n itself. As a result, $\phi(n) \leq n - 2$. This proves: for $n > 1$,

$$\phi(n) = n - 1 \text{ if and only if } n \text{ is prime.}$$

The first item on the agenda is to derive a formula that will allow us to calculate the value of $\phi(n)$ directly from the prime-power factorization of n.

THEOREM 7-1. *If p is a prime and $k > 0$, then*

$$\phi(p^k) = p^k - p^{k-1} = p^k(1 - 1/p).$$

Proof: Clearly, $\gcd(n, p^k) = 1$ if and only if $p \nmid n$. There are p^{k-1} integers between 1 and p^k which are divisible by p, namely

$$p, 2p, 3p, \ldots, (p^{k-1})p.$$

Thus, the set $\{1, 2, \ldots, p^k\}$ contains exactly $p^k - p^{k-1}$ integers which are relatively prime to p^k and so, by the definition of the phi-function, $\phi(p^k) = p^k - p^{k-1}$.

For an example, we have

$$\phi(9) = \phi(3^2) = 3^2 - 3 = 6;$$

the six integers less than and relatively prime to 9 are 1, 2, 4, 5, 7, 8. To give a second illustration, there are 8 integers which are less than 16 and relatively prime to it, to wit, 1, 3, 5, 7, 9, 11, 13, 15. Theorem 7-1 yields the same count:

$$\phi(16) = \phi(2^4) = 2^4 - 2^3 = 16 - 8 = 8.$$

We now know how to evaluate the phi-function for prime powers and our aim is to obtain a formula for $\phi(n)$ based on the factorization of n as a product of primes. The missing link in the chain is obvious: show that ϕ is a multiplicative function. We pave the way with an easy lemma.

LEMMA. *Given integers a, b, c, $\gcd(a, bc) = 1$ if and only if $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$.*

Proof: Suppose first that $\gcd(a, bc) = 1$ and put $d = \gcd(a, b)$. Then $d \mid a$ and $d \mid b$, whence $d \mid a$ and $d \mid bc$. This implies that $\gcd(a, bc) \geq d$, which forces $d = 1$. Similar reasoning gives rise to the statement $\gcd(a, c) = 1$.

For the other direction, let $\gcd(a, b) = 1 = \gcd(a, c)$ and assume that $\gcd(a, bc) = d_1 > 1$. Then d_1 must have a prime divisor p. Since $d_1 \mid bc$, it follows that $p \mid bc$; in consequence, $p \mid b$ or $p \mid c$. If $p \mid b$, then (by virtue of the fact that $p \mid a$) $\gcd(a, b) \geq p$, a contradiction. In the same way, the condition $p \mid c$ leads to the equally false conclusion that $\gcd(a, c) \geq p$. Thus $d_1 = 1$ and the lemma is proven.

THEOREM 7-2. *The function ϕ is a multiplicative function.*

Proof: It is required to show that $\phi(mn) = \phi(m)\phi(n)$, whenever m and n have no common factor. Since $\phi(1) = 1$, the result obviously holds if either m or n equals 1. Thus we may assume that $m > 1$ and $n > 1$. Arrange the integers from 1 to mn in m columns of n integers each, as follows:

$$\begin{array}{cccccc} 1 & 2 & \cdots & r & \cdots & m \\ m+1 & m+2 & & m+r & & 2m \\ 2m+1 & 2m+2 & & 2m+r & & 3m \\ \vdots & \vdots & & \vdots & & \vdots \\ (n-1)m+1 & (n-1)m+2 & & (n-1)m+r & & nm \end{array}$$

We know that $\phi(mn)$ is equal to the number of entries in the above array which are relatively prime to mn; by virtue of the lemma, this is the same as the number of integers which are relatively prime to both m and n.

Before embarking on the details, it is worth commenting on the tactics to be adopted: Since $\gcd(qm + r, m) = \gcd(r, m)$, the numbers in the rth column are relatively prime to m if and only if r itself is relatively prime to m. Therefore, only $\phi(m)$ columns contain integers relatively prime to m, and every entry in the column will be relatively prime to m. The problem is one of showing that in each of these $\phi(m)$ columns there are exactly $\phi(n)$ integers which are relatively prime to n; for then there would be altogether $\phi(m)\phi(n)$ numbers in the table which are relatively prime to both m and n.

Now the entries in the rth column (where it is assumed that $\gcd(r, m) = 1$) are

$$r, m + r, 2m + r, \ldots, (n - 1)m + r.$$

There are n integers in this sequence and no two are congruent modulo n. Indeed, were

$$km + r \equiv jm + r \pmod{n}$$

with $0 \leq k < j < n$, it would follow that $km \equiv jm \pmod{n}$. Since $\gcd(m, n) = 1$, we could cancel m from both sides of this congruence to arrive at the contradiction that $k \equiv j \pmod{n}$. Thus, the numbers in the rth column are congruent modulo n to $0, 1, 2, \ldots, n - 1$, in some order. But if $s \equiv t \pmod{n}$, then $\gcd(s, n) = 1$ if and only if $\gcd(t, n) = 1$. The implication is that the rth column contains as many integers which are relatively prime to n as does the set $\{0, 1, 2, \ldots, n - 1\}$, namely, $\phi(n)$ integers. Therefore, the total number of entries in the array that are relatively prime to both m and n is $\phi(m)\phi(n)$. This completes the proof of the theorem.

THEOREM 7-3. *If the integer $n > 1$ has the prime factorization $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, then*

$$\begin{aligned}\phi(n) &= (p_1^{k_1} - p_1^{k_1 - 1})(p_2^{k_2} - p_2^{k_2 - 1}) \cdots (p_r^{k_r} - p_r^{k_r - 1}) \\ &= n(1 - 1/p_1)(1 - 1/p_2) \cdots (1 - 1/p_r).\end{aligned}$$

Proof: We intend to use induction on r, the number of distinct prime factors of n. By Theorem 7-1, the result is true for $r = 1$. Suppose that it holds for $r = i$. Since

$$\gcd(p_1^{k_1} p_2^{k_2} \cdots p_i^{k_i}, p_{i+1}^{k_{i+1}}) = 1,$$

the definition of multiplicative function gives

$$\phi((p_1^{k_1}\cdots p_i^{k_i})p_{i+1}^{k_{i+1}}) = \phi(p_1^{k_1}\cdots p_i^{k_i})\phi(p_{i+1}^{k_{i+1}})$$
$$= \phi(p_1^{k_1}\cdots p_i^{k_i})(p_{i+1}^{k_{i+1}} - p_{i+1}^{k_{i+1}-1}).$$

Invoking the induction assumption, the first factor on the right-hand side becomes

$$\phi(p_1^{k_1}p_2^{k_2}\cdots p_i^{k_i}) = (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1})\cdots(p_i^{k_i} - p_i^{k_i-1})$$

and this serves to complete the induction step, as well as the proof.

Example 7-1

Let us calculate the value $\phi(360)$, for instance. The prime-power decomposition of 360 is $2^3 \cdot 3^2 \cdot 5$, and Theorem 7-3 tells us that

$$\phi(360) = 360(1 - \tfrac{1}{2})(1 - \tfrac{1}{3})(1 - \tfrac{1}{5})$$
$$= 360 \cdot \tfrac{1}{2} \cdot \tfrac{2}{3} \cdot \tfrac{4}{5} = 96.$$

The sharp-eyed reader will have noticed that, save for $\phi(1)$ and $\phi(2)$, the values of $\phi(n)$ in our examples are always even. This is no accident, as the next theorem shows.

THEOREM 7-4. *For $n > 2$, $\phi(n)$ is an even integer.*

Proof: First, assume that n is a power of 2, let us say $n = 2^k$, with $k \geq 2$. By Theorem 7-3,

$$\phi(n) = \phi(2^k) = 2^k(1 - \tfrac{1}{2}) = 2^{k-1},$$

an even integer. If n does not happen to be a power of 2, then it is divisible by an odd prime p; we may therefore write n as $n = p^k m$, where $k \geq 1$ and $\gcd(p^k, m) = 1$. Exploiting the multiplicative nature of the phi-function, one gets

$$\phi(n) = \phi(p^k)\phi(m) = p^{k-1}(p - 1)\phi(m),$$

which is again even since $2 \mid p - 1$.

We can establish Euclid's Theorem on the infinitude of primes in the following new way: As before, assume that there are only a finite number of primes. Call them $p_1, p_2, \ldots, p_r$ and consider the integer $n = p_1 p_2 \cdots p_r$. We argue that if $1 < a \leq n$, then $\gcd(a, n) \neq 1$. For, the Fundamental Theorem of Arithmetic tells us that a has a prime divisor q. Since $p_1, p_2, \ldots, p_r$ are the only primes, q must be one of these p_i, whence $q \mid n$; in other words, $\gcd(a, n) \geq q$. The implication of all this is that $\phi(n) = 1$, which is clearly impossible by Theorem 7-4.

PROBLEMS

1. Calculate $\phi(1001)$, $\phi(5040)$, and $\phi(36{,}000)$.
2. Verify that the equality $\phi(n) = \phi(n+1) = \phi(n+2)$ holds when $n = 5186$.
3. Show that the integers $m = 3^k \cdot 568$ and $n = 3^k \cdot 638$, where $k \geq 0$, satisfy simultaneously
$$\tau(m) = \tau(n),\ \sigma(m) = \sigma(n),\ \phi(m) = \phi(n).$$
4. Establish each of the assertions below:
   (a) If n is an odd integer, then $\phi(2n) = \phi(n)$.
   (b) If n is an even integer, then $\phi(2n) = 2\phi(n)$.
   (c) $\phi(3n) = 3\phi(n)$ if and only if $3 \mid n$.
   (d) $\phi(3n) = 2\phi(n)$ if and only if $3 \nmid n$.
   (e) $\phi(n) = n/2$ if and only if $n = 2^k$ for some $k \geq 1$. [*Hint:* Write $n = 2^k N$, where N is odd, and use the condition $\phi(n) = n/2$ to show that $N = 1$.]
5. Prove that the equation $\phi(n) = \phi(n+2)$ is satisfied by $n = 2(2p - 1)$ whenever p and $2p - 1$ are both odd primes.
6. Show that there are infinitely many integers n for which $\phi(n)$ is a perfect square. [*Hint:* Consider the integers $n = 2^{k+1}$ for $k = 1, 2, \ldots$.]

EULER'S THEOREM

As remarked earlier, the first published proof of Fermat's Theorem (that $a^{p-1} \equiv 1 \pmod{p}$ if $p \nmid a$) was given by Euler in 1736. Somewhat later, in 1760, he succeeded in generalizing Fermat's Theorem from the case of a prime p to an arbitrary integer n. This landmark result states: if $\gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$.

For example, putting $n = 30$ and $a = 11$, we have

$$11^{\phi(30)} \equiv 11^8 \equiv (11^2)^4 \equiv (121)^4 \equiv 1^4 \equiv 1 \pmod{30}.$$

As a prelude to launching our proof of Euler's Generalization of Fermat's Theorem, we require a preliminary lemma.

LEMMA. *Let $n > 1$ and $\gcd(a, n) = 1$. If $a_1, a_2, \ldots, a_{\phi(n)}$ are the positive integers less than n and relatively prime to n, then*

$$aa_1, aa_2, \ldots, aa_{\phi(n)}$$

are congruent modulo n to $a_1, a_2, \ldots, a_{\phi(n)}$ in some order.

Proof: Observe that no two of the integers $aa_1, aa_2, \ldots, aa_{\phi(n)}$ are congruent modulo n. For if $aa_i \equiv aa_j \pmod{n}$, with $1 \leq i < j \leq \phi(n)$, then the cancellation law yields $a_i \equiv a_j \pmod{n}$, a contradiction. Furthermore, since $\gcd(a_i, n) = 1$ for all i and $\gcd(a, n) = 1$, the lemma on page 137 guarantees that each of the aa_i is relatively prime to n.

Fixing on a particular aa_i, there exists a unique integer b, where $0 \leq b < n$, for which $aa_i \equiv b \pmod{n}$. Because

$$\gcd(b, n) = \gcd(aa_i, n) = 1,$$

b must be one of the integers $a_1, a_2, \ldots, a_{\phi(n)}$. All told, this proves that the numbers $aa_1, aa_2, \ldots, aa_{\phi(n)}$ and the numbers $a_1, a_2, \ldots, a_{\phi(n)}$ are identical (modulo n) in a certain order.

THEOREM 7-5 (Euler). *If n is a positive integer and $\gcd(a, n) = 1$ then $a^{\phi(n)} \equiv 1 \pmod{n}$.*

Proof: There is no harm in taking $n > 1$. Let $a_1, a_2, \ldots, a_{\phi(n)}$ be the positive integers less than n which are relatively prime to n. Since $\gcd(a, n) = 1$, it follows from the lemma that $aa_1, aa_2, \ldots, aa_{\phi(n)}$ are congruent, not necessarily in order of appearance, to

$a_1, a_2, \ldots, a_{\phi(n)}$. Then

$$\begin{aligned} aa_1 &\equiv a'_1 \pmod{n}, \\ aa_2 &\equiv a'_2 \pmod{n}, \\ &\vdots \qquad \vdots \\ aa_{\phi(n)} &\equiv a'_{\phi(n)} \pmod{n}, \end{aligned}$$

where $a'_1, a'_2, \ldots, a'_{\phi(n)}$ are the integers $a_1, a_2, \ldots, a_{\phi(n)}$ in order. On taking the product of these $\phi(n)$ congruences, v

$$\begin{aligned} (aa_1)(aa_2)\cdots(aa_{\phi(n)}) &\equiv a'_1\, a'_2 \cdots a'_{\phi(n)} \pmod{n} \\ &\equiv a_1 a_2 \cdots a_{\phi(n)} \pmod{n} \end{aligned}$$

and so

$$a^{\phi(n)}(a_1 a_2 \cdots a_{\phi(n)}) \equiv a_1 a_2 \cdots a_{\phi(n)} \pmod{n}.$$

Since $\gcd(a_i, n) = 1$ for each i, the lemma preceding Theore implies that $\gcd(a_1 a_2 \cdots a_{\phi(n)}, n) = 1$. Therefore we may both sides of the foregoing congruence by the common $a_1 a_2 \cdots a_{\phi(n)}$, leaving us with

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

This proof can best be illustrated by carrying it out with some specific numbers. Let $n = 9$, for instance. The positive integers less than and relatively prime to 9 are

$$1, 2, 4, 5, 7, 8.$$

These play the role of the integers $a_1, a_2, \ldots, a_{\phi(n)}$ in the proof of Theorem 7-5. If $a = -4$, then the integers aa_i are

$$-4, -8, -16, -20, -28, -32,$$

where, modulo 9,

$$-4 \equiv 5,\ -8 \equiv 1,\ -16 \equiv 2,\ -20 \equiv 7,\ -28 \equiv 8,\ -32 \equiv 4.$$

When the above congruences are all multiplied together, we obtain

$$(-4)(-8)(-16)(-20)(-28)(-32) \equiv 5 \cdot 1 \cdot 2 \cdot 7 \cdot 8 \cdot 4 \pmod 9,$$

which becomes

$$(1 \cdot 2 \cdot 4 \cdot 5 \cdot 7 \cdot 8)(-4)^6 \equiv (1 \cdot 2 \cdot 4 \cdot 5 \cdot 7 \cdot 8) \pmod 9.$$

Being relatively prime to 9, the six integers 1, 2, 4, 5, 7, 8 may be successively cancelled to give

$$(-4)^6 \equiv 1 \pmod 9.$$

The validity of this last congruence is confirmed by the calculation

$$(-4)^6 \equiv 4^6 \equiv (64)^2 \equiv 1^2 \equiv 1 \pmod 9.$$

Note that Theorem 7-5 does indeed generalize the one due to Fermat, which we proved earlier. For if p is a prime, then $\phi(p) = p - 1$; hence, whenever $\gcd(a, p) = 1$, we get

$$a^{p-1} \equiv a^{\phi(p)} \equiv 1 \pmod p$$

and so:

COROLLARY (Fermat). *If p is a prime and $p \nmid a$, then* $a^{p-1} \equiv 1 \pmod p$.

Example 7-2

Euler's Theorem is helpful in reducing large powers modulo n. To cite a typical example, let us find the last two digits in the decimal representation of 3^{256}; this is equivalent to obtaining the smallest nonnegative integer to which 3^{256} is congruent modulo 100. Since $\gcd(3,100) = 1$ and

$$\phi(100) = \phi(2^2 \cdot 5^2) = 100(1 - \tfrac{1}{2})(1 - \tfrac{1}{5}) = 40,$$

Euler's Theorem yields

$$3^{40} \equiv 1 \pmod{100}.$$

By the Division Algorithm, $256 = 6 \cdot 40 + 16$; whence

$$3^{256} \equiv 3^{6 \cdot 40 + 16} \equiv (3^{40})^6 3^{16} \equiv 3^{16} \pmod{100}$$

and our problem reduces to one of evaluating 3^{16}, modulo 100. The calculations are as follows, with reasons omitted:

$$3^{16} \equiv (81)^4 \equiv (-19)^4 \equiv (361)^2 \equiv 61^2 \equiv 21 \pmod{100}.$$

There is another path to Euler's Theorem, one which requires the use of Fermat's Theorem.

Second Proof of Euler's Theorem: To start, we argue by induction that if $p \nmid a$ (p a prime), then

$$a^{\phi(p^k)} \equiv 1 \pmod{p^k}, \qquad k > 0. \tag{1}$$

When $k = 1$, this assertion reduces to the statement of Fermat's Theorem. Assuming the truth of (1) for a fixed value of k, we wish to show that it is true with k replaced by $k + 1$.

Since (1) is assumed to hold, we may write

$$a^{\phi(p^k)} = 1 + qp^k$$

for some integer q. Notice too that

$$\phi(p^{k+1}) = p^{k+1} - p^k = p(p^k - p^{k-1}) = p\phi(p^k).$$

Using these facts, along with the Binomial Theorem, we obtain

$$\begin{aligned} a^{\phi(p^{k+1})} &= a^{p\phi(p^k)} \\ &= (1 + qp^k)^p \\ &= 1 + \binom{p}{1}(qp^k) + \binom{p}{2}(qp^k)^2 + \cdots + \binom{p}{p-1}(qp^k)^{p-1} + (qp^k)^p \\ &\equiv 1 + \binom{p}{1}(qp^k) \pmod{p^{k+1}}. \end{aligned}$$

But $p \mid \binom{p}{i}$ and so $p^{k+1} \mid \binom{p}{i}(qp^k)$. Thus, the last-written congruence becomes

$$a^{\phi(p^{k+1})} \equiv 1 \pmod{p^{k+1}},$$

completing the induction step.

Now let $\gcd(a, n) = 1$ and n have the prime factorization $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$. In view of what has already been proved, each of the congruences

$$a^{\phi(p_i^{k_i})} \equiv 1 \pmod{p_i^{k_i}}, \qquad i = 1, 2, \ldots, r \tag{2}$$

holds. Noting that $\phi(n)$ is divisible by $\phi(p_i^{k_i})$, we may raise both sides of (2) to the power $\phi(n)/\phi(p_i^{k_i})$ and arrive at

$$a^{\phi(n)} \equiv 1 \pmod{p_i^{k_i}}, \qquad i = 1, 2, \ldots, r.$$

Inasmuch as the moduli are relatively prime, this leads us to the relation

$$a^{\phi(n)} \equiv 1 \pmod{p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}}$$

or $a^{\phi(n)} \equiv 1 \pmod{n}$.

The usefulness of Euler's Theorem in number theory would be hard to exaggerate. It leads, for instance, to a different proof of the Chinese Remainder Theorem. In other words, we seek to establish that if $\gcd(n_i, n_j) = 1$ for $i \neq j$, then the system of linear congruences

$$x \equiv a_i \pmod{n_i}, \qquad i = 1, 2, \ldots, r$$

admits a simultaneous solution. Let $n = n_1 n_2 \cdots n_r$ and put $N_i = n/n_i$ for $i = 1, 2, \ldots, r$. Then the integer

$$x = a_1 N_1^{\phi(n_1)} + a_2 N_2^{\phi(n_2)} + \cdots + a_r N_r^{\phi(n_r)}$$

fulfills our requirements. To see this, first note that $N_j \equiv 0 \pmod{n_i}$ whenever $i \neq j$; whence,

$$x \equiv a_i N_i^{\phi(n_i)} \pmod{n_i}.$$

But, since $\gcd(N_i, n_i) = 1$, we have

$$N_i^{\phi(n_i)} \equiv 1 \pmod{n_i}$$

and so $x \equiv a_i \pmod{n_i}$ for each i.

As a second application of Euler's Theorem, let us show that if n is an odd integer which is not a multiple of 5, then n divides an integer all of whose digits are equal to 1. (For example: $7 \mid 111111$.) Since $\gcd(n, 10) = 1$ and $\gcd(9, 10) = 1$, we have $\gcd(9n, 10) = 1$ Quoting Theorem 7-5 again,

$$10^{\phi(9n)} \equiv 1 \pmod{9n}.$$

This says that $10^{\phi(9n)} - 1 = 9nk$ for some integer k or, what amounts to the same thing,

$$kn = \frac{10^{\phi(9n)} - 1}{9}.$$

The right-hand side of the above expression is an integer whose digits are all equal to 1, each digit of the numerator being clearly equal to 9.

PROBLEMS

1. Use Euler's Theorem to establish the following:
   (a) For any integer a, $a^{37} \equiv a \pmod{1729}$. [*Hint:* $1729 = 7 \cdot 13 \cdot 19$.]
   (b) For any integer a, $a^{13} \equiv a \pmod{2730}$. [*Hint:* $2730 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 13$.]
   (c) For any odd integer a, $a^{33} \equiv a \pmod{4080}$. [*Hint:* $4080 = 15 \cdot 16 \cdot 17$.]
2. Show that if $\gcd(a, n) = \gcd(a - 1, n) = 1$, then

$$1 + a + a^2 + \cdots + a^{\phi(n)-1} \equiv 0 \pmod{n}.$$

   [*Hint:* Recall that $a^{\phi(n)} - 1 = (a - 1)(a^{\phi(n)-1} + \cdots + a^2 + a + 1)$.]
3. If m and n are relatively prime positive integers, prove that

$$m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{mn}.$$

SOME PROPERTIES OF THE PHI-FUNCTION

The next theorem points out a curious feature of the phi-function; namely, that the sum of the values of $\phi(d)$, as d ranges over the positive divisors of n, is equal to n itself. This was first noticed by Gauss.

THEOREM 7-6 (Gauss). *For each positive integer $n \geq 1$,*

$$n = \sum_{d|n} \phi(d),$$

the sum being extended over all positive divisors of n.

Proof: The integers between 1 and n can be separated into classes as follows: if d is a positive divisor of n, we put the integer m in the class S_d provided that $\gcd(m, n) = d$. Stated in symbols,

$$S_d = \{m \mid \gcd(m, n) = d;\ 1 \leq m \leq n\}.$$

Now $\gcd(m, n) = d$ if and only if $\gcd(m/d, n/d) = 1$. Thus the number of integers in the class S_d is equal to the number of positive integers not exceeding n/d which are relatively prime to n/d; in other words, equal to $\phi(n/d)$. Since each of the n integers in the set $\{1, 2, \ldots, n\}$ lies in exactly one class S_d, we obtain the formula

$$n = \sum_{d|n} \phi(n/d).$$

But as d runs through all positive divisors of n, so does n/d; hence,

$$\sum_{d|n} \phi(n/d) = \sum_{d|n} \phi(d)$$

and the theorem follows.

Example 7-3

A simple numerical example of what we have just said is provided by $n = 10$. Here, the classes S_d are

$$S_1 = \{1, 3, 7, 9\},$$
$$S_2 = \{2, 4, 6, 8\},$$
$$S_5 = \{5\},$$
$$S_{10} = \{10\}.$$

These contain $\phi(10) = 4$, $\phi(5) = 4$, $\phi(2) = 1$, and $\phi(1) = 1$ integers, respectively. Therefore,

$$\sum_{d|10} \phi(d) = \phi(10) + \phi(5) + \phi(2) + \phi(1) = 4 + 4 + 1 + 1 = 10.$$

It is instructive to give a second proof of Theorem 7-6, this one depending on the fact that ϕ is multiplicative. The details are as follows: If $n = 1$, then clearly

$$\sum_{d|n} \phi(d) = \sum_{d|1} \phi(d) = \phi(1) = 1 = n.$$

Assuming that $n > 1$, let us consider the number-theoretic function

$$F(n) = \sum_{d|n} \phi(d).$$

Since ϕ is known to be a multiplicative function, Theorem 6-4 asserts that F is also multiplicative. Hence, if $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ is the prime factorization of n, then

$$F(n) = F(p_1^{k_1}) F(p_2^{k_2}) \cdots F(p_r^{k_r}).$$

For each value of i,

$$F(p_i^{k_i}) = \sum_{d|p_i^{k_i}} \phi(d)$$

$$= \phi(1) + \phi(p_i) + \phi(p_i^2) + \phi(p_i^3) + \cdots + \phi(p_i^{k_i})$$

$$= 1 + (p_i - 1) + (p_i^2 - p_i) + (p_i^3 - p_i^2) + \cdots + (p_i^{k_i} - p_i^{k_i - 1})$$
$$= p_i^{k_i},$$

since the terms in the foregoing expression cancel each other, save for the term $p_i^{k_i}$. Knowing this, we end up with

$$F(n) = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} = n$$

and so

$$n = \sum_{d|n} \phi(d),$$

as desired.

We should mention in passing that there is another interesting identity which involves the phi-function.

THEOREM 7-7. *For $n > 1$, the sum of the positive integers less than n and relatively prime to n is $\frac{1}{2}n\phi(n)$; in symbols,*

$$\tfrac{1}{2}n\phi(n) = \sum_{\substack{\gcd(k,n)=1 \\ 1 \le k < n}} k.$$

Proof: Let $a_1, a_2, \ldots, a_{\phi(n)}$ be the positive integers less than n and relatively prime to n. Now, since $\gcd(a, n) = 1$ if and only if $\gcd(n - a, n) = 1$, we have

$$a_1 + a_2 + \cdots + a_{\phi(n)} = (n - a_1) + (n - a_2) + \cdots + (n - a_{\phi(n)})$$
$$= \phi(n)n - (a_1 + a_2 + \cdots + a_{\phi(n)}).$$

Hence,

$$2(a_1 + a_2 + \cdots + a_{\phi(n)}) = \phi(n)n,$$

leading to the stated conclusion.

Example 7-4

Consider the case $n = 30$. The $\phi(30) = 8$ integers which are less than 30 and relatively prime to it are

1, 7, 11, 13, 17, 19, 23, 29.

In this setting, we find that the desired sum is

$$1 + 7 + 11 + 13 + 17 + 19 + 23 + 29 = 120 = \tfrac{1}{2} \cdot 30 \cdot 8.$$

This is a good point at which to give an application of the Möbius Inversion Formula.

THEOREM 7-8. *For any positive integer n,*

$$\phi(n) = n \sum_{d|n} \mu(d)/d.$$

Proof: The proof is deceptively simple: If one applies the inversion formula to

$$F(n) = n = \sum_{d|n} \phi(d),$$

the result is

$$\phi(n) = \sum_{d|n} \mu(d) F(n/d) = \sum_{d|n} \mu(d) n/d.$$

Let us illustrate the situation with $n = 10$ again. As can easily be seen,

$$\begin{aligned} 10 \sum_{d|10} \mu(d)/d &= 10[\mu(1) + \mu(2)/2 + \mu(5)/5 + \mu(10)/10] \\ &= 10[1 + (-1)/2 + (-1)/5 + (-1)^2/10] \\ &= 10[1 - 1/2 - 1/5 + 1/10] = 10 \cdot 2/5 = 4 = \phi(10). \end{aligned}$$

Starting with Theorem 7-8, it is an easy matter to determine the value of the phi-function for any positive integer n. Suppose that the prime-power decomposition of n is $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ and consider the product

$$P = \prod_{p_i|n} (\mu(1) + \mu(p_i)/p_i + \cdots + \mu(p_i^{k_i})/p_i^{k_i}).$$

Multiplying this out, we obtain a sum of terms of the form

$$\mu(1)\mu(p_1^{a_1})\mu(p_2^{a_2})\cdots\mu(p_r^{a_r})/p_1^{a_1}p_2^{a_2}\cdots p_r^{a_r}, \qquad 0 \le a_i \le k_i$$

or, since μ is known to be multiplicative,

$$\mu(p_1^{a_1}p_2^{a_2}\cdots p_r^{a_r})/p_1^{a_1}p_2^{a_2}\cdots p_r^{a_r} = \mu(d)/d,$$

where the summation is over the set of divisors $d = p_1^{a_1}p_2^{a_2}\cdots p_r^{a_r}$ of n. Hence, $P = \sum_{d|n}\mu(d)/d$. It follows from Theorem 7-8 that

$$\phi(n) = n\sum_{d|n}\mu(d)/d = n\prod_{p_i|n}(\mu(1) + \mu(p_i)/p_i + \cdots + \mu(p_i^{k_i})/p_i^{k_i}).$$

But $\mu(p_i^{a_i}) = 0$ whenever $a_i \ge 2$. As a result, the last-written equation reduces to

$$\phi(n) = n\prod_{p_i|n}(\mu(1) + \mu(p_i)/p_i) = n\prod_{p_i|n}(1 - 1/p_i),$$

which agrees with the formula established earlier by different reasoning. What is significant about this argument is that no assumption is made concerning the multiplicative character of the phi-function, only of μ.

PROBLEMS

1. For a positive integer n, prove that

$$\sum_{d|n}(-1)^{n/d}\phi(d) = \begin{cases} 0 \text{ if } n \text{ is even} \\ -n \text{ if } n \text{ is odd} \end{cases}$$

[*Hint*: If $n = 2^k N$, where N is odd, then $\sum_{d|n}(-1)^{n/d}\phi(d) = \sum_{d|2^{k-1}N}\phi(d) - \sum_{d|N}\phi(2^k d)$.]

2. Confirm that $\sum_{d|36}\phi(d) = 36$ and $\sum_{d|36}(-1)^{36/d}\phi(d) = 0$.

3. For a positive integer n, prove that $\sum_{d|n}\mu^2(d)/\phi(d) = n/\phi(n)$. [*Hint:* See the hint in Problem 1.]

4. Use Problem 3, Section 6.2, to give a different proof of the fact that

$$n\sum_{d|n}\mu(d)/d = \phi(n).$$

5. If the integer $n > 1$ has the prime factorization $n = p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$, establish the following:

(a) $\sum_{d|n} \mu(d)\phi(d) = (2-p_1)(2-p_2)\cdots(2-p_r)$

(b) $\sum_{d|n} d\phi(d) = \left(\frac{{p_1}^{2k_1+1}+1}{p_1+1}\right)\left(\frac{{p_2}^{2k_2+1}+1}{p_2+1}\right)\cdots\left(\frac{{p_r}^{2k_r+1}+1}{p_r+1}\right)$

(c) $\sum_{d|n} \phi(d)/d = \left(1+\frac{k_1(p_1-1)}{p_1}\right)\left(1+\frac{k_2(p_2-1)}{p_2}\right)\cdots\left(1+\frac{k_r(p_r-1)}{p_r}\right)$

[*Hint:* For part (a), use Problem 3, Section 6-2.]

POSSIBLE QUESTIONS

2 Mark Questions:

1. Define Mobius Inversion Formula.
2. Prove that the function μ is a multiplicative function.
3. Define greatest positive integer.
4. If N is a positive integer, then $\sum_{n=1}^{N}\tau(n)=\sum_{n=1}^{N}[N/n]$.
5. Define Euler Phi function with example.
6. Find the value of $\phi(36000)$.
7. Prove that for $n>2$, $\phi(n)$ is an even integer.
8. Prove that for any positive integer n, $\phi(n)=n\sum_{d|n}\mu(d)/d$.
9. State Gauss lemma.
10. Prove that if p is a prime and p does not divides a ,then $a^{p-1}\equiv 1(\text{mod } p)$.

8 Mark Questions:

1. State and prove Mobius inverse formula.
2. Prove that if F is multiplicative function

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

Then f is also multiplicative.

3. Prove that if n is a positive integer and p is a prime, then the exponent of the highest power of p that divides n! is

$$\sum_{n=1}^{\infty}[n/pk]$$

(That is an infinite series, since $[n/p^k]=0$ for p^k >n.)

4. Prove if n and r are positive integers with $1\le r<n$, then the binomial coefficient

$$\binom{n}{r}=\frac{n!}{r!(n-r)!}$$

is also an integer.

5. Let f and F be number-theoretic function such that

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

then, prove for any positive integer N,

$$\sum_{k=1}^{N}F(n)=\sum_{k=1}^{N}f(k)[N/k].$$

6. Prove that the function ϕ is a multiplicative function.

7. Prove that if the integer $n > 1$ has the prime factorization $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$, then
$$\phi(n) = (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1}) \dots (p_r^{k_r} - p_r^{k_r-1})$$
$$= n(1-1/p_1)(1-1/p_2) \dots (1-1/p_r).$$
8. Let $n > 1$ and $\gcd(a, n) = 1$. If $a_1, a_2, \dots, a_{\phi(n)}$ are the positive integer less than n and relatively prime to n, then
$$aa_1, aa_2, \dots, aa_{\phi(n)}$$
are congruent modulo n to $a_1, a_2, \dots, a_{\phi(n)}$ in some order.
9. State and prove Euler theorem.
10. Prove that for each positive integer $n \geq 1$,
$$n = \sum_{d|n} \phi(d),$$
the sum being extended over all positive divisor of n.

UNIT-IV

SYLLABUS

Order of an integer modulo n, primitive roots for primes, composite numbers having primitive roots, Euler's criterion, the Legendre symbol and its properties.

THE ORDER OF AN INTEGER MODULO n

In view of Euler's Theorem, we know that $a^{\phi(n)} \equiv 1 \pmod{n}$, whenever $\gcd(a, n) = 1$. However, there are often powers of a smaller than $a^{\phi(n)}$ which are congruent to 1 modulo n. This prompts the following definition:

DEFINITION 8-1. Let $n > 1$ and $\gcd(a, n) = 1$. The *order of a modulo n* (in older terminology: the *exponent to which a belongs modulo n*) is the smallest positive integer k such that $a^k \equiv 1 \pmod{n}$.

Consider the successive powers of 2 modulo 7. For this modulus, we obtain the congruences

$$2^1 \equiv 2,\ 2^2 \equiv 4,\ 2^3 \equiv 1,\ 2^4 \equiv 2,\ 2^5 \equiv 4,\ 2^6 \equiv 1, \ldots,$$

from which it follows that the integer 2 has order 3 modulo 7.

Observe that if two integers are congruent modulo n, then they have the same order modulo n. For if $a \equiv b \pmod{n}$ and $a^k \equiv 1 \pmod{n}$, Theorem 4-2 implies that $a^k \equiv b^k \pmod{n}$, whence $b^k \equiv 1 \pmod{n}$.

It should be emphasized that our definition of order modulo n concerns only integers a for which $\gcd(a, n) = 1$. Indeed, if $\gcd(a, n) > 1$, then we know from Theorem 4-7 that the linear congruence $ax \equiv 1 \pmod{n}$ has no solution; hence, the relation

$$a^k \equiv 1 \pmod{n}, \qquad k \geq 1$$

cannot hold, for this would imply that $x = a^{k-1}$ is a solution of $ax \equiv 1 \pmod{n}$. Thus, whenever there is reference to the order of a modulo n, it is to be assumed that $\gcd(a, n) = 1$, even if it is not explicitly stated.

In the example given above, we have $2^k \equiv 1 \pmod{7}$ whenever k is a multiple of 3, the order of 2 modulo 7. Our first theorem shows that this is typical of the general situation.

THEOREM 8-1. *Let the integer a have order k modulo n. Then $a^h \equiv 1 \pmod{n}$ if and only if $k \mid h$; in particular, $k \mid \phi(n)$.*

Proof: Suppose to begin with that $k \mid h$, so that $h = jk$ for some integer j. Since $a^k \equiv 1 \pmod{n}$, Theorem 4-2 tells us that $(a^k)^j \equiv 1^j \pmod{n}$ or $a^h \equiv 1 \pmod{n}$.

Conversely, let h be any positive integer satisfying $a^h \equiv 1 \pmod{n}$. By the Division Algorithm, there exist q and r such that $h = qk + r$, where $0 \leq r < k$. Consequently,

$$a^h = a^{qk+r} = (a^k)^q a^r.$$

By hypothesis both $a^h \equiv 1 \pmod{n}$ and $a^k \equiv 1 \pmod{n}$, the implication of which is that $a^r \equiv 1 \pmod{n}$. Since $0 \leq r < k$, we end up with $r = 0$; otherwise, the choice of k as the smallest positive integer such that $a^k \equiv 1 \pmod{n}$ is contradicted. Hence $h = qk$, and $k \mid h$.

Theorem 8-1 expedites the computation when attempting to find the order of an integer a modulo n: instead of considering all powers of a, the exponents can be restricted to the divisors of $\phi(n)$. Let us obtain, by way of illustration, the order of 2 modulo 13. Since $\phi(13) = 12$, the order of 2 must be one of the integers 1, 2, 3, 4, 6, 12. From

$$2^2 \equiv 4,\ 2^3 \equiv 8,\ 2^4 \equiv 3,\ 2^6 \equiv 12,\ 2^{12} \equiv 1 \pmod{13},$$

it is seen that 2 has order 12 modulo 13.

For an arbitrarily selected divisor d of $\phi(n)$, it is not always true that there exists an integer a having order d modulo n. An example is $n = 12$. Here $\phi(12) = 4$, yet there is no integer which is of order 4 modulo 12; indeed, one finds that

$$1^2 \equiv 5^2 \equiv 7^2 \equiv 11^2 \equiv 1 \pmod{12}$$

and so the only choice for orders is 1 or 2.

Here is another basic fact regarding the order of an integer.

THEOREM 8-2. *If a has order k modulo n, then $a^i \equiv a^j \pmod{n}$ if and only if $i \equiv j \pmod{k}$.*

Proof: First, suppose that $a^i \equiv a^j \pmod{n}$, where $i \geq j$. Since a is relatively prime to n, we may cancel a power of a to obtain $a^{i-j} \equiv 1$

(mod n). According to Theorem 8-1, this last congruence holds only if $k \mid i-j$, which is just another way of saying that $i \equiv j \pmod{k}$.

Conversely, let $i \equiv j \pmod{k}$. Then we have $i = j + qk$ for some integer q. By the definition of k, $a^k \equiv 1 \pmod{n}$, so that

$$a^i \equiv a^{j+qk} \equiv a^j (a^k)^q \equiv a^j \pmod{n},$$

which is the desired conclusion.

COROLLARY. *If a has order k modulo n, then the integers $a, a^2, \ldots, a^k$ are incongruent modulo n.*

Proof: If $a^i \equiv a^j \pmod{n}$ for $1 \leq i \leq j \leq k$, then the theorem insures that $i \equiv j \pmod{k}$. But this is impossible unless $i = j$.

THEOREM 8-3. *If the integer a has order k modulo n and $h > 0$, then a^h has order $k/\gcd(h, k)$ modulo n.*

Proof: Let $d = \gcd(h, k)$. Then we may write $h = h_1 d$ and $k = k_1 d$, with $\gcd(h_1, k_1) = 1$. Clearly,

$$(a^h)^{k_1} = (a^{h_1 d})^{k/d} = (a^k)^{h_1} \equiv 1 \pmod{n}.$$

If a^h is assumed to have order r modulo n, then Theorem 8-1 asserts that $r \mid k_1$. On the other hand, since a has order k modulo n, the congruence

$$a^{hr} \equiv (a^h)^r \equiv 1 \pmod{n}$$

indicates that $k \mid hr$; in other words, $k_1 d \mid h_1 dr$ or $k_1 \mid h_1 r$. But $\gcd(k_1, h_1) = 1$ and therefore $k_1 \mid r$. This divisibility relation, when combined with the one obtained earlier, gives

$$r = k_1 = k/d = k/\gcd(h, k),$$

proving the theorem.

The last theorem has a corollary for which the reader may supply a proof.

COROLLARY. *Let a have order k modulo n. Then a^h also has order k if and only if* $\gcd(h, k) = 1$.

Example 8-1

The following table exhibits the orders modulo 13 of the positive integers less than 13:

integer	1	2	3	4	5	6	7	8	9	10	11	12
order	1	12	3	6	4	12	12	4	3	6	12	2

We observe that the order of 2 modulo 13 is 12, while the orders of 2^2 and 2^3 are 6 and 4, respectively; it is easy to verify that

$$6 = 12/\gcd(2, 12) \quad \text{and} \quad 4 = 12/\gcd(3, 12)$$

in accordance with Theorem 8-3. Those integers which also have order 12 modulo 13 are powers 2^k for which $\gcd(k, 12) = 1$; namely,

$$2^5 \equiv 6,\ 2^7 \equiv 11,\ 2^{11} \equiv 7 \pmod{13}.$$

If an integer a has the largest order possible, then we call it a primitive root of n.

DEFINITION 8-2. If $\gcd(a, n) = 1$ and a is of order $\phi(n)$ modulo n, then a is a *primitive root of* n.

To put it another way, n has a as a primitive root if $a^{\phi(n)} \equiv 1 \pmod{n}$, but $a^k \not\equiv 1 \pmod{n}$ for all positive integers $k < \phi(n)$.

It is easy to see that 3 is a primitive root of 7, for

$$3^1 \equiv 3,\ 3^2 \equiv 2,\ 3^3 \equiv 6,\ 3^4 \equiv 4,\ 3^5 \equiv 5,\ 3^6 \equiv 1 \pmod{7}.$$

More generally, one can prove that primitive roots exist for any prime modulus, a result of fundamental importance. While it is possible for a primitive root of n to exist when n is not a prime (for instance, 2 is a primitive root of 9), there is no reason to expect that every integer n will possess a primitive root; indeed, the existence of primitive roots is more the exception than the rule.

Example 8-2

Let us show that if $F_n = 2^{2^n} + 1$, $n > 1$, is a prime, then 2 is not a primitive root of F_n. (Clearly, 2 is a primitive root of $5 = F_1$.) Since $2^{2^{n+1}} - 1 = (2^{2^n} + 1)(2^{2^n} - 1)$, we have

$$2^{2^{n+1}} \equiv 1 \pmod{F_n},$$

which implies that the order of 2 modulo F_n does not exceed 2^{n+1}. But if F_n is assumed to be prime,

$$\phi(F_n) = F_n - 1 = 2^{2^n}$$

and a straightforward induction argument confirms that $2^{2^n} > 2^{n+1}$, whenever $n > 1$. Thus the order of 2 modulo F_n is smaller than $\phi(F_n)$; referring to Definition 8-2 we see that 2 cannot be a primitive root of F_n.

One of the chief virtues of primitive roots lies in our next theorem.

THEOREM 8-4. *Let* $\gcd(a, n) = 1$ *and let* $a_1, a_2, \ldots, a_{\phi(n)}$ *be the positive integers less than n and relatively prime to n. If a is a primitive root of n, then*

$$a, a^2, \ldots, a^{\phi(n)}$$

are congruent modulo n to $a_1, a_2, \ldots, a_{\phi(n)}$, *in some order.*

Proof: Since a is relatively prime to n, the same holds for all the powers of a; hence, each a^k is congruent modulo n to some one of the a_i. The $\phi(n)$ numbers in the set $\{a, a^2, \ldots, a^{\phi(n)}\}$ are incongruent by the corollary to Theorem 8-2, hence these powers must represent (not necessarily in order of appearance) the integers $a_1, a_2, \ldots, a_{\phi(n)}$.

One consequence of what has just been proved is that, in those cases in which a primitive root exists, we can now state exactly how many there are.

COROLLARY. *If n has a primitive root, then it has exactly* $\phi(\phi(n))$ *of them.*

Proof: Suppose that a is a primitive root of n. By the theorem, any other primitive root of n is found among the members of the set $\{a, a^2, \ldots, a^{\phi(n)}\}$. But the number of powers a^k, $1 \leq k \leq \phi(n)$, which have order $\phi(n)$ is equal to the number of integers k for which $\gcd(k, \phi(n)) = 1$; there are $\phi(\phi(n))$ such integers, hence $\phi(\phi(n))$ primitive roots of n.

Theorem 8-4 can be illustrated by taking $a = 2$ and $n = 9$. Since $\phi(9) = 6$, the first six powers of 2 must be congruent modulo 9, in some order, to the positive integers less than 9 and relatively prime to it. Now the integers less than and relatively prime to 9 are 1, 2, 4, 5, 7, 8 and we see that

$$2^1 \equiv 2,\ 2^2 \equiv 4,\ 2^3 \equiv 8,\ 2^4 \equiv 7,\ 2^5 \equiv 5,\ 2^6 \equiv 1 \pmod 9.$$

By virtue of the corollary, there are exactly $\phi(\phi(9)) = \phi(6) = 2$ primitive roots of 9, these being the integers 2 and 5.

PROBLEMS

1. Find the order of the integers 2, 3, and 5: (a) modulo 17, (b) modulo 19, and (c) modulo 23.
2. Establish each of the statements below:
   (a) If a has order hk modulo n, then a^h has order k modulo n.
   (b) If a has order $2k$ modulo the odd prime p, then $a^k \equiv -1 \pmod p$.
   (c) If a has order $n - 1$ modulo n, then n is a prime.
3. Prove that $\phi(2^n - 1)$ is a multiple of n for any $n > 1$. [*Hint:* The integer 2 has order n modulo $2^n - 1$.]
4. Assume that the order of a modulo n is h and the order of b modulo n is k. Show that the order of ab modulo n divides hk; in particular, if $\gcd(h, k) = 1$, then ab has order hk.

5. Given that a has order 3 modulo p, where p is an odd prime, show that $a+1$ must have order 6 modulo p. [*Hint:* Because $a^2+a+1 \equiv 0 \pmod{p}$, it follows that $(a+1)^2 \equiv a \pmod{p}$ and $(a+1)^3 \equiv -1 \pmod{p}$.]
6. Verify the following assertions:
   (a) The odd prime divisors of the integer n^2+1 are of the form $4k+1$. [*Hint:* $n^2 \equiv -1 \pmod{p}$, where p is an odd prime, implies that $4 \mid \phi(p)$ by Theorem 8-1.]
   (b) The odd prime divisors of the integer n^4+1 are of the form $8k+1$.
   (c) The odd prime divisors of the integer n^2+n+1 which are different from 3 are of the form $6k+1$.

PRIMITIVE ROOTS FOR PRIMES

Since primitive roots play a crucial role in many theoretical investigations, a problem exerting a natural appeal is that of describing all integers which possess primitive roots. We shall, over the course of the next few pages, prove the existence of primitive roots for all primes. Before doing this, let us turn aside briefly to establish a theorem dealing with the number of solutions of a polynomial congruence.

THEOREM 8-5 (Lagrange). *If p is a prime and*

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0, \qquad a_n \not\equiv 0 \pmod{p}$$

is a polynomial of degree $n \geq 1$ with integral coefficients, then the congruence

$$f(x) \equiv 0 \pmod{p}$$

has at most n incongruent solutions modulo p.

Proof: We proceed by induction on n, the degree of $f(x)$. If $n = 1$, then our polynomial is of the form

$$f(x) = a_1 x + a_0.$$

Since $\gcd(a_1, p) = 1$, we know by Theorem 4-7 that the congruence $a_1 x \equiv -a_0 \pmod{p}$ has a unique solution modulo p. Thus, the theorem holds for $n = 1$.

Now assume inductively that the theorem is true for polynomials of degree $k-1$ and consider the case in which $f(x)$ has degree k. Either $f(x) \equiv 0 \pmod{p}$ has no solutions (and we are finished) or it has at least one solution, call it a. If $f(x)$ is divided by $x-a$, the result is

$$f(x) = (x-a)q(x) + r,$$

in which $q(x)$ is a polynomial of degree $k-1$ with integral coefficients and r is an integer. Substituting $x = a$, we obtain

$$0 \equiv f(a) = (a-a)q(a) + r = r \pmod{p}$$

and so $f(x) \equiv (x-a)q(x) \pmod{p}$.

If b is another one of the incongruent solutions of $f(x) \equiv 0 \pmod{p}$, then

$$0 \equiv f(b) = (b-a)q(b) \pmod{p}.$$

Since $b - a \not\equiv 0 \pmod{p}$, this implies that $q(b) \equiv 0 \pmod{p}$; in other words, any solution of $f(x) \equiv 0 \pmod{p}$ which is different from a must satisfy $q(x) \equiv 0 \pmod{p}$. By our induction assumption, the latter congruence can possess at most $k-1$ incongruent solutions and so $f(x) \equiv 0 \pmod{p}$ will have no more than k incongruent solutions. This completes the induction step and the proof.

COROLLARY. *If p is a prime number and $d \mid p-1$, then the congruence*

$$x^d - 1 \equiv 0 \pmod{p}$$

has exactly d solutions.

Proof: Since $d \mid p-1$, we have $p - 1 = dk$ for some k. Then

$$x^{p-1} - 1 = (x^d - 1)f(x),$$

where the polynomial $f(x) = x^{d(k-1)} + x^{d(k-2)} + \cdots + x^d + 1$ has integral coefficients and is of degree $d(k-1) = p - 1 - d$. By Lagrange's Theorem, the congruence $f(x) \equiv 0 \pmod{p}$ has at most $p - 1 - d$ solutions. We also know from Fermat's Theorem that $x^{p-1} - 1 \equiv 0 \pmod{p}$ has precisely $p-1$ incongruent solutions; namely, the integers $1, 2, \ldots, p-1$.

Now any solution $x = a$ of $x^{p-1} - 1 \equiv 0 \pmod{p}$ that is not a solution of $f(x) \equiv 0 \pmod{p}$ must satisfy $x^d - 1 \equiv 0 \pmod{p}$. For

$$0 \equiv a^{p-1} - 1 = (a^d - 1)f(a) \pmod{p},$$

with $p \nmid f(a)$, implies that $p \mid a^d - 1$. It follows that $x^d - 1 \equiv 0 \pmod{p}$ must have at least

$$p - 1 - (p - 1 - d) = d$$

solutions. This last congruence can possess no more than d solutions (Lagrange's Theorem enters again), hence has exactly d solutions.

We take immediate advantage of this corollary to prove Wilson's Theorem in a different way: given a prime p, define the polynomial $f(x)$ by

$$\begin{aligned} f(x) &= (x-1)(x-2)\cdots(x-(p-1)) - (x^{p-1} - 1) \\ &= a_{p-2}x^{p-2} + a_{p-3}x^{p-3} + \cdots + a_1 x + a_0, \end{aligned}$$

which is of degree $p - 2$. Fermat's Theorem implies that the $p - 1$ integers $1, 2, \ldots, p - 1$ are incongruent solutions of the congruence

$$f(x) \equiv 0 \pmod{p}.$$

But this contradicts Lagrange's Theorem, unless

$$a_{p-2} \equiv a_{p-3} \equiv \cdots \equiv a_1 \equiv a_0 \equiv 0 \pmod{p}.$$

It follows that, for any choice of the integer x,

$$(x-1)(x-2)\cdots(x-(p-1)) - (x^{p-1} - 1) \equiv 0 \pmod{p}.$$

Now substitute $x = 0$ to obtain

$$(-1)(-2)\cdots(-(p-1)) + 1 \equiv 0 \pmod{p}$$

or $(-1)^{p-1}(p-1)! + 1 \equiv 0 \pmod{p}$. Either $p - 1$ is even or else $p = 2$, in which case $-1 \equiv 1 \pmod{p}$; at any rate, we get

$$(p-1)! \equiv -1 \pmod{p}.$$

Lagrange's Theorem has provided us with the entering wedge. We are now in a position to prove that, for any prime p, there exist integers with order corresponding to each divisor of $p-1$. Stated more precisely:

THEOREM 8-6. *If p is a prime number and $d \mid p-1$, then there are exactly $\phi(d)$ incongruent integers having order d modulo p.*

Proof: Let $d \mid p-1$ and let $\psi(d)$ denote the number of integers k, $1 \leq k \leq p-1$, which have order d modulo p. Since each integer between 1 and $p-1$ has order d for some $d \mid p-1$,

$$p-1 = \sum_{d \mid p-1} \psi(d).$$

At the same time, Gauss' Theorem tells us that

$$p-1 = \sum_{d \mid p-1} \phi(d)$$

and so, putting these together,

$$\sum_{d \mid p-1} \psi(d) = \sum_{d \mid p-1} \phi(d). \tag{1}$$

Our aim is to show that $\psi(d) \leq \phi(d)$ for each divisor d of $p-1$, since this, in conjunction with equation (1), would produce the equality $\psi(d) = \phi(d) \neq 0$ (otherwise, the first sum would be strictly smaller than the second).

Given an arbitrary divisor d of $p-1$, there are two possibilities: either $\psi(d) = 0$ or $\psi(d) > 0$. If $\psi(d) = 0$, then certainly $\psi(d) \leq \phi(d)$. Suppose that $\psi(d) > 0$, so that there exists an integer a of order d. Then the d integers $a, a^2, \ldots, a^d$ are incongruent modulo p and each of them satisfies the polynomial congruence

$$x^d - 1 \equiv 0 \pmod{p}; \tag{2}$$

for, $(a^k)^d \equiv (a^d)^k \equiv 1 \pmod{p}$. By the corollary to Lagrange's Theorem, there can be no other solutions of (2). It follows that any integer which has order d modulo p must be congruent to one of $a, a^2, \ldots, a^d$. But only $\phi(d)$ of the just-mentioned powers have order d, namely those a^k for which the exponent k has the property $\gcd(k, d) = 1$. Hence, in the present situation, $\psi(d) = \phi(d)$, and the number of integers having order d modulo p is equal to $\phi(d)$. This establishes the result we set out to prove.

COROLLARY. *If p is a prime, then there are exactly $\phi(p-1)$ incongruent primitive roots of p.*

An illustration is afforded by the prime $p = 13$. For this modulus, 1 has order 1; 12 has order 2; 3 and 9 have order 3; 5 and 8 have order 4; 4 and 10 have order 6; and four integers, namely 2, 6, 7, 11, have order 12. Thus,

$$\sum_{d|12} \psi(d) = \psi(1) + \psi(2) + \psi(3) + \psi(4) + \psi(6) + \psi(12)$$
$$= 1 + 1 + 2 + 2 + 2 + 4 = 12$$

as it should. Notice too that

$$\psi(1) = 1 = \phi(1), \qquad \psi(4) = 2 = \phi(4)$$
$$\psi(2) = 1 = \phi(2), \qquad \psi(6) = 2 = \phi(6)$$
$$\psi(3) = 2 = \phi(3), \qquad \psi(12) = 4 = \phi(12)$$

Incidentally, there is a shorter and more elegant way of proving that $\psi(d) = \phi(d)$ for each $d \mid p-1$. We simply subject the formula $d = \sum_{c|d} \psi(c)$ to Möbius inversion to deduce that

$$\psi(d) = \sum_{c|d} \mu(c)(d/c).$$

In light of Theorem 7-8, the right-hand side of the foregoing equation is equal to $\phi(d)$. Of course, the validity of this argument rests upon knowing that ψ is a multiplicative function.

We can use this last theorem to give another proof of the fact that if p is a prime of the form $4k+1$, then the quadratic congruence $x^2 \equiv -1 \pmod{p}$ admits a solution. Since $4 \mid p-1$, Theorem 8-6 tells us that there is an integer a having order 4 modulo p; in other words,

$$a^4 \equiv 1 \pmod{p}$$

or equivalently,

$$(a^2-1)(a^2+1) \equiv 0 \pmod{p}.$$

Because p is a prime, it follows that either

$$a^2 - 1 \equiv 0 \pmod{p} \quad \text{or} \quad a^2 + 1 \equiv 0 \pmod{p}.$$

If the first congruence held, then a would have order less than or equal to 2, a contradiction. Hence, $a^2+1 \equiv 0 \pmod{p}$, making the integer a a solution to the congruence $x^2 \equiv -1 \pmod{p}$.

Theorem 8-6, as proved, has an obvious drawback; while it does indeed imply the existence of primitive roots for a given prime p, the proof is nonconstructive. To find a primitive root, one must usually proceed by brute force or else fall back on the extensive tables that have been constructed. The accompanying table lists the smallest positive primitive root for each prime below 200.

If $\chi(p)$ designates the smallest positive primitive root of the prime p, then the table presented above shows that $\chi(p) \leq 19$ for all $p < 200$. In fact, $\chi(p)$ becomes arbitrarily large as p increases without bound. The table suggests, although the answer is not yet known, that there exist an infinite number of primes p for which $\chi(p) = 2$.

Prime	*Least positive primitive root*	*Prime*	*Least positive primitive root*
2	1	89	3
3	2	97	5
5	2	101	2
7	3	103	5
11	2	107	2
13	2	109	6
17	3	113	3
19	2	127	3
23	5	131	2
29	2	137	3
31	3	139	2
37	2	149	2
41	6	151	6
43	3	157	5
47	5	163	2
53	2	167	5
59	2	173	2
61	2	179	2
67	2	181	2
71	7	191	19
73	5	193	5
79	3	197	2
83	2	199	3

In his *Disquisitiones Arithmeticae*, Gauss conjectured that there are infinitely many primes having 10 as a primitive root. In 1927 Emil Artin generalized this unresolved question as: For a not equal to 1, -1, or a perfect square, do there exist infinitely many primes having a as a primitive root?

The restrictions in Artin's conjecture are justified as follows. Let a be a perfect square, say $a = x^2$, and let p be an odd prime with $\gcd(a, p) = 1$. If $p \nmid x$, then Fermat's Theorem yields $x^{p-1} \equiv 1 \pmod{p}$, whence

$$a^{(p-1)/2} \equiv (x^2)^{(p-1)/2} \equiv 1 \pmod{p}.$$

Thus a cannot serve as a primitive root of p [if $p \mid x$, then $p \mid a$ and surely $a^{p-1} \not\equiv 1 \pmod{p}$]. Furthermore, since $(-1)^2 = 1$, -1 is not a primitive root of p whenever $p - 1 > 2$.

Example 8-3

Let us employ the various techniques of this section to find the $\phi(6) = 2$ integers having order 6 modulo 31. To start, we know that there are

$$\phi(\phi(31)) = \phi(30) = 8$$

primitive roots of 31. Obtaining one of them is a matter of trial and error. Since $2^5 \equiv 1 \pmod{31}$, the integer 2 is clearly ruled out. We need not search too far, since 3 turns out to be a primitive root of 31. Observe that in computing the integral powers of 3 it is not necessary to go beyond 3^{15}; for the order of 3 must divide $\phi(31) = 30$ and the calculation

$$3^{15} \equiv (27)^5 \equiv (-4)^5 \equiv (-64)(16) \equiv -2(16) \equiv -1 \not\equiv 1 \pmod{31}$$

shows that its order is greater than 15.

Because 3 is a primitive root of 31, any integer which is relatively prime to 31 is congruent modulo 31 to an integer of the form 3^k, where $1 \leq k \leq 30$. Theorem 8-3 asserts that the order of 3^k is $30/\gcd(k, 30)$; this will equal 6 if and only if $\gcd(k, 30) = 5$. The values of k for which the last equality holds are $k = 5$ and $k = 25$. Thus our problem is now reduced to evaluating 3^5 and 3^{25} modulo 31. A simple calculation gives

$$3^5 \equiv (27)9 \equiv (-4)9 \equiv -36 \equiv 26 \pmod{31},$$
$$3^{25} \equiv (3^5)^5 \equiv (26)^5 \equiv (-5)^5 \equiv (-125)(25) \equiv -1(25) \equiv 6 \pmod{31},$$

so that 6 and 26 are the only integers having order 6 modulo 31.

PROBLEMS

1. If p is an odd prime, prove that
   (a) the only incongruent solutions of $x^2 \equiv 1 \pmod{p}$ are 1 and $p-1$;
   (b) the congruence $x^{p-2} + \cdots + x^2 + x + 1 \equiv 0 \pmod{p}$ has exactly $p-2$ incongruent solutions and they are $2, 3, \ldots, p-1$.

2. Verify that each of the congruences $x^2 \equiv 1 \pmod{15}$, $x^2 \equiv -1 \pmod{65}$ and $x^2 \equiv -2 \pmod{33}$ has four incongruent solutions; hence, Lagrange's Theorem need not hold if the modulus is a composite number.

3. Determine all the primitive roots of the primes $p = 17$, 19, and 23, expressing each as a power of some one of the roots.

4. Given that 3 is a primitive root of 43, find
   (a) all positive integers less than 43 having order 6 modulo 43;
   (b) all positive integers less than 43 having order 21 modulo 43.

5. Find all positive integers less than 61 having order 4 modulo 61.

COMPOSITE NUMBERS HAVING PRIMITIVE ROOTS

We saw earlier that 2 is a primitive root of 9, so that composite numbers can also possess primitive roots. The next step of our program is to determine all composite numbers for which there exist primitive roots. Some information is available in the following two negative results.

THEOREM 8-7. *For $k \geq 3$, the integer 2^k has no primitive roots.*

Proof: For reasons that will become clear later, we start by showing that if a is an odd integer, then for $k \geq 3$

$$a^{2^{k-2}} \equiv 1 \pmod{2^k}.$$

If $k = 3$, this congruence becomes $a^2 \equiv 1 \pmod{8}$, which is certainly true (indeed, $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod{8}$). For $k > 3$, we proceed by induction on k. Assume that the asserted congruence holds for the integer k; that is, $a^{2^{k-2}} \equiv 1 \pmod{2^k}$. This is equivalent to the equation

$$a^{2^{k-2}} = 1 + b2^k,$$

where b is an integer. Squaring both sides, we obtain

$$\begin{aligned} a^{2^{k-1}} = (a^{2^{k-2}})^2 &= 1 + 2(b2^k) + (b2^k)^2 \\ &= 1 + 2^{k+1}(b + b^2 2^{k-1}) \\ &\equiv 1 \pmod{2^{k+1}}, \end{aligned}$$

so that the asserted congruence holds for $k+1$ and hence for all $k \geq 3$.

Now the integers which are relatively prime to 2^k are precisely the odd integers; also, $\phi(2^k) = 2^{k-1}$. By what was just proved, if a is an odd integer and $k \geq 3$,

$$a^{\phi(2^k)/2} \equiv 1 \pmod{2^k}$$

and, consequently, there are no primitive roots of 2^k.

THEOREM 8-8. *If* $\gcd(m, n) = 1$, *where* $m > 2$ *and* $n > 2$, *then the integer* mn *has no primitive roots.*

Proof: Consider any integer a for which $\gcd(a, mn) = 1$; then $\gcd(a, m) = 1$ and $\gcd(a, n) = 1$. Put $h = \operatorname{lcm}(\phi(m), \phi(n))$ and $d = \gcd(\phi(m), \phi(n))$.

Since $\phi(m)$ and $\phi(n)$ are both even (Theorem 7-4), surely $d \geq 2$. In consequence,

$$h = \frac{\phi(m)\phi(n)}{d} \leq \frac{\phi(mn)}{2}.$$

Now Euler's Theorem asserts that $a^{\phi(m)} \equiv 1 \pmod{m}$. Raising this equation to the $\phi(n)/d$ power, we get

$$a^h = (a^{\phi(m)})^{\phi(n)/d} \equiv 1^{\phi(n)/d} \equiv 1 \pmod{m}.$$

Similar reasoning leads to $a^h \equiv 1 \pmod{n}$. Together with the hypothesis $\gcd(m, n) = 1$, these congruences force the conclusion that

$$a^h \equiv 1 \pmod{mn}.$$

The point which we wish to make is that the order of any integer relatively prime to mn does not exceed $\phi(mn)/2$, whence there can be no primitive roots for mn.

Some special cases of Theorem 8-8 are of particular interest and we list these below.

COROLLARY. *The integer n fails to have a primitive root if either*

(1) *n is divisible by two odd primes, or*

(2) *n is of the form $n = 2^m p^k$, where p is an odd prime and $m \geq 2$.*

The significant feature of this last series of results is that they restrict our search for primitive roots to the integers 2, 4, p^k and $2p^k$, where p is an odd prime. In this section, we shall prove that each of the numbers just mentioned has a primitive root, the major task being the establishment of the existence of primitive roots for powers of an odd prime. The argument is somewhat long-winded, but otherwise routine; for the sake of clarity, it is broken down into several steps.

LEMMA 1. *If p is an odd prime, then there exists a primitive root r of p such that $r^{p-1} \not\equiv 1 \pmod{p^2}$.*

Proof: From Theorem 8-6, it is known that p has primitive roots. Choose any one, call it r. If $r^{p-1} \not\equiv 1 \pmod{p^2}$, then we are finished.

In the contrary case, replace r by $r' = r + p$, which is also a primitive root of p. Then employing the Binomial Theorem,

$$(r')^{p-1} \equiv (r+p)^{p-1} \equiv r^{p-1} + (p-1)pr^{p-2} \pmod{p^2}.$$

But we have assumed that $r^{p-1} \equiv 1 \pmod{p^2}$; hence

$$(r')^{p-1} \equiv 1 - pr^{p-2} \pmod{p^2}.$$

Since r is a primitive root of p, $\gcd(r, p) = 1$ and so $p \nmid r^{p-2}$. The outcome of all this is that $(r')^{p-1} \not\equiv 1 \pmod{p^2}$, as desired.

COROLLARY. *If p is an odd prime, then p^2 has a primitive root; in fact, for a primitive root r of p, either r or $r + p$ is a primitive root of p^2.*

Proof: The assertion is almost obvious: If r is a primitive root of p, then the order of r modulo p^2 is either $p - 1$ or else $p(p - 1) = \phi(p^2)$. The foregoing proof shows that if r has order $p - 1$ modulo p^2, then $r + p$ will be a primitive root of p^2.

To reach our goal, another somewhat technical lemma is needed.

LEMMA 2. *Let p be an odd prime and r be a primitive root of p such that $r^{p-1} \not\equiv 1 \pmod{p^2}$. Then for each positive integer $k \geq 2$,*

$$r^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}.$$

Proof: The proof proceeds by induction on k. By hypothesis, the assertion holds for $k = 2$. Let us assume that it is true for some $k \geq 2$ and show that it is true for $k + 1$. Since $\gcd(r, p^{k-1}) = \gcd(r, p^k) = 1$, Euler's Theorem indicates that

$$r^{p^{k-2}(p-1)} = r^{\phi(p^{k-1})} \equiv 1 \pmod{p^{k-1}}.$$

Hence, there exists an integer a satisfying

$$r^{p^{k-2}(p-1)} = 1 + ap^{k-1},$$

where $p \nmid a$ by our induction hypothesis. Raise both sides of this last-written equation to the pth power and expand to obtain

$$r^{p^{k-1}(p-1)} = (1 + ap^{k-1})^p \equiv 1 + ap^k \pmod{p^{k+1}}.$$

Since the integer a is not divisible by p, we have

$$r^{p^{k-1}(p-1)} \not\equiv 1 \pmod{p^{k+1}}.$$

This completes the induction step, thereby proving the lemma.

THEOREM 8-9. *If p is an odd prime number and $k \geq 1$, then there exists a primitive root for p^k.*

Proof: The two lemmas allow us to choose a primitive root r of p for which $r^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}$; in fact, any r satisfying the condition $r^{p-1} \not\equiv 1 \pmod{p^2}$ will do. We argue that such an r serves as a primitive root for all powers of p.

Let n be the order of r modulo p^k. In compliance with Theorem 8-1, n must divide $\phi(p^k) = p^{k-1}(p-1)$. Since $r^n \equiv 1 \pmod{p^k}$ implies that $r^n \equiv 1 \pmod{p}$, we also have $p-1 \mid n$ (Theorem 8-1 serves again). Consequently, n assumes the form $n = p^m(p-1)$, where $0 \leq m \leq k-1$. If it happened that $n \neq p^{k-1}(p-1)$, then $p^{k-2}(p-1)$ would be divisible by n and we would arrive at

$$r^{p^{k-2}(p-1)} \equiv 1 \pmod{p^k},$$

contradicting the way in which r was initially picked. Therefore, $n = p^{k-1}(p-1)$ and r is a primitive root for p^k.

This leaves only the case $2p^k$ for our consideration.

COROLLARY. *There are primitive roots for $2p^k$, where p is an odd prime and $k \geq 1$.*

Proof: Let r be a primitive root for p^k. There is no harm in assuming that r is an odd integer; for, if it is even, then $r + p^k$ is odd and is still a primitive root for p^k. Then $\gcd(r, 2p^k) = 1$. The order n of r modulo $2p^k$ must divide

$$\phi(2p^k) = \phi(2)\phi(p^k) = \phi(p^k).$$

But $r^n \equiv 1 \pmod{2p^k}$ implies that $r^n \equiv 1 \pmod{p^k}$, and so $\phi(p^k) \mid n$. Together these divisibility conditions force $n = \phi(2p^k)$, making r a primitive root of $2p^k$.

The prime 5 has $\phi(4) = 2$ primitive roots, namely the integers 2 and 3. Since

$$2^{5-1} \equiv 16 \not\equiv 1 \pmod{25} \quad \text{and} \quad 3^{5-1} \equiv 6 \not\equiv 1 \pmod{25},$$

..

these also serve as primitive roots for 5^2, hence for all higher powers of 5. The proof of the last corollary guarantees that 3 is a primitive root for all numbers of the form $2 \cdot 5^k$.

We summarize what has been accomplished in

THEOREM 8-10. *An integer $n > 1$ has a primitive root if and only if*

$$n = 2,\ 4,\ p^k,\ \text{or}\ 2p^k,$$

where p is an odd prime.

Proof: By virtue of Theorems 8-7 and 8-8, the only positive integers with primitive roots are those mentioned in the statement of our theorem. It may be checked that 1 is a primitive root for 2, while 3 is a primitive root of 4. We have just finished proving that primitive roots exist for any power of an odd prime and for twice such a power.

This seems the opportune moment to mention that Euler gave an essentially correct (although incomplete) proof in 1773 of the existence of primitive roots for any prime p and listed all the primitive roots for $p \leq 37$. Legendre, using Lagrange's Theorem, managed to repair the deficiency and showed (1785) that there are $\phi(d)$ integers of order d for each $d \mid (p-1)$. The greatest advances in this direction were made by Gauss when, in 1801, he published a proof that there exist primitive roots of n if and only if $n = 2,\ 4,\ p^k$, and $2p^k$, where p is an odd prime.

PROBLEMS

1. (a) Find the four primitive roots of 26 and the eight primitive roots of 25.
   (b) Determine all the primitive roots of 3^2, 3^3 and 3^4.
2. For an odd prime p, establish the following facts:
   (a) There are as many primitive roots of $2p^n$ as of p^n.
   (b) Any primitive root r of p^n is also a primitive root of p. [*Hint:* Let r have order k modulo p. Show that $r^{pk} \equiv 1 \pmod{p^2}, \ldots, r^{p^{n-1}k} \equiv 1 \pmod{p^n}$, hence $\phi(p^n) \mid p^{n-1}k$.]
   (c) A primitive root of p^2 is also a primitive root of p^n for $n \geq 2$.
3. If r is a primitive root of p^2, p being an odd prime, show that the solutions of the congruence $x^{p-1} \equiv 1 \pmod{p^2}$ are precisely the integers $r^p, r^{2p}, \ldots, r^{(p-1)p}$.
4. (a) Prove that 3 is a primitive root of all integers of the form 7^k and $2 \cdot 7^k$.
   (b) Find a primitive root for any integer of the form 17^k.
5. Obtain all the primitive roots of 41 and 82.

EULER'S CRITERION

As the heading suggests, the present chapter has as its goal another major contribution of Gauss: the Quadratic Reciprocity Law. For those who consider the theory of numbers "the Queen of Mathematics," this is one of the jewels in her crown. The instrinsic beauty of the Quadratic Reciprocity Law has long exerted a strange fascination for mathematicians. Since Gauss' time, over a hundred proofs of it, all more or less different, have been published (in fact, Gauss himself eventually devised seven). Among the eminent mathematicians of the 19th century who contributed their proofs appear the names of Cauchy, Jacobi, Dirichlet, Eisenstein, Kronecker, and Dedekind.

Roughly speaking, the Quadratic Reciprocity Law deals with the solvability of quadratic congruences. It therefore seems appropriate to begin by considering the congruence

$$ax^2 + bx + c \equiv 0 \pmod{p}, \tag{1}$$

where p is an odd prime and $a \not\equiv 0 \pmod{p}$; that is, $\gcd(a, p) = 1$. The supposition that p is an odd prime implies that $\gcd(4a, p) = 1$. Thus, congruence (1) is equivalent to

$$4a(ax^2 + bx + c) \equiv 0 \pmod{p}.$$

Using the identity

$$4a(ax^2 + bx + c) = (2ax + b)^2 - (b^2 - 4ac),$$

the last-written congruence may be expressed as

$$(2ax + b)^2 \equiv (b^2 - 4ac) \pmod{p}.$$

Now put $y = 2ax + b$ and $d = b^2 - 4ac$ to get

$$y^2 \equiv d \pmod{p}. \tag{2}$$

If $x \equiv x_0 \pmod{p}$ is a solution of (1), then $y \equiv 2ax_0 + b \pmod{p}$ satisfies the congruence (2). Conversely, if $y \equiv y_0 \pmod{p}$ is a solution of (2), then $2ax \equiv y_0 - b \pmod{p}$ can be solved to obtain a solution of (1).

Thus, the problem of finding a solution to the quadratic congruence (1) is equivalent to that of finding a solution to a linear congruence and a quadratic congruence of the form

$$x^2 \equiv a \pmod{p}. \tag{3}$$

If $p \mid a$, then (3) has $x \equiv 0 \pmod{p}$ as its only solution. To avoid trivialities, let us agree to assume hereafter that $p \nmid a$.

Granting this, whenever $x^2 \equiv a \pmod{p}$ admits a solution $x = x_0$, then there is also a second solution $x = p - x_0$. This second solution is not congruent to the first. For $x_0 \equiv p - x_0 \pmod{p}$ implies that $2x_0 \equiv 0 \pmod{p}$, or $x_0 \equiv 0 \pmod{p}$, which is impossible. By Lagrange's Theorem, these two solutions exhaust the incongruent solutions of $x^2 \equiv a \pmod{p}$. In short: $x^2 \equiv a \pmod{p}$ has exactly two solutions or no solutions.

A simple numerical example of what we have just said is provided by the congruence

$$5x^2 - 6x + 2 \equiv 0 \pmod{13}.$$

To obtain the solution, one replaces this congruence by the simpler one

$$y^2 \equiv 9 \pmod{13}$$

with solutions $y \equiv 3, 10 \pmod{13}$. Next, solve the linear congruences

$$10x \equiv 9 \pmod{13}, \quad 10x \equiv 16 \pmod{13}.$$

It is not difficult to see that $x \equiv 10, 12 \pmod{13}$ satisfy these equations and, by our previous remarks, the original quadratic congruence also.

The major effort in this presentation is directed towards providing a test for the existence of solutions of the congruence

$$x^2 \equiv a \pmod{p}, \quad \gcd(a, p) = 1. \tag{4}$$

To put it differently, we wish to identify those integers a which are perfect squares modulo p. Some additional terminology will help us to discuss this situation in a concise way:

DEFINITION 9-1. Let p be an odd prime and $\gcd(a, p) = 1$. If the congruence $x^2 \equiv a \pmod{p}$ has a solution, then a is said to be a *quadratic residue of* p. Otherwise, a is called a *quadratic nonresidue* of p.

The point to be borne in mind is that if $a \equiv b \pmod{p}$, then a is a quadratic residue of p if and only if b is a quadratic residue of p. Thus, we need only determine the quadratic character of those positive integers less than p in order to ascertain that of any integer.

Example 9-1

Consider the case of the prime $p = 13$. To find out how many of the integers $1, 2, 3, \ldots, 12$ are quadratic residues of 13, we must know which of the congruences

$$x^2 \equiv a \pmod{13}$$

are solvable when a runs through the set $\{1, 2, \ldots, 12\}$. Modulo 13, the squares of the integers $1, 2, 3, \ldots, 12$ are

$$1^2 \equiv 12^2 \equiv 1,$$
$$2^2 \equiv 11^2 \equiv 4,$$
$$3^2 \equiv 10^2 \equiv 9,$$
$$4^2 \equiv 9^2 \equiv 3,$$
$$5^2 \equiv 8^2 \equiv 12,$$
$$6^2 \equiv 7^2 \equiv 10.$$

Consequently, the quadratic residues of 13 are 1, 3, 4, 9, 10, 12, while the nonresidues are 2, 5, 6, 7, 8, 11. Observe that the integers between 1 and 12 are divided equally among the quadratic residues and nonresidues; this is typical of the general situation.

Euler devised a simple criterion for deciding whether an integer a is a quadratic residue of a given prime p.

THEOREM 9-1 (Euler's Criterion). *Let p be an odd prime and* $\gcd(a, p) = 1$. *Then a is a quadratic residue of p if and only if* $a^{(p-1)/2} \equiv 1 \pmod{p}$.

Proof: Suppose that a is a quadratic residue of p, so that $x^2 \equiv a \pmod{p}$ admits a solution, call it x_1. Since $\gcd(a, p) = 1$, evidently $\gcd(x_1, p) = 1$. We may therefore appeal to Fermat's Theorem to obtain

$$a^{(p-1)/2} \equiv (x_1^2)^{(p-1)/2} \equiv x_1^{p-1} \equiv 1 \pmod{p}.$$

For the opposite direction, assume that $a^{(p-1)/2} \equiv 1 \pmod{p}$ holds and let r be a primitive root of p. Then $a \equiv r^k \pmod{p}$ for some integer k, with $1 \leq k \leq p-1$. It follows that

$$r^{k(p-1)/2} \equiv a^{(p-1)/2} \equiv 1 \pmod{p}.$$

By Theorem 8-1, the order of r (namely, $p-1$) must divide the exponent $k(p-1)/2$. The implication is that k is an even integer, say $k = 2j$. Hence,

$$(r^j)^2 = r^{2j} = r^k \equiv a \pmod{p},$$

making the integer r^j a solution of the congruence $x^2 \equiv a \pmod{p}$. This proves that a is a quadratic residue of the prime p.

Now if p (as always) is an odd prime and $\gcd(a, p) = 1$, then

$$(a^{(p-1)/2} - 1)(a^{(p-1)/2} + 1) = a^{p-1} - 1 \equiv 0 \pmod{p},$$

the last congruence being justified by Fermat's Theorem. Hence either

$$a^{(p-1)/2} \equiv 1 \pmod{p} \quad \text{or} \quad a^{(p-1)/2} \equiv -1 \pmod{p},$$

but not both. For, if both congruences held simultaneously, then we would have $1 \equiv -1 \pmod{p}$, or equivalently, $p \mid 2$, which conflicts with our hypothesis. Since a quadratic nonresidue of p does not satisfy $a^{(p-1)/2} \equiv 1 \pmod{p}$, it must therefore satisfy $a^{(p-1)/2} \equiv -1 \pmod{p}$. This observation provides an alternate formulation of Euler's Criterion: the integer a is a quadratic nonresidue of p if and only if $a^{(p-1)/2} \equiv -1 \pmod{p}$.

COROLLARY. *Let p be an odd prime and $\gcd(a, p) = 1$. Then a is a quadratic residue or nonresidue of p according as*

$$a^{(p-1)/2} \equiv 1 \pmod{p} \quad \textit{or} \quad a^{(p-1)/2} \equiv -1 \pmod{p}.$$

Example 9-2

In the case $p = 13$, we find that

$$2^{(13-1)/2} = 2^6 = 64 \equiv 12 \equiv -1 \pmod{13}.$$

Thus, by virtue of the last corollary, the integer 2 is a quadratic nonresidue of 13. Since

$$3^{(13-1)/2} = 3^6 = (27)^2 \equiv 1^2 \equiv 1 \pmod{13},$$

the same result indicates that 3 is a quadratic residue of 13 and so the congruence $x^2 \equiv 3 \pmod{13}$ is solvable; in fact, its two incongruent solutions are $x \equiv 4$ and $9 \pmod{13}$.

There is an alternative proof of Euler's Criterion (due to Dirichlet) which is longer, but perhaps more illuminating. The reasoning proceeds as follows: Let a be a quadratic nonresidue of p and let c be any one of the integers $1, 2, \ldots, p-1$. By the theory of linear congruences, there exists a solution c' of $cx \equiv a \pmod{p}$, with c' also in the set $\{1, 2, \ldots, p-1\}$. Notice that $c' \neq c$, for otherwise we would have $c^2 \equiv a \pmod{p}$, contradicting what we assumed. Thus, the integers between 1 and $p-1$ can be divided into $(p-1)/2$ pairs c, c', where $cc' \equiv a \pmod{p}$. This leads to $(p-1)/2$ congruences,

$$\begin{aligned} c_1 c_1' &\equiv a \pmod{p}, \\ c_2 c_2' &\equiv a \pmod{p}, \\ &\vdots \\ c_{(p-1)/2}\, c'_{(p-1)/2} &\equiv a \pmod{p}. \end{aligned}$$

Multiplying them together and observing that the product

$$c_1 c_1' c_2 c_2' \cdots c_{(p-1)/2}\, c'_{(p-1)/2}$$

is simply a rearrangement of $1 \cdot 2 \cdot 3 \cdots (p-1)$, we obtain

$$(p-1)! \equiv a^{(p-1)/2} \pmod{p}.$$

At this point, Wilson's Theorem enters the picture; for, $(p-1)! \equiv -1 \pmod{p}$, so that

$$a^{(p-1)/2} \equiv -1 \pmod{p},$$

which is Euler's Criterion when a is a quadratic nonresidue of p.

We next examine the case in which a is a quadratic residue of p. In this setting the congruence $x^2 \equiv a \pmod{p}$ admits two solutions $x = x_1$ and $x = p - x_1$, for some x_1 with $1 \leq x_1 \leq p-1$. If x_1 and $p - x_1$ are removed from the set $\{1, 2, \ldots, p-1\}$, then the remaining $p-3$ integers can be grouped into pairs c, c' (where $c \neq c'$) such that $cc' \equiv a \pmod{p}$. To these $(p-3)/2$ congruences, add the congruence

$$x_1(p - x_1) \equiv -x_1^2 \equiv -a \pmod{p}.$$

Upon taking the product of all the congruences involved, we arrive at the relation

$$(p-1)! \equiv -a^{(p-1)/2} \pmod{p}.$$

Wilson's Theorem plays its role once again to produce

$$a^{(p-1)/2} \equiv 1 \pmod{p}.$$

Summing up, we have shown that $a^{(p-1)/2} \equiv 1 \pmod{p}$ or $a^{(p-1)/2} \equiv -1 \pmod{p}$ according as a is a quadratic residue or nonresidue of p.

Euler's Criterion is not offered as a practical test for determining whether a given integer is or is not a quadratic residue; the calculations involved are too cumbersome unless the modulus is small. But as a crisp criterion, easily worked with for theoretical purposes, it leaves little to be desired. A more effective method of computation is embodied in the Quadratic Reciprocity Law, which we shall prove later in the chapter.

PROBLEMS

1. Solve the following quadratic congruences:
   (a) $x^2 + 7x + 10 \equiv 0 \pmod{11}$;
   (b) $3x^2 + 9x + 7 \equiv 0 \pmod{13}$;
   (c) $5x^2 + 6x + 1 \equiv 0 \pmod{23}$.
2. (a) For an odd prime p, prove that the quadratic residues of p are congruent modulo p to the integers

$$1^2, 2^2, 3^2, \ldots, \left(\frac{p-1}{2}\right)^2.$$

   (b) Verify that the quadratic residues of 17 are 1, 2, 4, 8, 9, 13, 15, 16.
3. Employ the index calculus to derive Euler's Criterion. [*Hint:* See Theorem 8-2.]
4. Show that 3 is a quadratic residue of 23, but a nonresidue of 19.
5. Given that a is a quadratic residue of the odd prime p, prove that
   (a) a is not a primitive root of p;

(b) $p - a$ is a quadratic residue or nonresidue of p according as $p \equiv 1 \pmod 4$ or $p \equiv 3 \pmod 4$.

6. If $p = 2^k + 1$ is prime, establish that every quadratic nonresidue of p is a primitive root of p. [*Hint:* Apply Euler's Criterion.]

THE LEGENDRE SYMBOL AND ITS PROPERTIES

Euler's studies on quadratic residues were further developed by the French mathematician Adrien Marie Legendre (1752–1833). Legendre's memoir "Recherches d'Analyse Indéterminée" (1785) contains an account of the Quadratic Reciprocity Law and its many applications, a sketch of a theory of the representation of an integer as the sum of three squares and the statement of a theorem that was later to become famous: Every arithmetic progression $ax + b$, where $\gcd(a, b) = 1$, contains an infinite number of primes. The topics covered in "Recherches" were taken up in a more thorough and systematic fashion in his *Essai sur la Théorie des Nombres*, which appeared in 1798. This represented the first "modern" treatise devoted exclusively to number theory, its precursors being translations or commentaries on Diophantus. Legendre's *Essai* was subsequently expanded into his *Théorie des Nombres*. The results of his later research papers, inspired to a large extent by Gauss, were included in 1830 in a two-volume third edition of the *Théorie des Nombres*. This remained, together with the *Disquisitiones Arithmeticae* of Gauss, a standard work on the subject for many years. Although Legendre made no great innovations in number theory, he raised fruitful questions which provided subjects of investigation for the mathematicians of the 19th century.

Before leaving Legendre's mathematical contributions, we should mention that he is also known for his work on elliptic integrals and for his *Eléments de Géométrie* (1794). In this last book, he attempted a pedagogical improvement of Euclid's *Elements* by rearranging and simplifying many of the proofs without lessening the rigor of the ancient treatment. The result was so favorably received that it became one of the most successful textbooks ever written, dominating

instruction in geometry for over a century through its numerous editions and translations. An English translation was made in 1824 by the famous Scottish essayist and historian Thomas Carlyle, who was in early life a teacher of mathematics; Carlyle's translation ran through 33 American editions, the last not appearing until 1890. In fact, Legendre's revision was used at Yale University as late as 1885, when Euclid was finally abandoned as a text.

Our future efforts will be greatly simplified by the use of the symbol (a/p); this notation was introduced by Legendre in his *Essai* and is called, naturally enough, the Legendre symbol.

DEFINITION 9-2. Let p be an odd prime and $\gcd(a, p) = 1$. The *Legendre symbol* (a/p) is defined by

$$(a/p) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue of } p \\ -1 & \text{if } a \text{ is a quadratic nonresidue of } p \end{cases}$$

For the want of better terminology, we shall refer to a as the *numerator* and p as the *denominator* of the symbol (a/p). Other standard notations for the Legendre symbol are $\left(\frac{a}{p}\right)$ or $(a \mid p)$.

Example 9-3

Let us look at the prime $p = 13$, in particular. Using the Legendre symbol, the results of an earlier example may be expressed as

$$(1/13) = (3/13) = (4/13) = (9/13) = (10/13) = (12/13) = 1$$

and

$$(2/13) = (5/13) = (6/13) = (7/13) = (8/13) = (11/13) = -1.$$

REMARK: For $p \mid a$, we have purposely left the symbol (a/p) undefined. Some authors find it convenient to extend Legendre's definition to this case by setting $(a/p) = 0$. One advantage of this would be that the number of solutions of $x^2 \equiv a \pmod{p}$ can then be given by the simple formula $1 + (a/p)$.

The next theorem sets in evidence certain elementary facts concerning the Legendre symbol.

THEOREM 9-2. *Let p be an odd prime and a and b be integers which are relatively prime to p. Then the Legendre symbol has the following properties:*

(1) *If* $a \equiv b \pmod{p}$, *then* $(a/p) = (b/p)$.

(2) $(a^2/p) = 1$.

(3) $(a/p) \equiv a^{(p-1)/2} \pmod{p}$.

(4) $(ab/p) = (a/p)(b/p)$.

(5) $(1/p) = 1$ and $(-1/p) = (-1)^{(p-1)/2}$.

Proof: If $a \equiv b \pmod{p}$, then $x^2 \equiv a \pmod{p}$ and $x^2 \equiv b \pmod{p}$ have exactly the same solutions, if any at all. Thus $x^2 \equiv a \pmod{p}$ and $x^2 \equiv b \pmod{p}$ are both solvable, or neither one has a solution. This is reflected in the statement that $(a/p) = (b/p)$.

As regards (2), observe that the integer a trivially satisfies the congruence $x^2 \equiv a^2 \pmod{p}$; hence, $(a^2/p) = 1$. Part (3) is just the corollary to Theorem 9-1 rephrased in terms of the Legendre symbol. We use (3) to establish (4):

$$(ab/p) \equiv (ab)^{(p-1)/2} \equiv a^{(p-1)/2} b^{(p-1)/2} \equiv (a/p)(b/p) \pmod{p}.$$

Now the Legendre symbol assumes only the values 1 or -1. Were $(ab/p) \neq (a/p)(b/p)$, we would have $1 \equiv -1 \pmod{p}$ or $2 \equiv 0 \pmod{p}$; this cannot occur, since $p > 2$. It follows that

$$(ab/p) = (a/p)(b/p).$$

Finally, we observe that the first equality in (5) is a special case of (2), while the second one is obtained from property (3) upon setting $a = -1$. Since the quantities $(-1/p)$ and $(-1)^{(p-1)/2}$ are either 1 or -1, the resulting congruence

$$(-1/p) \equiv (-1)^{(p-1)/2} \pmod{p}$$

implies that $(-1/p) = (-1)^{(p-1)/2}$.

From parts (2) and (4) of Theorem 9-2, we may also abstract the relation

$$(6) \qquad (ab^2/p) = (a/p)(b^2/p) = (a/p).$$

In other words, a square factor which is relatively prime to p can be deleted from the numerator of the Legendre symbol without affecting its value.

Since $(p-1)/2$ is even for p of the form $4k+1$ and odd for p of the form $4k+3$, the equation $(-1/p) = (-1)^{(p-1)/2}$ permits us to add a small supplement to Theorem 9-2.

COROLLARY. *If p is an odd prime, then*

$$(-1/p) = \begin{cases} 1 \text{ if } p \equiv 1 \pmod 4 \\ -1 \text{ if } p \equiv 3 \pmod 4 \end{cases}$$

This corollary may be viewed as asserting that the congruence $x^2 \equiv -1 \pmod{p}$ has a solution if and only if p is a prime of the form $4k+1$. The result is not new, of course; we have merely provided the reader with a different path to Theorem 5-3.

Example 9-4

Let us ascertain whether the congruence $x^2 \equiv -38 \pmod{13}$ is solvable. This can be done by evaluating the symbol $(-38/13)$. We first appeal to parts (4) and (5) of Theorem 9-2 to write

$$(-38/13) = (-1/13)(38/13) = (38/13).$$

Since $38 \equiv 12 \pmod{13}$, it follows that

$$(38/13) = (12/13).$$

Now property (6) above gives

$$(12/13) = (3 \cdot 2^2/13) = (3/13).$$

But

$$(3/13) \equiv 3^{(13-1)/2} \equiv 3^6 \equiv (27)^2 \equiv 1 \pmod{13},$$

where we have made appropriate use of (3) of Theorem 9-2; hence, $(3/13) = 1$. Inasmuch as $(-38/13) = 1$, the quadratic congruence $x^2 \equiv -38 \pmod{13}$ admits solution.

The Corollary to Theorem 9-2 lends itself to an application concerning the distribution of primes.

THEOREM 9-3. *There are infinitely many primes of the form* $4k + 1$.

Proof: Suppose that there are finitely many such primes; call them $p_1, p_2, \ldots, p_n$ and consider the integer

$$N = (2p_1 p_2 \cdots p_n)^2 + 1.$$

Clearly N is odd, so that there exists some odd prime p with $p \mid N$. To put it another way,

$$(2p_1 p_2 \cdots p_n)^2 \equiv -1 \pmod{p}$$

or, if one prefers to phrase this in terms of the Legendre symbol, $(-1/p) = 1$. But the relation $(-1/p) = 1$ holds only if p is of the form $4k + 1$. Hence, p is one of the primes p_i. This implies that p_i divides $N - (2p_1 p_2 \cdots p_n)^2$, or $p_i \mid 1$, a contradiction. The conclusion: there must exist infinitely many primes of the form $4k + 1$.

THEOREM 9-4. *If p is an odd prime, then*

$$\sum_{a=1}^{p-1} (a/p) = 0.$$

Hence, there are precisely $(p-1)/2$ *quadratic residues and* $(p-1)/2$ *quadratic nonresidues of* p.

Proof: Let r be a primitive root of p. We know that, modulo p, the powers $r, r^2, \ldots, r^{p-1}$ are just a permutation of the integers 1,

$2, \ldots, p-1$. Thus for any a between 1 and $p-1$, inclusive, there exists a unique positive integer $k\,(1 \leq k \leq p-1)$, such that $a \equiv r^k \pmod{p}$. By appropriate use of Euler's Criterion, we have

$$(1) \qquad (a/p) = (r^k/p) \equiv (r^k)^{(p-1)/2} = (r^{(p-1)/2})^k \equiv (-1)^k \pmod{p},$$

where, since r is a primitive root of p, $r^{(p-1)/2} \equiv -1 \pmod{p}$. But (a/p) and $(-1)^k$ are equal to either 1 or -1, so that equality holds in (1). Now add up the Legendre symbols in question to obtain

$$\sum_{a=1}^{p-1} (a/p) = \sum_{k=1}^{p-1} (-1)^k = 0,$$

the desired conclusion.

COROLLARY. *The quadratic residues of an odd prime p are congruent modulo p to the even powers of a primitive root r of p; the quadratic nonresidues are congruent to the odd powers of r.*

For an illustration of the idea just introduced, we again fall back on the prime $p = 13$. Since 2 is a primitive root of 13, the quadratic residues of 13 are given by the even powers of 2, namely,

$$2^2 \equiv 4 \qquad 2^8 \equiv 9$$
$$2^4 \equiv 3 \qquad 2^{10} \equiv 10$$
$$2^6 \equiv 12 \qquad 2^{12} \equiv 1$$

all congruences being modulo 13. Similarly, the nonresidues occur as the odd powers of 2:

$$2^1 \equiv 2 \qquad 2^7 \equiv 11$$
$$2^3 \equiv 8 \qquad 2^9 \equiv 5$$
$$2^5 \equiv 6 \qquad 2^{11} \equiv 7.$$

Most proofs of the Quadratic Reciprocity Law, and ours as well, rest ultimately upon what is known as Gauss' Lemma. While this lemma gives the quadratic character of an integer, it is more useful from a theoretical point of view than as a computational device.

THEOREM 9-5 (Gauss' Lemma). *Let p be an odd prime and let* $\gcd(a, p) = 1$. *If n denotes the number of integers in the set*

$$S = \left\{a, 2a, 3a, \ldots, \left(\frac{p-1}{2}\right)a\right\}$$

whose remainders upon division by p exceed $p/2$, then

$$(a/p) = (-1)^n.$$

Proof: Since $\gcd(a, p) = 1$, none of the $(p-1)/2$ integers in S is congruent to zero and no two are congruent to each other modulo p. Let $r_1, \ldots, r_m$ be those remainders upon division by p such that $0 < r_i < p/2$ and $s_1, \ldots, s_n$ be those remainders such that $p > s_i > p/2$. Then $m + n = (p-1)/2$, and the integers

$$r_1, \ldots, r_m, p - s_1, \ldots, p - s_n$$

are all positive and less than $p/2$.

In order to prove that these integers are all distinct, it suffices to show that no $p - s_i$ is equal to any r_j. Assume to the contrary that

$$p - s_i = r_j$$

for some choice of i and j. Then there exist integers u and v, with $1 \leq u, v \leq (p-1)/2$, satisfying $s_i \equiv ua \pmod{p}$ and $r_j \equiv va \pmod{p}$. Hence,

$$(u + v)a \equiv s_i + r_j \equiv p \equiv 0 \pmod{p}$$

which says that $u + v \equiv 0 \pmod{p}$. But the latter congruence cannot take place, since $1 < u + v \leq p - 1$.

The point which we wish to bring out is that the $(p-1)/2$ numbers

$$r_1, \ldots, r_m, p - s_1, \ldots, p - s_n$$

are simply the integers $1, 2, \ldots, (p-1)/2$, not necessarily in order of appearance. Thus, their product is $[(p-1)/2]!$:

$$\left(\frac{p-1}{2}\right)! = r_1 \cdots r_m (p-s_1)\cdots(p-s_n)$$
$$\equiv r_1 \cdots r_m (-s_1)\cdots(-s_n) \pmod{p}$$
$$\equiv (-1)^n r_1 \cdots r_m s_1 \cdots s_n \pmod{p}.$$

But we know that $r_1, \ldots, r_m, s_1, \ldots, s_n$ are congruent modulo p to $a, 2a, \ldots, [(p-1)/2]a$, in some order, so that

$$\left(\frac{p-1}{2}\right)! \equiv (-1)^n a \cdot 2a \cdots \left(\frac{p-1}{2}\right) a \pmod{p}$$
$$\equiv (-1)^n a^{(p-1)/2}\left(\frac{p-1}{2}\right)! \pmod{p}.$$

Since $[(p-1)/2]!$ is relatively prime to p, it may be cancelled from both sides of this congruence to give

$$1 \equiv (-1)^n a^{(p-1)/2} \pmod{p}$$

or, upon multiplying by $(-1)^n$,

$$a^{(p-1)/2} \equiv (-1)^n \pmod{p}.$$

Use of Euler's Criterion now completes the argument:

$$(a/p) \equiv a^{(p-1)/2} \equiv (-1)^n \pmod{p},$$

which implies that

$$(a/p) = (-1)^n.$$

By way of illustration, let $p = 13$ and $a = 5$. Then $(p-1)/2 = 6$, so that

$$S = \{5, 10, 15, 20, 25, 30\}.$$

Three of these are greater than 13/2; hence, $n = 3$ and Theorem 9-5 says that

$$(5/13) = (-1)^3 = -1.$$

Gauss' Lemma allows us to proceed to a variety of interesting results. For one thing, it provides a means for determining which primes have 2 as a quadratic residue.

THEOREM 9-6. *If p is an odd prime, then*

$$(2/p) = \begin{cases} 1 \text{ if } p \equiv 1 \pmod 8 \quad or \quad p \equiv 7 \pmod 8; \\ -1 \text{ if } p \equiv 3 \pmod 8 \quad or \quad p \equiv 5 \pmod 8. \end{cases}$$

Proof: According to Gauss' Lemma, $(2/p) = (-1)^n$, where n is the number of integers in the set

$$S = \left\{2, 2 \cdot 2, 3 \cdot 2, \ldots, \left(\frac{p-1}{2}\right) \cdot 2\right\}$$

which, upon division by p, have remainders greater than $p/2$. The members of S are all less than p, so that it suffices to count the number that exceed $p/2$. For $1 \leq k \leq (p-1)/2$, $2k < p/2$ if and only if $k < p/4$. If [ ] denotes the greatest integer function, then there are $[p/4]$ integers in S less than $p/2$, hence

$$n = \frac{p-1}{2} - [p/4]$$

integers which are greater than $p/2$.

Now we have four possibilities; for, any odd prime has one of the forms $8k + 1$, $8k + 3$, $8k + 5$, or $8k + 7$. A simple calculation shows that

if $p = 8k + 1$, then $n = 4k - [2k + \frac{1}{4}] = 4k - 2k = 2k$,

if $p = 8k + 3$, then $n = 4k + 1 - [2k + \frac{3}{4}] = 4k + 1 - 2k = 2k + 1$,

if $p = 8k + 5$, then $n = 4k + 2 - [2k + 1 + \frac{1}{4}] = 4k + 2 - (2k + 1)$
$= 2k + 1$,

if $p = 8k + 7$, then $n = 4k + 3 - [2k + 1 + \frac{3}{4}] = 4k + 3 - (2k + 1)$
$= 2k + 2$.

Thus, when p is of the form $8k + 1$ or $8k + 7$, n is even and $(2/p) = 1$; on the other hand, when p assumes the form $8k + 3$ or $8k + 5$, n is odd and $(2/p) = -1$.

Notice that if the odd prime p is of the form $8k \pm 1$ (equivalently, $p \equiv 1 \pmod 8$ or $p \equiv 7 \pmod 8$), then

$$\frac{p^2 - 1}{8} = \frac{(8k \pm 1)^2 - 1}{8} = \frac{64k^2 \pm 16k}{8} = 8k^2 \pm 2k,$$

which is an even integer; in this situation, $(-1)^{(p^2-1)/8} = 1 = (2/p)$. On the other hand, if p is of the form $8k \pm 3$ (equivalently, $p \equiv 1 \pmod 8$ or $p \equiv 5 \pmod 8$), then

$$\frac{p^2 - 1}{8} = \frac{(8k \pm 3)^2 - 1}{8} = \frac{64k^2 \pm 48k + 8}{8} = 8k^2 \pm 6k + 1,$$

which is odd; here, we have $(-1)^{(p^2-1)/8} = -1 = (2/p)$. These observations are incorporated in the statement of the following corollary to Theorem 9-6.

COROLLARY. *If p is an odd prime, then*

$$(2/p) = (-1)^{(p^2-1)/8}.$$

It is time for another look at primitive roots. As we have remarked, there is no general technique for obtaining a primitive root of an odd prime p; the reader might, however, find the next theorem useful on occasion.

THEOREM 9-7. *If p and $2p+1$ are both odd primes, then the integer $(-1)^{(p-1)/2}2$ is a primitive root of $2p+1$.*

Proof: For ease of discussion, let us put $q = 2p+1$. We distinguish two cases: $p \equiv 1 \pmod 4$ and $p \equiv 3 \pmod 4$.

If $p \equiv 1 \pmod 4$, then $(-1)^{(p-1)/2}2 = 2$. Since $\phi(q) = q - 1 = 2p$, the order of 2 modulo q is one of the numbers 1, 2, p, or $2p$. Taking note of part (3) of Theorem 9-2, we have

$$(2/q) \equiv 2^{(q-1)/2} = 2^p \pmod q.$$

But, in the present setting, $q \equiv 3 \pmod 8$; whence, the Legendre symbol $(2/q) = -1$. It follows that $2^p \equiv -1 \pmod q$ and so 2 cannot have order p modulo q. The order of 2 being neither 1, 2, ($2^2 \equiv 1 \pmod q$ implies that $q \mid 3$, an impossibility) nor p, we are forced to conclude that the order of 2 modulo q is $2p$. This makes 2 a primitive root of q.

We now deal with the case $p \equiv 3 \pmod 4$. This time, $(-1)^{(p-1)/2}2 = -2$ and

$$(-2)^p \equiv (-2/q) = (-1/q)(2/q) \pmod q.$$

Since $q \equiv 7 \pmod 8$, the corollary to Theorem 9-2 asserts that $(-1/q) = -1$, while once again we have $(2/q) = 1$. This leads to the congruence $(-2)^p \equiv -1 \pmod q$. From here on, the argument duplicates that of the last paragraph. Without analyzing further, we announce the decision: -2 is a primitive root of q.

Theorem 9-7 indicates, for example, that the primes 11, 59, 107, and 179 have 2 as a primitive root. Likewise, the integer -2 serves as a primitive root for 7, 23, 47, and 167.

Before retiring from the field, we should mention another result of the same character: if p and $4p+1$ are both primes, then 2 is a primitive root of $4p+1$. Thus, to the list of prime numbers having 2 for a primitive root, one could add, say, 13, 29, 53, and 173.

There is an attractive proof of the infinitude of primes of the form $8k - 1$ which can be based on Theorem 9-6.

THEOREM 9-8. *There are infinitely many primes of the form* $8k - 1$.

Proof: As usual, suppose that there are only a finite number of such primes. Let these be $p_1, p_2, \ldots, p_n$ and consider the integer

$$N = (4p_1 p_2 \cdots p_n)^2 - 2.$$

There exists at least one odd prime divisor p of N, so that

$$(4p_1 p_2 \cdots p_n)^2 \equiv 2 \pmod{p}$$

or $(2/p) = 1$. In view of Theorem 9-6, $p \equiv \pm 1 \pmod 8$. If all the odd prime divisors of N were of the form $8k + 1$, then N itself would be of the form $16a + 2$; this is clearly impossible, since N is of the form $16a - 2$. Thus, N must have a prime divisor q of the form $8k - 1$. But $q \mid N$ and $q \mid (4p_1 p_2 \cdots p_n)^2$ leads to the contradiction that $q \mid 2$.

LEMMA. *If p is an odd prime and a an odd integer, with* $\gcd(a, p) = 1$, *then*

$$(a/p) = (-1)^{\sum_{k=1}^{(p-1)/2} [ka/p]}.$$

Proof: We shall employ the same notation as in the proof of Gauss' Lemma. Consider the set of integers

$$S = \left\{a, 2a, \ldots, \left(\frac{p-1}{2}\right) a\right\}.$$

Divide each of these multiples of a by p to obtain

$$ka = q_k p + t_k, \qquad 1 \le t_k \le p - 1.$$

Then $ka/p = q_k + t_k/p$, so that $[ka/p] = q_k$. Thus for $1 \le k \le (p-1)/2$, we may write ka in the form

(1) $$ka = [ka/p]p + t_k .$$

If the remainder $t_k < p/2$, then it is one of the integers $r_1, \ldots, r_m$; if $t_k > p/2$, then it is one of the integers $s_1, \ldots, s_n$.

Taking the sum of the equations (1), we get the relation

(2) $$\sum_{k=1}^{(p-1)/2} ka = \sum_{k=1}^{(p-1)/2} [ka/p]p + \sum_{k=1}^{m} r_k + \sum_{k=1}^{n} s_k .$$

It was learned in proving Gauss' Lemma that the $(p-1)/2$ numbers

$$r_1, \ldots, r_m, p - s_1, \ldots, p - s_n$$

are just a rearrangement of the integers $1, 2, \ldots, (p-1)/2$. Hence,

(3) $$\sum_{k=1}^{(p-1)/2} k = \sum_{k=1}^{m} r_k + \sum_{k=1}^{n} (p - s_k) = pn + \sum_{k=1}^{m} r_k - \sum_{k=1}^{n} s_k .$$

Subtracting (3) from (2) gives

(4) $$(a-1)\sum_{k=1}^{(p-1)/2} k = p\left(\sum_{k=1}^{(p-1)/2} [ka/p] - n\right) + 2\sum_{k=1}^{n} s_k .$$

Let us use the fact that $p \equiv a \equiv 1 \pmod 2$ and translate this last equation into a congruence modulo 2:

$$0 \cdot \sum_{k=1}^{(p-1)/2} k \equiv 1 \cdot \left(\sum_{k=1}^{(p-1)/2} [ka/p] - n\right) \pmod 2$$

or

$$n \equiv \sum_{k=1}^{(p-1)/2} [ka/p] \pmod 2.$$

The rest follows from Gauss' Lemma; for,

$$(a/p) = (-1)^n = (-1)^{\sum_{k=1}^{(p-1)/2} [ka/p]}$$

For an example of this last result, again consider $p = 13$ and $a = 5$. Since $(p-1)/2 = 6$, it is necessary to calculate $[ka/p]$ for $k = 1, \ldots, 6$:

$$[5/13] = [10/13] = 0;$$
$$[15/13] = [20/13] = [25/13] = 1;$$
$$[30/13] = 2.$$

By the lemma, we have

$$(5/13) = (-1)^{1+1+1+2} = (-1)^5 = -1,$$

confirming what was earlier seen.

PROBLEMS

1. Use Gauss' Lemma to evaluate each of the Legendre symbols below (that is, in each case find the integer n for which $(a/p) = (-1)^n$):
   (a) (8/11), (b) (7/13), (c) (5/19), (d) (11/23), (e) (6/31).

2. If p is an odd prime, show that

$$\sum_{a=1}^{p-2} (a(a+1)/p) = -1$$

   [*Hint:* If a' is defined by $aa' \equiv 1 \pmod{p}$, then $(a(a+1)/p) = ((1+a')/p)$. Note that $1 + a'$ runs through a complete set of residues modulo p, except for the integer 1.]

3. Prove the statements below:
   (a) If p and $q = 2p + 1$ are both odd primes, then -4 is a primitive root of q.
   (b) If $p \equiv 1 \pmod 4$ is a prime, then -4 and $(p-1)/4$ are both quadratic residues of p.

4. If $p \equiv 7 \pmod 8$, show that $p \mid 2^{(p-1)/2} - 1$. [*Hint:* By Theorem 9-6, $1 = (2/p) \equiv 2^{(p-1)/2} \pmod p$.]

5. Use Problem 4 to confirm that the numbers $2^n - 1$ are composite for $n = 11, 23, 83, 131, 179, 183, 239, 251$.

POSSIBLE QUESTIONS

2 Mark Questions:

1. Define order of an integer modulo n.
2. If a has order k modulo n, then prove the integer $a, a^2, ..., a^k$ are in-congruent modulo n.
3. What is Primitive root with example.
4. If n has a primitive root, then prove it has exactly $\phi(\phi(n))$ of them.
5. Suppose p is an odd prime, then prove there exists a primitive root r of p such that $r^{p-1} \not\equiv 1 (\text{mod } p^2)$.
6. Prove that there are primitive roots for $2p^k$, where p is an odd prime and $k \geq 1$.
7. Define quadratic residue and non residue for prime p.
8. Define Legendre symbol.

8 Mark Questions:

1. Let the integer a have order k modulo n. then prove $a^h \equiv 1 (\text{mod } n)$ if and only if $k | h$; in particular, $k | \phi(n)$.
2. If a has order k modulo n, then prove that $a^i \equiv a^j (\text{mod } n)$ if and only if $i \equiv j (\text{mod } k)$.
3. If the integer a has order k modulo n and $h > 0$, then a^k has order $k / \gcd(h,k)$ modulo n.
4. Let $\gcd(a,n) = 1$ and let $a_1, a_2, ..., a_{\phi(n)}$ be the positive integers less than n and relatively prime to n. If a is a primitive root of n, then prove
$$a, a^2, ..., a^{\phi(n)}$$
are congruent modulo n to $a_1, a_2, ..., a_{\phi(n)}$, in some order.
5. State and prove Lagrange theorem.
6. If p is a prime number and $d | (p-1)$, then prove there are exactly $\phi(d)$ in-congruent integer having order d modulo p.
7. Prove that for $k \geq 3$, the integer 2^k has no primitive roots.
8. Suppose $\gcd(m,n) = 1$, where $m > 2$ and $n > 2$, then the integer mn has no primitive roots.
9. Let p be an odd prime and r be a primitive root of p such that $r^{p-1} \not\equiv 1 (\text{mod } p^2)$. then for each positive integer $k \geq 2$,

$$r^{p^{k-2}(p-1)} \not\equiv 1 (\mathrm{mod}\, p^k).$$

10. If p is an odd prime number and $k \geq 1,$ then prove there exists a primitive root for p^k.
11. State and prove Euler criterion.
12. State and Prove the properties of Legendre symbol.
13. If p is an odd prime, then prove

$$\sum_{a=1}^{p-1} (a/p) = 0.$$

Hence, there are precisely $(p-1)/2$ quadratic residues and $(p-1)/2$ quadratic non residues of p.

14. State and prove Gauss lemma.
15. If p is an odd prime, then prove $(2/p) = \begin{cases} 1 & if \quad p \equiv 1(\mathrm{mod}\, 8) \quad or \quad p \equiv 7(\mathrm{mod}\, 8); \\ -1 & if \quad p \equiv 3(\mathrm{mod}\, 8) \quad or \quad p \equiv 5(\mathrm{mod}\, 8). \end{cases}$
16. If p and $2p+1$ are both odd primes, then prove that the integer $(-1)^{(p-1)/2} 2$ is a primitive root of $2p+1$.
17. If p is an odd prime and a an odd integer, with $\gcd(a, p) = 1,$ then prove $(a/p) = (-1)^{\sum_{k=1}^{(p-1)/2} [ka/p]}$.

UNIT-V

SYLLABUS

Quadratic reciprocity-quadratic congruences with composite moduli. Public key encryption, RSA encryption and decryption, the equation $x^2 + y^2 = z^2$, Fermat's Last theorem.

QUADRATIC RECIPROCITY

Let p and q be distinct odd primes, so that both of the Legendre symbols (p/q) and (q/p) are defined. It is natural to inquire whether the value of (p/q) can be determined if that of (q/p) is known. To put the question more generally, is there any connection at all between the values of these two symbols? The basic relationship was conjectured experimentally by Euler in 1783 and imperfectly proved by Legendre two years thereafter. Using his symbol, Legendre stated this relationship in the elegant form that has since become known as the Quadratic Reciprocity Law:

$$(p/q)(q/p) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Legendre went amiss in assuming a result which is as difficult to prove as the law itself, namely, that for any prime $p \equiv 1 \pmod 8$, there exists another prime $q \equiv 3 \pmod 4$ for which p is a quadratic residue. Undaunted, he attempted another proof in his *Essai sur la Théorie des Nombres* (1798); this one too contained a gap, since Legendre took for granted that there are an infinite number of primes in certain arithmetical progressions (a fact eventually proved by Dirichlet in 1837, using in the process very subtle arguments from complex variable theory).

At the age of eighteen, Gauss (in 1795), apparently unaware of the work of either Euler or Legendre, rediscovered this reciprocity law and, after a year's unremitting labor, obtained the first complete proof. "It tortured me," says Gauss, "for the whole year and eluded my most strenuous efforts before, finally, I got the proof explained in the fourth section of the *Disquisitiones Arithmeticae*." In the *Disquisitiones Arithmeticae*—which was published in 1801, although finished in 1798—Gauss attributed the Quadratic Reciprocity Law to himself, taking the view that a theorem belongs to the one who gives the first rigorous demonstration. The indignant Legendre was led to complain: "This excessive impudence is unbelievable in a man who has sufficient personal merit not to have the need of appropriating the discoveries of others." All

discussion of priority between the two was futile; since each clung to the correctness of his position, neither took heed of the other. Gauss went on to publish five different demonstrations of what he called "the gem of higher arithmetic," while another was found among his papers. The version presented below, a variant of one of Gauss' own arguments, is due to his student, Ferdinand Eisenstein (1823–1852). The proof is complicated (and it would perhaps be unreasonable to expect an easy proof), but the underlying idea is simple enough.

THEOREM 9-9 (Gauss' Quadratic Reciprocity Law). *If p and q are distinct odd primes, then*

$$(p/q)(q/p) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

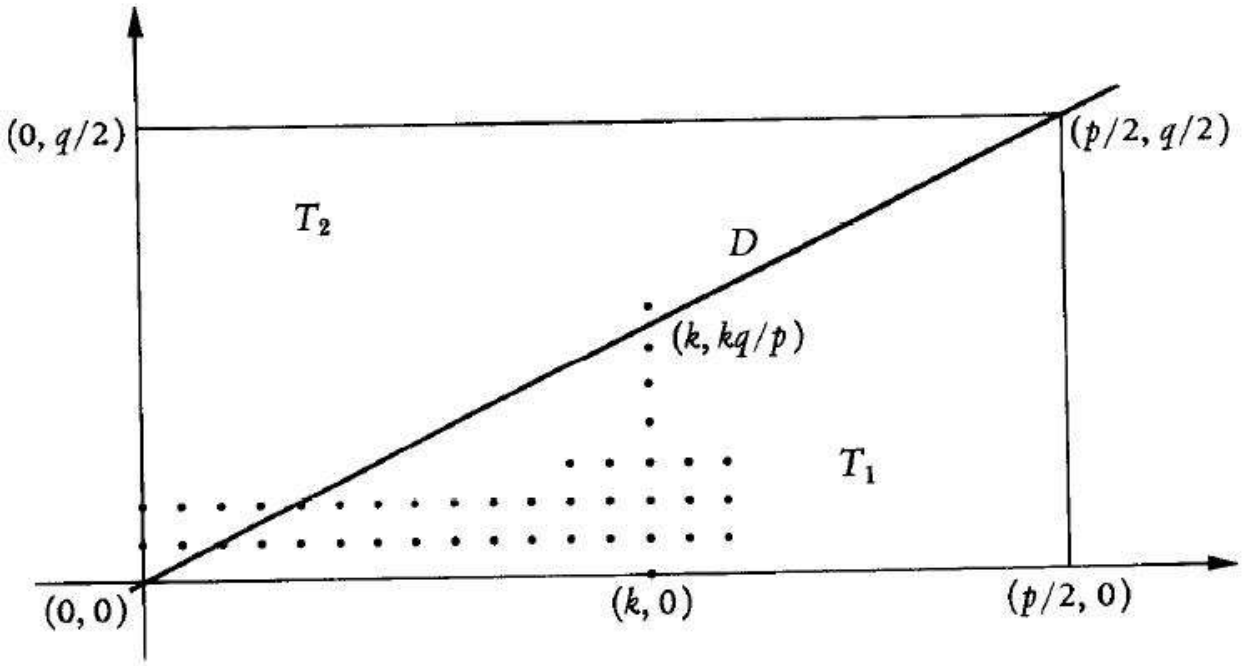
Proof: Consider the rectangle in the xy coordinate plane whose vertices are $(0, 0)$, $(p/2, 0)$, $(0, q/2)$, and $(p/2, q/2)$. Let R denote the region within this rectangle, not including any of the bounding lines. The general plan of attack is to count the number of lattice points (that is, the points whose coordinates are integers) inside R in two different ways. Since p and q are both odd, the lattice points in R consist of all points (n, m), where $1 \leq n \leq (p-1)/2$ and $1 \leq m \leq (q-1)/2$; the number of such points is clearly

$$\frac{p-1}{2} \cdot \frac{q-1}{2}.$$

Now the diagonal D from $(0, 0)$ to $(p/2, q/2)$ has the equation $y = (q/p)x$, or equivalently, $py = qx$. Since $\gcd(p, q) = 1$, none of the lattice points inside R will lie on D. For p must divide the x coordinate of any lattice point on the line $py = qx$, and q must divide its y coordinate; there are are no such points in R. Suppose that T_1 denotes the portion of R which is below the diagonal D, and T_2 the portion above. By what we have just seen, it suffices to count the lattice points inside each of these triangles.

The number of integers in the interval $0 < y < kq/p$ is $[kq/p]$. Thus, for $1 \leq k \leq (p-1)/2$, there are precisely $[kq/p]$ lattice points in T_1 directly above the point $(k, 0)$ and below D; in other words, lying on the vertical line segment from $(k, 0)$ to $(k, kq/p)$. It follows that the total number of lattice points contained in T_1 is

$$\sum_{k=1}^{(p-1)/2} [kq/p].$$



A similar calculation, with the roles of p and q interchanged, shows that the number of lattice points within T_2 is

$$\sum_{j=1}^{(q-1)/2} [jp/q].$$

This accounts for all of the lattice points inside R, so that

$$\frac{p-1}{2} \cdot \frac{q-1}{2} = \sum_{k=1}^{(p-1)/2} [kq/p] + \sum_{j=1}^{(q-1)/2} [jp/q].$$

The time has come for Gauss' Lemma to do its duty:

$$(p/q)(q/p) = (-1)^{\sum_{j=1}^{(q-1)/2} [jp/q]} \cdot (-1)^{\sum_{k=1}^{(p-1)/2} [kq/p]}$$
$$= (-1)^{\sum_{j=1}^{(q-1)/2} [jp/q] + \sum_{k=1}^{(p-1)/2} [kq/p]}$$
$$= (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

The proof of the Quadratic Reciprocity Law is now complete.

COROLLARY 1. *If p and q are distinct odd primes, then*

$$(p/q)(q/p) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \text{ or } q \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv q \equiv 3 \pmod 4 \end{cases}$$

Proof: The number $(p-1)/2 \cdot (q-1)/2$ is even if and only if at least one of the integers p and q is of the form $4k+1$; if both are of the form $4k+3$, then $(p-1)/2 \cdot (q-1)/2$ is odd.

Multiplying each side of the Quadratic Reciprocity equation by (q/p) and using the fact that $(q/p)^2 = 1$, we could also formulate this as

COROLLARY 2. *If p and q are distinct odd primes, then*

$$(p/q) = \begin{cases} (q/p) & \text{if } p \equiv 1 \pmod 4 \text{ or } q \equiv 1 \pmod 4 \\ -(q/p) & \text{if } p \equiv q \equiv 3 \pmod 4 \end{cases}$$

Let us see what this last series of results accomplishes. Take p to be an odd prime and $a \neq \pm 1$ to be an integer not divisible by p. Suppose further that a has the factorization

$$a = \pm 2^{k_0} p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r},$$

where the p_i are odd primes. Since the Legendre symbol is multiplicative,

$$(a/p) = (\pm 1/p)(2/p)^{k_0}(p_1/p)^{k_1} \cdots (p_r/p)^{k_r}.$$

In order to evaluate (a/p), we have only to calculate the symbols $(-1/p)$, $(2/p)$, and (p_i/p). The values of $(-1/p)$ and $(2/p)$ were discussed earlier, so that the one stumbling block is (p_i/p), where p_i and p are distinct odd primes; this is where the Quadratic Reciprocity Law enters. For Corollary 2 allows us to replace (p_i/p) by a new Legendre symbol having a smaller denominator. Through continued inversion and division, the computation can be reduced to that of the known quantities

$$(-1/q),\ (1/q),\ \text{and}\ (2/q).$$

Example 9-5

Consider the Legendre symbol (29/53), for instance. Since both $29 \equiv 1 \pmod 4$ and $53 \equiv 1 \pmod 4$, we see that

$$\begin{aligned}(29/53) &= (53/29) = (24/29) = (2/29)(3/29)(4/29)\\ &= (2/29)(3/29).\end{aligned}$$

With reference to Theorem 9-6, $(2/29) = -1$, while inverting again,

$$(3/29) = (29/3) = (2/3) = -1,$$

where we used the congruence $29 \equiv 2 \pmod 3$. The net effect is that

$$(29/53) = (2/29)(3/29) = (-1)(-1) = 1.$$

The Quadratic Reciprocity Law provides a very satisfactory answer to the problem of finding all odd primes $p \neq 3$ for which 3 is a quadratic residue. Since $3 \equiv 3 \pmod 4$, Corollary 2 above implies that

$$(3/p) = \begin{cases} (p/3) & \text{if } p \equiv 1 \pmod 4 \\ -(p/3) & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Now $p \equiv 1 \pmod 3$ or $p \equiv 2 \pmod 3$. By Theorems 9-2 and 9-6,

$$(p/3) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 3 \\ -1 & \text{if } p \equiv 2 \pmod 3 \end{cases}$$

the implication of which is that $(3/p) = 1$ if and only if

(1) $$p \equiv 1 \pmod 4 \quad \text{and} \quad p \equiv 1 \pmod 3,$$

or

(2) $$p \equiv 3 \pmod 4 \quad \text{and} \quad p \equiv 2 \pmod 3.$$

The restrictions in (1) are equivalent to requiring that $p \equiv 1 \pmod{12}$ while those in (2) are equivalent to $p \equiv 11 \equiv -1 \pmod{12}$.

THEOREM 9-10. *If $p \neq 3$ is an odd prime, then*

$$(3/p) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{12} \\ -1 & \text{if } p \equiv \pm 5 \pmod{12} \end{cases}$$

Example 9-6

The purpose of this example is to investigate the existence of solutions of the congruence

$$x^2 \equiv 196 \pmod{1357}.$$

Since $1357 = 23 \cdot 59$, the given congruence is solvable if and only if both

$$x^2 \equiv 196 \pmod{23} \quad \text{and} \quad x^2 \equiv 196 \pmod{59}$$

are solvable. Our procedure is to find the values of the Legendre symbols (196/23) and (196/59).

The evaluation of (196/23) requires the use of Theorem 9-10:

$$(196/23) = (12/23) = (3/23) = 1.$$

Thus, the congruence $x^2 \equiv 196 \pmod{23}$ admits a solution. As regards the symbol (196/59), the Quadratic Reciprocity Law enables us to write

$$(196/59) = (19/59) = -(59/19) = -(2/19) = -(-1) = 1.$$

It is therefore possible to solve $x^2 \equiv 196 \pmod{59}$ and, in consequence, the congruence $x^2 \equiv 196 \pmod{1357}$ as well.

Let us turn to a quite different application of these ideas. At an earlier stage, it was observed that if $F_n = 2^{2^n} + 1$, $n > 1$, is a prime, then 2 is not a primitive root of F_n. We now possess the means to show that the integer 3 serves as a primitive root of any prime of this type.

As a step in this direction, note that any F_n is of the form $12k + 5$. A simple induction argument confirms that $4^m \equiv 4 \pmod{12}$ for $m = 1, 2, \ldots$; hence, we must have

$$F_n = 2^{2^n} + 1 = 2^{2m} + 1 = 4^m + 1 \equiv 5 \pmod{12}.$$

If F_n happens to be prime, then Theorem 9-10 permits the conclusion

$$(3/F_n) = -1,$$

or, using Euler's Criterion,

$$3^{\frac{F_n - 1}{2}} \equiv -1 \pmod{F_n}.$$

Switching to the phi-function, the last congruence says that

$$3^{\phi(F_n)/2} \equiv -1 \pmod{F_n}.$$

From this, it may be inferred that 3 has order $\phi(F_n)$ modulo F_n, and so 3 is a primitive root of F_n.

PROBLEMS

1. Evaluate the following Legendre symbols:
   (a) (71/73), (b) (−219/383), (c) (461/773), (d) (1234/4567), (e) (3658/12703). [*Hint:* $3658 = 2 \cdot 31 \cdot 59$.]
2. Prove that 3 is a quadratic nonresidue of all primes of the form $2^{2n} + 1$, as well as all primes of the form $2^p - 1$, where p is an odd prime. [*Hint:* For all n, $4^n \equiv 4 \pmod{12}$.]
3. Determine whether the following quadratic congruences are solvable:
   (a) $x^2 \equiv 219 \pmod{419}$.
   (b) $3x^2 + 6x + 5 \equiv 0 \pmod{89}$.

(c) $2x^2 + 5x - 9 \equiv 0 \pmod{101}$.

4. Verify that if p is an odd prime, then

$$(-2/p) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 8 \text{ or } p \equiv 3 \pmod 8 \\ -1 & \text{if } p \equiv 5 \pmod 8 \text{ or } p \equiv 7 \pmod 8 \end{cases}$$

5. (a) Prove that if $p > 3$ is an odd prime, then

$$(-3/p) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 6 \\ -1 & \text{if } p \equiv 5 \pmod 6 \end{cases}$$

(b) Using part (a), show that there are infinitely many primes of the form $6k + 1$. [*Hint:* Assume that $p_1, p_2, \ldots, p_r$ are all the primes of the form $6k + 1$ and consider the integer $(2p_1p_2 \cdots p_r)^2 + 3$.]

6. Use Theorem 9-2 and Problems 4 and 5 to determine which primes can divide each of $n^2 + 1$, $n^2 + 2$, $n^2 + 3$ for some value of n.

QUADRATIC CONGRUENCES WITH COMPOSITE MODULI

So far in the proceedings, quadratic congruences with (odd) prime moduli have been of paramount importance. The remaining theorems broaden the horizon by allowing a composite modulus. To start, let us consider the situation where the modulus is a power of a prime.

THEOREM 9-11. *If p is an odd prime and $\gcd(a, p) = 1$, then the congruence*

$$x^2 \equiv a \pmod{p^n}, \qquad n \geq 1$$

has a solution if and only if $(a/p) = 1$.

Proof: As is common with many "if and only if" theorems, one half of the proof is trivial while the other half requires considerable effort: If $x^2 \equiv a \pmod{p^n}$ has a solution, then so does $x^2 \equiv a \pmod p$ —in fact, the same solution—whence $(a/p) = 1$.

For the converse, suppose that $(a/p) = 1$. We argue that $x^2 \equiv a \pmod{p^n}$ is solvable by inducting on n. If $n = 1$ there is really nothing to prove; indeed, $(a/p) = 1$ is just another way of say-

ing that $x^2 \equiv a \pmod{p}$ can be solved. Assume that the result holds for $n = k \geq 1$, so that $x^2 \equiv a \pmod{p^k}$ admits a solution x_0. Then

$$x_0^2 = a + bp^k$$

for an appropriate choice of b. In passing from k to $k+1$, we shall use x_0 and b to write down explicitly a solution to the congruence $x^2 \equiv a \pmod{p^{k+1}}$.

Towards this end, we first solve the linear congruence

$$2x_0 y \equiv -b \pmod{p},$$

obtaining a unique solution y_0 modulo p (this is certainly possible, since $\gcd(2x_0, p) = 1$). Next, consider the integer

$$x_1 = x_0 + y_0 p^k.$$

Upon squaring this integer, we get

$$\begin{aligned}(x_0 + y_0 p^k)^2 &= x_0^2 + 2x_0 y_0 p^k + y_0^2 p^{2k} \\ &= a + (b + 2x_0 y_0)p^k + y_0^2 p^{2k}.\end{aligned}$$

But $p \mid (b + 2x_0 y_0)$, from which it follows that

$$x_1^2 = (x_0 + y_0 p^k)^2 \equiv a \pmod{p^{k+1}}.$$

Thus, the congruence $x^2 \equiv a \pmod{p^n}$ has a solution for $n = k + 1$ and, by induction, for all positive integers n.

Let us run through a specific example in detail. The first step in obtaining a solution of, say, the quadratic congruence

$$x^2 \equiv 23 \pmod{7^2}$$

is to solve $x^2 \equiv 23 \pmod{7}$, or what amounts to the same thing, the congruence

$$x^2 \equiv 2 \pmod{7}.$$

Since $(2/7) = 1$, a solution surely exists; in fact $x_0 = 3$ is an obvious choice. Now x_0^2 can be represented as

$$3^2 = 9 = 23 + (-2)7,$$

so that $b = -2$ (in our special case, the integer 23 plays the role of a). Following the proof of Theorem 9-11, we next determine y so that

$$6y \equiv 2 \pmod 7;$$

that is, $3y \equiv 1 \pmod 7$. This linear congruence is satisfied by $y_0 = 5$. Hence,

$$x_0 + 7y_0 = 3 + 7 \cdot 5 = 38$$

serves as a solution to the original congruence $x^2 \equiv 23 \pmod{49}$. It should be noted that $-38 \equiv 11 \bmod (49)$ is the only other solution.

If, instead, the congruence

$$x^2 \equiv 23 \pmod{7^3}$$

were proposed for solution, we would start with

$$x^2 \equiv 23 \pmod{7^2},$$

obtaining a solution $x_0 = 38$. Since

$$38^2 = 23 + 29 \cdot 7^2,$$

the integer $b = 29$. We would then find the unique solution $y_0 = 1$ of the linear congruence

$$76y \equiv -29 \pmod 7.$$

Then $x^2 \equiv 23 \pmod{7^3}$ is satisfied by

$$x_0 + y_0 7^2 = 38 + 1 \cdot 49 = 87,$$

as well as $-87 \equiv 256 \pmod{7^3}$.

Having dwelt at length on odd primes, let us now take up the case $p = 2$. The next theorem supplies the pertinent information.

THEOREM 9-12. *Let a be an odd integer. Then*

(1) $x^2 \equiv a \pmod 2$ *always has a solution*;
(2) $x^2 \equiv a \pmod 4$ *has a solution if and only if* $a \equiv 1 \pmod 4$;
(3) $x^2 \equiv a \pmod{2^n}$, *for* $n \geq 3$, *has a solution if and only if* $a \equiv 1 \pmod 8$.

Proof: The first assertion is obvious. The second depends on the observation that the square of any odd integer is congruent to 1 modulo 4. Thus, $x^2 \equiv a \pmod 4$ can be solved only when a is of the form $4k + 1$; in this event, there are two solutions modulo 4, namely $x = 1$ and $x = 3$.

Now consider the case in which $n \geq 3$. Since the square of any odd integer is congruent to 1 modulo 8, we see that for the congruence $x^2 \equiv a \pmod{2^n}$ to be solvable it is necessary that a should be of the form $8k + 1$. To go the other way, let us suppose that $a \equiv 1 \pmod 8$ and proceed by induction on n. When $n = 3$, the congruence $x^2 \equiv a \pmod{2^n}$ is certainly solvable; indeed, each of the integers 1, 3, 5, 7 satisfies $x^2 \equiv 1 \pmod 8$. Fix a value of $n > 3$ and assume, for the induction hypothesis, that the congruence $x^2 \equiv a \pmod{2^n}$ admits a solution x_0. Then there exists an integer b for which

$$x_0^2 = a + b2^n.$$

Since a is odd, so is the integer x_0. It is therefore possible to find a unique solution y_0 of the linear congruence

$$x_0 y \equiv -b \pmod 2.$$

We argue that the integer

$$x_1 = x_0 + y_0 2^{n-1}$$

satisfies the congruence $x^2 \equiv a \pmod{2^{n+1}}$. Squaring yields

$$(x_0 + y_0 2^{n-1})^2 = x_0^2 + x_0 y_0 2^n + y_0^2 2^{2n-2}$$
$$= a + (b + x_0 y_0)2^n + y_0^2 2^{2n-2}.$$

By the way y_0 was chosen, $2 \mid (b + x_0 y_0)$, hence

$$x_1^2 = (x_0 + y_0 2^{n-1})^2 \equiv a \pmod{2^{n+1}}$$

(one also uses the fact that $2n - 2 = n + 1 + (n - 3) > n + 1$). Thus $x^2 \equiv a \pmod{2^{n+1}}$ is solvable, completing the induction step and the proof.

To illustrate: the congruence $x^2 \equiv 5 \pmod 4$ has a solution, but $x^2 \equiv 5 \pmod 8$ does not; on the other hand, $x^2 \equiv 17 \pmod{16}$ and $x^2 \equiv 17 \pmod{32}$ are both solvable.

In theory, we can now completely settle the question of when there exists an integer x such that

$$x^2 \equiv a \pmod n, \quad \gcd(a, n) = 1, \qquad n > 1.$$

For suppose that n has the prime-power decomposition

$$n = 2^{k_0} p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}, \qquad k_0 \geq 0,\ k_i > 0$$

where the p_i are distinct odd primes. Since the problem of solving the quadratic congruence $x^2 \equiv a \pmod n$ is equivalent to that of solving the system of congruences

$$\begin{aligned} x^2 &\equiv a \pmod{2^{k_0}}, \\ x^2 &\equiv a \pmod{p_1^{k_1}}, \\ &\vdots \\ x^2 &\equiv a \pmod{p_r^{k_r}}, \end{aligned}$$

our last two results may be combined to give the following general conclusion.

THEOREM 9-13. *Let* $n = 2^{k_0} p_1^{k_1} \cdots p_r^{k_r}$ *be the prime factorization of* $n > 1$ *and let* $\gcd(a, n) = 1$. *Then* $x^2 \equiv a \pmod n$ *is solvable if and only if*

(1) $(a/p_i) = 1$ *for* $i = 1, 2, \ldots, r$;
(2) $a \equiv 1 \pmod 4$ *if* $4 \mid n$, *but* $8 \nmid n$; $a \equiv 1 \pmod 8$ *if* $8 \mid n$.

PROBLEMS

1. (a) Show that 7 and 18 are the only incongruent solutions of $x \equiv -1 \pmod{5^2}$.
   (b) Use part (a) to find the solutions of $x^2 \equiv -1 \pmod{5^3}$.
2. Solve each of the following quadratic congruences:
   (a) $x^2 \equiv 7 \pmod{3^3}$;
   (b) $x^2 \equiv 14 \pmod{5^3}$;
   (c) $x^2 \equiv 2 \pmod{7^3}$.
3. Solve the congruence $x^2 \equiv 31 \pmod{11^4}$.
4. Find the solutions of $x^2 + 5x + 6 \equiv 0 \pmod{5^3}$ and $x^2 + x + 3 \equiv 0 \pmod{3^3}$.
5. Prove that if the congruence $x^2 \equiv a \pmod{2^n}$, where $n \geq 3$, has a solution, then it has exactly four incongruent solutions. [*Hint:* If x_0 is any solution, then the four integers x_0, $-x_0$, $x_0 + 2^{n-1}$, $-x_0 + 2^{n-1}$ are incongruent modulo 2^n and comprise all the solutions.]
6. From $23^2 \equiv 17 \pmod{2^7}$, find three other solutions of the congruence $x^2 \equiv 17 \pmod{2^7}$.

Public Key

1 The idea of public key cryptography

Recall that a cryptosystem consists of a 1-to-1 enciphering transformation f from a set $\mathcal{P}$ of all possible plaintext message units to a set $\mathcal{C}$ of all possible ciphertext message units. Actually, the term "cryptosystem" is more often used to refer to a whole family of such transformations, each corresponding to a choice of *parameters* (the sets $\mathcal{P}$ and $\mathcal{C}$, as well as the map f, may depend upon the values of the parameters). For example, for a fixed N-letter alphabet (with numerical equivalents also fixed once and for all), we might consider the affine cryptosystem (or "family of cryptosystems") which for each $a \in (\mathbf{Z}/N\mathbf{Z})^*$ and $b \in \mathbf{Z}/N\mathbf{Z}$ is the map from $\mathcal{P} = \mathbf{Z}/N\mathbf{Z}$ to $\mathcal{C} = \mathbf{Z}/N\mathbf{Z}$ defined by $C \equiv aP + b \ mod \ N$. In this example, the sets $\mathcal{P}$ and $\mathcal{C}$ are fixed (because N is fixed), but the enciphering transformation f depends upon the choice of parameters a, b. The enciphering transformation can then be described by (i) an algorithm, which is the same for the whole family, and (ii) the values of the parameters. The values of the parameters are called the *enciphering key* K_E. In our example, K_E is the pair (a, b). In practice, we shall suppose that the algorithm is publicly known, i.e., the general procedure used to encipher cannot be kept secret. However, the keys can easily be changed periodically and, if one wants, kept secret.

One also needs an algorithm and a key in order to decipher, i.e., compute f^{-1}! The key is called the *deciphering key* K_D. In our example of the affine cryptosystem family, deciphering is also accomplished by an affine map, namely $P \equiv a^{-1}C - a^{-1}b \ mod \ N$, and so the deciphering transformation uses the same algorithm as the enciphering transformation, except with a different key, namely, the pair $(a^{-1}, -a^{-1}b)$. (In some cryptosystems, the deciphering algorithm, as well as the key, is different from the enciphering algorithm.) We shall always suppose that the deciphering and enciphering algorithms are publicly known, and that it is the keys K_E and K_D which can be concealed.

Let us suppose that someone wishes to communicate secretly using the above affine cryptosystem $C \equiv aP + b$. We saw in §III.1 that it is not hard to break the system if one uses single-letter message units in an N-letter alphabet. It is a little more difficult to break the system if one uses

digraphs, which can be regarded as symbols in an N^2-letter alphabet. It would be safer to use blocks of k letters, which have numerical equivalents in $\mathbf{Z}/N^k\mathbf{Z}$. At least for $k > 3$ it is not easy to use frequency analysis, since the number of possible k-letter blocks is very large, and one will find many that are close contenders for the title of most frequently occurring k-graph. If we want to increase k, we must be concerned about the length of time it takes to do various arithmetic tasks (the most important one being finding a^{-1} by the Euclidean algorithm) involved in setting up our keys and carrying out the necessary transformations every time we send a message or our friend at the other end deciphers a message from us. That is, it is useful to have big-O estimates for the order of magnitude of time (as the parameters increase, i.e., as the cryptosystem becomes "larger") that it takes to: encipher (knowing K_E), decipher (knowing K_D), or break the code by enciphering without knowledge of K_E or deciphering without knowledge of K_D.

In all of the examples in Chapter III — and in all of the cryptosystems used historically until about fifteen years ago — it is not really necessary to specify the deciphering key once the enciphering key (and the general algorithms) are known. Even if we are working with large numbers — such as N^k with k fairly large — it is possible to determine the deciphering key from the enciphering key using an order of magnitude of time which is roughly the same as that needed to implement the various algorithms. For example, in the case of an affine enciphering transformation of $\mathbf{Z}/N^k\mathbf{Z}$, once we know the enciphering key $K_E = (a, b)$ we can compute the deciphering key $K_D = (a^{-1} \ mod \ N^k, \ -a^{-1}b \ mod \ N^k)$ by the Euclidean algorithm in $O(log^3(N^k))$ bit operations.

Thus, with a traditional cryptosystem anyone who knew enough to decipher messages could, with little or no extra effort, determine the enciphering key. Indeed, it was considered naive or foolish to think that someone who had broken a cipher might nevertheless not know the enciphering key. We see this in the following passage from the autobiography of a well-known historical personality:

Thus, with a traditional cryptosystem anyone who knew enough to decipher messages could, with little or no extra effort, determine the enciphering key. Indeed, it was considered naive or foolish to think that someone who had broken a cipher might nevertheless not know the enciphering key.

We see this in the following passage from the autobiography of a well-known historical personality:

Thus, with a traditional cryptosystem anyone who knew enough to decipher messages could, with little or no extra effort, determine the enciphering key. Indeed, it was considered naive or foolish to think that someone who had broken a cipher might nevertheless not know the enciphering key.

> Five or six weeks later, she [Madame d'Urfé] asked me if I had deciphered the manuscript which had the transmutation procedure. I told her that I had.
>
> "Without the key, sir, excuse me if I believe the thing impossible."
>
> "Do you wish me to name your key, madame?"
>
> "If you please."
>
> I then told her the key-word, which belonged to no language, and I saw her surprise. She told me that it was impossible, for she believed herself the only possessor of that word which she kept in her memory and which she had never written down.
>
> I could have told her the truth — that the same calculation which had served me for deciphering the manuscript had enabled me to learn the word — but on a caprice it struck me to tell her that a genie had revealed it to me. This false disclosure fettered Madame d'Urfé to me. That day I became the master of her soul, and I abused my power. Every time I think of it, I am distressed and ashamed, and I do penance now in the obligation under which I place myself of telling the truth in writing my memoirs.
>
> — Casanova, 1757, quoted in D. Kahn's *The Codebreakers*

The situation persisted for another 220 years after this encounter between Casanova and Madame d'Urfé: knowledge of how to encipher and knowledge of how to decipher were regarded as essentially equivalent in any cryptosystem. However, in 1976 W. Diffie and M. Hellman discovered an entirely different type of cryptosystem and invented "public key cryptography."

By definition, a public key cryptosystem has the property that someone who knows only how to encipher cannot use the enciphering key to find

the deciphering key without a prohibitively lengthy computation. In other words the enciphering function $f: \mathcal{P} \longrightarrow \mathcal{C}$ is easy to compute once the enciphering key K_E is known, but it is very hard in practice to compute the inverse function $f^{-1}: \mathcal{C} \longrightarrow \mathcal{P}$. That is, from the standpoint of realistic computability, the function f is not invertible (without some additional information — the deciphering key K_D). Such a function f is called a *trapdoor function*. That is, a trapdoor function f is a function which is easy to compute but whose inverse f^{-1} is hard to compute without having some additional auxiliary information beyond what is necessary to compute f. The inverse f^{-1} is easy to compute, however, for someone who has this information K_D (the "deciphering key").

There is a closely related concept of a *one-way* function. This is a function f which is easy to compute but for which f^{-1} is hard to compute and cannot be made easy to compute even by acquiring some additional information. While the notion of a trapdoor function apparently appeared for the first time in 1978 along with the invention of the RSA public-key cryptosystem, the notion of a one-way function is somewhat older. What seems to have been the first use of one-way functions for cryptography was described in Wilkes' book about time-sharing systems that was published in 1968. The author describes a new *one-way cipher* used by R. M. Needham in order to make it possible for a computer to verify passwords without storing information that could be used by an intruder to impersonate a legitimate user.

> In Needham's system, when the user first sets his password, or whenever he changes it, it is immediately subjected to the enciphering process, and it is the enciphered form that is stored in the computer. Whenever the password is typed in response to a demand from the supervisor for the user's identity to be established, it is again enciphered and the result compared with the stored version. It would be of no immediate use to a would-be malefactor to obtain a copy of the list of enciphered passwords, since he would have to decipher them before he could use them. For this purpose, he would need access to a computer and even if full details of the enciphering algorithm were available, the deciphering process would take a long time.

In 1974, G. Purdy published the first detailed description of such a one-way function. The original passwords and their enciphered forms are regarded as integers modulo a large prime p, and the "one-way" map $\mathbf{F}_p \longrightarrow \mathbf{F}_p$ is given by a polynomial $f(x)$ which is not hard to evaluate by computer but which takes an unreasonably long time to invert. Purdy used $p = 2^{64} - 59$, $f(x) = x^{2^{24}+17} + a_1x^{2^{24}+3} + a_2x^3 + a_3x^2 + a_4x + a_5$, where the coefficients a_i were arbitrary 19-digit integers.

The above definitions of a public key cryptosystem and a one-way or trapdoor function are not precise from a rigorous mathematical standpoint. The notion of "realistic computability" plays a basic role. But that is an empirical concept that is affected by advances in computer technology (e.g., parallel processor techniques) and the discovery of new algorithms which speed up the performance of arithmetic tasks (sometimes by a large factor). Thus, it is possible that an enciphering transformation that can safely be regarded as a one-way or trapdoor function in 1994 might lose its one-way or trapdoor status in 2004 or in the year 2994.

It is conceivable that some transformation could be *proved* to be trapdoor. That is, there could be a theorem that provides a nontrivial lower bound for the number of bit operations that would be required ("on the average," i.e., for random values of the key parameters) in order to figure out and implement a deciphering algorithm without the deciphering key. Here one would have to allow the possibility of examining a large number of corresponding plaintext–ciphertext message units (as in our frequency analysis of the simple systems in Chapter III), because, by the definition of a public key system, any user can generate an arbitrary number of plaintext–ciphertext pairs. One would also have to allow the use of "probabilistic" methods which, while not guaranteed to break the code at once, would be likely to work if repeated many times. (Examples of probabilistic algorithms will be given in the next chapter.) Unfortunately, no such theorems have been proved for any of the functions that have been used as enciphering maps. Thus, while there are now many cryptosystems which empirically seem to earn the right to be called "public key," there is no cryptosystem in existence which is *provably* public key.

The reason for the name "public key" is that the information needed to send secret messages — the enciphering key K_E — can be made public information without enabling anyone to read the secret messages. That is,

suppose we have some population of users of the cryptosystem, each one of whom wants to be able to receive confidential communications from any of the other users without a third party (either another user or an outsider) being able to decipher the message. Some central office can collect the enciphering key $K_{E,A}$ from each user A and publish all of the keys in a "telephone book" having the form

AAA Banking Company	(9974398087453939, 2975290017591012)
Aardvark, Aaron	(8870004228331, 7234752637937)
⋮	⋮

Someone wanting to send a message merely has to look up the enciphering key in this "telephone book" and then use the general enciphering algorithm with the key parameters corresponding to the intended recipient. Only the intended recipient has the matching deciphering key needed to read the message.

In earlier ages this type of system would not have seemed to have any particularly striking advantages. Traditionally, cryptography was used mainly for military and diplomatic purposes. Usually there was a small, well-defined group of users who could all share a system of keys, and new keys could be distributed periodically (using couriers) so as to keep the enemy guessing.

However, in recent years the actual and potential applications of cryptography have expanded to include many other areas where communication systems play a vital role — collecting and keeping records of confidential data, electronic financial transactions, and so on. Often one has a large network of users, any two of whom should be able to keep their communications secret from all other users as well as intruders from outside the network. Two parties may share a secret communication on one occasion, and then a little later one of them may want to send a confidential message to a third party. That is, the "alliances" — who is sharing a secret with whom — may be continually shifting. It might be impractical always to be exchanging keys with all possible confidential correspondents.

Notice that with a public key system it is possible for two parties to initiate secret communications without ever having had any prior contact, without having established any prior trust for one another, without ex-

changing any preliminary information. All of the information necessary to send an enciphered message is publicly available.

Classical vesus public key. By a *classical* cryptosystem (also called a *private key* cryptosystem or a *symmetrical* cryptosystem), we mean a cryptosystem in which, once the enciphering information is known, the deciphering transformation can be implemented in approximately the same order of magnitude of time as the enciphering transformation. All of the cryptosystems in Chapter III are classical. Occasionally, it takes a little longer for the deciphering — because one needs to apply the Euclidean algorithm to find an inverse modulo N or one must invert a matrix (and this can take a fairly long time if we work with $k \times k$ -matrices for k larger than 2) — nevertheless, the additional time required is not prohibitive. (Moreover, usually the additional time is required only once — to find K_D — after which it takes no longer to decipher than to encipher.) For example, we might need only $O(log^2 B)$ to encipher a message unit, and $O(log^3 B)$ bit operations to decipher one by finding K_D from K_E, where B is a bound on the size of the key parameters. Notice the role of big-O estimates here.

If, on the other hand, the enciphering time were polynomial in $log\ B$ and the deciphering time (based on knowledge of K_E but not K_D) were, say, polynomial in B but not in $\log B$, then we would have a *public key* rather than a classical cryptosystem.

Authentication. Often, one of the most important parts of a message is the *signature*. A person's signature — hopefully, written with an idiosyncratic flourish of the pen which is hard to duplicate — lets the recipient know that the message really is from the person whose name is typed below. If the message is particularly important, it might be necessary to use additional methods to *authenticate* the communication. And in electronic communication, where one does not have a physical signature, one has to rely entirely on other methods. For example, when an officer of a corporation wants to withdraw money from the corporate account by telephone, he/she is often asked to give some personal information (e.g., mother's maiden name) which the corporate officer knows and the bank knows (from data submitted when the account was opened) but which an imposter would not be likely to know.

In public key cryptography there is an especially easy way to identify oneself in such a way that no one could be simply pretending to be you. Let A (Alice) and B (Bob) be two users of the system. Let f_A be the enciphering transformation with which any user of the system sends a message to Alice, and let f_B be the same for Bob. For simplicity, we shall assume that the set $\mathcal{P}$ of all possible plaintext message units and the set $\mathcal{C}$ of all possible ciphertext message units are equal, and are the same for all users. Let P be Alice's "signature" (perhaps including an identification number, a statement of the time the message was sent, etc.). It would not be enough for Alice to send Bob the encoded message $f_B(P)$, since *everyone* knows how to do that, so there would be no way of knowing that the signature was not forged. Rather, at the beginning (or end) of the message Alice transmits $f_B f_A^{-1}(P)$. Then, when Bob deciphers the whole message, including this part, by applying f_B^{-1}, he finds that everything has become plaintext except for a small section of jibberish, which is $f_A^{-1}(P)$. Since Bob knows that the message is claimed to be from Alice, he applies f_A (which he knows, since Alice's enciphering key is public), and obtains P. Since no one other than Alice could have applied the function f_A^{-1} which is inverted by f_A, he knows that the message was from Alice.

Hash functions. A common way to sign a document is with the help of a *hash function*. Roughly speaking, a hash function is an easily computable map $f : x \mapsto h$ from a very long input x to a much shorter output h (for example, from strings of about 10^6 bits to strings of 150 or 200 bits) that has the following property: *it is not computationally feasible to find two different inputs x and x' such that $f(x') = f(x)$*. If part of Alice's "signature" consists of the hash value $h = f(x)$, where x is the entire text of her message, then Bob can verify not only that the message was really sent by Alice, but also that it wasn't tampered with during transmission. Namely, Bob applies the hash function f to his deciphered plaintext from Alice, and checks that the result agrees with the value h in Alice's signature. By assumption, no tamperer would have been able to change x without changing the value $h = f(x)$.

Key exchange. In practice, the public key cryptosystems for sending messages tend to be slower to implement than the classical systems that are in current use. The number of plaintext message units per second that can be transmitted is less. However, even if a network of users feels attached

to the traditional type of cryptosystem, they may want to use a public key cryptosystem in an auxiliary capacity to send one another their keys $K = (K_E, K_D)$ for the classical system. Thus, the ground rules for the classical cryptosystem can be agreed upon, and keys can be periodically exchanged, using the slower public key cryptography; while the large volume of messages would then be sent by the faster, older methods.

Probabilistic Encryption. Most of the number theory based cryptosystems for message transmission are *deterministic*, in the sense that a given plaintext will always be encrypted into the same ciphertext any time it is sent. However, deterministic encryption has two disadvantages: (1) if an eavesdropper knows that the plaintext message belongs to a small set (for example, the message is either "yes" or "no"), then she can simply encrypt all possibilities in order to determine which is the supposedly secret message; and (2) it seems to be very difficult to *prove* anything about the security of a system if the encryption is deterministic. For these reasons, *probabilistic encryption* was introduced. We will not discuss this further or give examples in this book. For more information, see the fundamental papers on the subject by Goldwasser and Micali (*Proc. 14th ACM Symp. Theory of Computing*, 1982, 365–377, and *J. Comput. System Sci.* **28** (1984), 270–299).

2 RSA

In looking for a trapdoor function f to use for a public key cryptosystem, one wants to use an idea which is fairly simple conceptually and lends itself to easy implementation. On the other hand, one wants to have very strong empirical evidence — based on a long history of attempts to find algorithms for f^{-1} — that decryption cannot feasibly be accomplished without knowledge of the secret deciphering key. For this reason it is natural to look at an ancient problem of number theory: the problem of finding the complete factorization of a large composite integer whose prime factors are not known in advance. The success of the so-called "RSA" cryptosystem (from the last names of the inventors Rivest, Shamir, and Adleman), which is one of the oldest (16 years old) and most popular public key cryptosystems, is based on the tremendous difficulty of factoring.

We now describe how RSA works. Each user first chooses two extremely large prime numbers p and q (say, of about 100 decimal digits each), and sets $n = pq$. Knowing the factorization of n, it is easy to compute $\varphi(n) = (p-1)(q-1) = n+1-p-q$. Next, the user randomly chooses an integer e between 1 and $\varphi(n)$ which is prime to $\varphi(n)$.

Remark. Whenever we say "random" we mean that the number was chosen with the help of a random-number generator (or "pseudo-random" number generator), i.e., a computer program that generates a sequence of digits in a way that no one could duplicate or predict, and which is likely to have all of the statistical properties of a truly random sequence. A lot has been written concerning efficient and secure ways to generate random numbers, but we shall not concern ourselves with this question here. In the RSA cryptosystem we need a random number generator not only to choose e, but also to choose the large primes p and q (so that no one could guess our choices by looking at tables of special types of primes, for example, Mersenne primes or factors of $b^k \pm 1$ for small b and relatively small k). What does a "randomly generated" prime number mean? Well, first generate a large random integer m. If m is even, replace m by $m+1$. Then apply suitable *primality tests* to see if the odd number m is prime (primality tests will be examined systematically in the next chapter). If m is not prime, try $m+2$, then $m+4$, and so on, until you reach the first prime number $\geq m$, which is what you take as your "random" prime. According to the Prime Number Theorem (for the statement see Exercise 13 of § I.1), the frequency of primes among the numbers near m is about $1/log(m)$, so you can expect to test $O(log\, m)$ numbers for primality before reaching the first prime $\geq m$.

Similarly, the "random" number e prime to $\varphi(n)$ can be chosen by first generating a random (odd) integer with an appropriate number of bits, and then successively incrementing it until one finds an e with $g.c.d.(e, \varphi(n)) = 1$. (Alternately, one can perform primality tests until one finds a prime e, say between $max(p,q)$ and $\varphi(n)$; such a prime must necessarily satisfy $g.c.d.(e, \varphi(n)) = 1$.)

Thus, each user A chooses two primes p_A and q_A and a random number e_A which has no common factor with $(p_A - 1)(q_A - 1)$. Next, A computes $n_A = p_A q_A$, $\varphi(n_A) = n_A + 1 - p_A - q_A$, and also the multiplicative inverse of e_A modulo $\varphi(n_A)$: $d_A \underset{\text{def}}{=} e_A^{-1} \bmod \varphi(n_A)$. She makes public the enciphering

key $K_{E,A} = (n_A, e_A)$ and conceals the deciphering key $K_{D,A} = (n_A, d_A)$. The enciphering transformation is the map from $\mathbf{Z}/n_A\mathbf{Z}$ to itself given by $f(P) \equiv P^{e_A} \bmod n_A$. The deciphering transformation is the map from $\mathbf{Z}/n_A\mathbf{Z}$ to itself given by $f^{-1}(C) \equiv C^{d_A} \bmod n_A$. It is not hard to see that these two maps are inverse to one another, because of our choice of d_A. Namely, performing f followed by f^{-1} or f^{-1} followed by f means raising to the $d_A e_A$-th power. But, because $d_A e_A$ leaves a remainder of 1 when divided by $\varphi(n_A)$, this is the same as raising to the 1-st power (see the corollary of Proposition I.3.5, which gives this in the case when P has no common factor with n_A; if $g.c.d.(P, n_A) > 1$, see Exercise 6 below).

From the description in the last paragraph, it seems that we are working with sets $\mathcal{P} = \mathcal{C}$ of plaintext and ciphertext message units that vary from one user to another. In practice, we would probably want to choose $\mathcal{P}$ and $\mathcal{C}$ uniformly throughout the system. For example, suppose we are working in an N-letter alphabet. Then let $k < \ell$ be suitably chosen positive integers, such that, for example, N^k and N^ℓ have approximately 200 decimal digits. We take as our plaintext message units all blocks of k letters, which we regard as k-digit base-N integers, i.e., we assign them numerical equivalents between 0 and N^k. We similarly take ciphertext message units to be blocks of ℓ letters in our N-letter alphabet. Then each user must choose his/her large primes p_A and q_A so that $n_A = p_A q_A$ satisfies $N^k < n_A < N^\ell$. Then any plaintext message unit, i.e., integer less than N^k, corresponds to an element in $\mathbf{Z}/n_A\mathbf{Z}$ (for any user's n_A); and, since $n_A < N^\ell$, the image $f(P) \in \mathbf{Z}/n_A\mathbf{Z}$ can be uniquely written as an ℓ-letter block. (Not all ℓ-letter blocks can arise — only those corresponding to integers less than n_A for the particular user's n_A.)

Example 1. For the benefit of a reader who doesn't have a computer handy (or does not have good multiple precision software), we shall sacrifice realism and choose most of our examples so as to involve relatively small integers. Choose $N = 26$, $k = 3$, $\ell = 4$. That is, the plaintext consists of trigraphs and the ciphertext consists of four-graphs in the usual 26-letter alphabet. To send the message "YES" to a user A with enciphering key $(n_A, e_A) = (46927, 39423)$, we first find the numerical equivalent of "YES," namely: $24 \cdot 26^2 + 4 \cdot 26 + 18 = 16346$, and then compute $16346^{39423} \bmod 46927$, which is $21166 = 1 \cdot 26^3 + 5 \cdot 26^2 + 8 \cdot 26 + 2 =$ "BFIC."

The recipient A knows the deciphering key $(n_A, d_A) = (46927, 26767)$, and so computes $21166^{26767} \ mod\ 46927 = 16346$ ="YES." How did user A generate her keys? First, she multiplied the primes $p_A = 281$ and $q_A = 167$ to get n_A; then she chose e_A at random (but subject to the condition that $g.c.d.(e_A, 280) = g.c.d.(e_A, 166) = 1$). Then she found $d_A = e_A^{-1} \ mod\ 280 \cdot 166$. The numbers p_A, q_A, d_A remain secret.

In Example 1, how cumbersome are the computations? The most time-consuming step is modular exponentiation, e.g., $16346^{39423} \ mod\ 46927$. But this can be done by the repeated squaring method (see §I.3) in $O(k^3)$ bit operations, where k is the number of bits in our integers. Actually, if we were working with much larger integers, potentially the most time-consuming step would be for each user A to find two very large primes p_A and q_A. In order to quickly choose suitable very large primes, one must use an efficient primality test. Such tests will be described in the next chapter.

Remarks. **1.** In choosing p and q, user A should take care to see that certain conditions hold. The most important are: that the two primes not be too close together (for example, one should be a few decimal digits longer than the other); and that $p-1$ and $q-1$ have a fairly small g.c.d. and both have at least one large prime factor. Some of the reasons for these conditions are indicated in the exercises below. Of course, if someone discovers a factorization method that works quickly under certain other conditions on p and q, then future users of RSA would have to take care to avoid those conditions as well.

2. In §I.3 we saw that, when n is a product of two primes p and q, knowledge of $\varphi(n)$ is equivalent to knowledge of the factorization. Let's suppose now that we manage to break an RSA system by determining a positive integer d such that $a^{ed} \equiv a \ mod\ n$ for all a prime to n. This is equivalent to $ed-1$ being a multiple of the least common multiple of $p-1$ and $q-1$. Knowing this integer $m = ed-1$ is weaker than actually knowing $\varphi(n)$. But we now give a procedure that with a high probability is nevertheless able to use the integer m to factor n.

So suppose we know n — which is a product of two unknown primes — and also an integer m such that $a^m \equiv 1 \ mod\ n$ for all a prime to n. Notice that any such m must be even (as we see by taking $a = -1$). We first check whether $m/2$ has the same property, in which case we can replace m by $m/2$. If $a^{m/2}$ is *not* $\equiv 1 \ mod\ n$ for all a prime to n, then we

must have $a^{m/2} \not\equiv 1 \ mod\ n$ for at least 50% of the a's in $(\mathbf{Z}/n\mathbf{Z})^*$ (this statement is proved in exactly the same way as part (a) of Exercise 21 in §II.2). Thus, if we test several dozen randomly chosen a's and find that in all cases $a^{m/2} \equiv 1 \ mod\ n$, then with very high probability we have this congruence for all a prime to n, and so may replace m by $m/2$. We keep on doing this until we no longer have the congruence when we take half of the exponent. There are now two possibilities:

(i) $m/2$ is a multiple of one of the two numbers $p-1$, $q-1$ (say, $p-1$) but not both. In this case $a^{m/2}$ is always $\equiv 1 \ mod\ p$ but exactly 50% of the time is congruent to -1 rather than $+1$ modulo q.

(ii) $m/2$ is not a multiple of either $p-1$ or $q-1$. In this case $a^{m/2}$ is $\equiv 1$ modulo both p and q (and hence modulo n) exactly 25% of the time, it is $\equiv -1$ modulo both p and q exactly 25% of the time, and for the remaining 50% of the values of a it is $\equiv 1$ modulo one of the primes and $\equiv -1$ modulo the other prime.

Thus, by trying a's at random with high probability we will soon find an a for which $a^{m/2}-1$ is divisible by one of the two primes (say, p) but not the other. (Each randomly selected a has a 50% chance of satisfying this statement.) Once we find such an a we can immediately factor n, because $g.c.d.(n,\ a^{m/2}-1) = p$.

The above procedure is an example of a *probabilistic algorithm*. We shall encounter other probabilistic algorithms in the next chapter.

3. How do we send a signature in RSA? When discussing authentication in the last section, we assumed for simplicity that $\mathcal{P} = \mathcal{C}$. We have a slightly more complicated set-up in RSA. Here is one way to avoid the problem of different n_A's and different block sizes (k, the number of letters in a plaintext message unit, being less than ℓ, the number of letters in a ciphertext message unit). Suppose that, as in the last section, Alice is sending her signature (some plaintext P) to Bob. She knows Bob's enciphering key $K_{E,B} = (n_B, e_B)$ and her own deciphering key $K_{D,A} = (n_A, d_A)$. What she does is send $f_B f_A^{-1}(P)$ if $n_A < n_B$, or else $f_A^{-1} f_B(P)$ if $n_A > n_B$. That is, in the former case she takes the least positive residue of P^{d_A} modulo n_A; then, regarding that number modulo n_B, she computes $(P^{d_A} \ mod\ n_A)^{e_B} \ mod\ n_B$, which she sends as a ciphertext message unit. In the case $n_A > n_B$, she first computes $P^{e_B} \ mod\ n_B$ and then, working modulo n_A, she raises this to the d_A-th power. Clearly, Bob can verify the authenticity of the message

in the first case by raising to the d_B-th power modulo n_B and then to the e_A-th power modulo n_A; in the second case he does these two operations in the reverse order.

THE FAMOUS "LAST THEOREM"

With our knowledge of Pythagorean triples, we are now prepared to take up the one case in which Fermat himself had a proof of his conjecture, the case $n = 4$. The technique used in the proof is a form of induction sometimes called "Fermat's method of infinite descent." In brief, the method may be described as follows: It is assumed that a solution of the problem in question is possible in the positive integers. From this solution, one constructs a new solution in smaller positive integers, which then leads to a still smaller solution and so on. Since the positive integers cannot be decreased in magnitude indefinitely, it follows that the initial assumption must be false and therefore no solution is possible.

Instead of giving a proof of the Fermat Conjecture for $n = 4$, it turns out to be easier to establish a fact which is slightly stronger; namely, the impossibility of solving the equation $x^4 + y^4 = z^2$ in the positive integers.

THEOREM 11-3 (Fermat). *The Diophantine equation* $x^4 + y^4 = z^2$ *has no solution in positive integers* x, y, z.

Proof: With the idea of deriving a contradiction, let us assume that there exists a positive solution x_0, y_0, z_0 of $x^4 + y^4 = z^2$. Nothing is lost in supposing also that $\gcd(x_0, y_0) = 1$; otherwise, put $\gcd(x_0, y_0) = d$, $x_0 = dx_1, y_0 = dy_1, z_0 = d^2 z_1$ to get $x_1^4 + y_1^4 = z_1^2$ with $\gcd(x_1, y_1) = 1$.

Expressing the supposed equation $x_0^4 + y_0^4 = z_0^2$ in the form

$$(x_0^2)^2 + (y_0^2)^2 = z_0^2$$

we see that x_0^2, y_0^2, z_0 meet all the requirements of a primitive Pythagorean triple, and so Theorem 11-1 can be brought into play.

In such triples, one of the integers x_0^2 or y_0^2 is necessarily even, while the other is odd. Taking x_0^2 (and hence x_0) to be even, there exist relatively prime integers $s > t > 0$ satisfying

$$x_0^2 = 2st,$$
$$y_0^2 = s^2 - t^2,$$
$$z_0 = s^2 + t^2,$$

where exactly one of s and t is even. If it happened that s were even, then we would have

$$1 \equiv y_0^2 = s^2 - t^2 \equiv 0 - 1 \equiv 3 \pmod 4,$$

an impossibility. Therefore, s must be the odd integer and, in consequence, t is the even one. Let us put $t = 2r$. Then the equation $x_0^2 = 2st$ becomes $x_0^2 = 4sr$, which says that

$$(x_0/2)^2 = sr.$$

But Lemma 2 asserts that the product of two relatively prime integers [gcd $(s, t) = 1$ implies that gcd $(s, r) = 1$] is a square only if each of the integers is itself a square; hence, $s = z_1^2$, $r = w_1^2$ for positive integers z_1, w_1.

We wish to apply Theorem 11-1 again, this time to the equation

$$t^2 + y_0^2 = s^2.$$

Since gcd $(s, t) = 1$, it follows that gcd $(t, y_0, s) = 1$, making t, y_0, s a primitive Pythagorean triple. With t even, we obtain

$$t = 2uv,$$
$$y_0 = u^2 - v^2,$$
$$s = u^2 + v^2,$$

for relatively prime integers $u > v > 0$. Now the relation

$$uv = t/2 = r = w_1^2$$

signifies that u and v are both squares (Lemma 2 serves its purpose once more); say, $u = x_1^2$ and $v = y_1^2$. When these values are substituted into the equation for s the result is

$$z_1^2 = s = u^2 + v^2 = x_1^4 + y_1^4.$$

A crucial point is that, z_1 and t being positive, we also have the inequality

$$0 < z_1 \leq z_1^2 = s \leq s^2 < s^2 + t^2 = z_0.$$

What has happened is this: starting with one solution x_0, y_0, z_0 of $x^4 + y^4 = z^2$, we have constructed another solution x_1, y_1, z_1 such that $0 < z_1 < z_0$. Repeating the whole argument, our second solution would lead to a third solution x_2, y_2, z_2 with $0 < z_2 < z_1$, which in its turn gives rise to a fourth. This process can be carried out indefinitely to produce an infinite decreasing sequence of positive integers

$$z_0 > z_1 > z_2 > \cdots.$$

Since there is only a finite supply of positive integers less than z_0, a contradiction occurs. We are forced to conclude that $x^4 + y^4 = z^2$ is not solvable in the positive integers.

COROLLARY. *The equation $x^4 + y^4 = z^4$ has no solution in the positive integers.*

Proof: If x_0, y_0, z_0 were a positive solution of $x^4 + y^4 = z^4$, then x_0, y_0, z_0^2 would satisfy the equation $x^4 + y^4 = z^2$, in conflict with Theorem 11-3.

If $n > 2$, then n is either a power of 2 or divisible by an odd prime p. In the first case, $n = 4k$ for some $k \geq 1$ and the Fermat equation $x^n + y^n = z^n$ can be written as

$$(x^k)^4 + (y^k)^4 = (z^k)^4.$$

We have just seen that this equation is impossible in the positive integers. When $n = pk$, the Fermat equation is the same as

$$(x^k)^p + (y^k)^p = (z^k)^p.$$

If it could be shown that the equation $u^p + v^p = w^p$ has no solution, then, in particular, there would be no solution of the form $u = x^k$, $v = y^k$, $w = z^k$ and hence $x^n + y^n = z^n$ would not be solvable. Fermat's Conjecture therefore reduces to this: for no odd prime p does the equation

$$x^p + y^p = z^p$$

admit a solution in the positive integers.

Although the problem has challenged the foremost mathematicians of the last 300 years, their efforts have only produced partial results and proofs of individual cases. Euler gave the first proof of the Fermat Conjecture for the prime $p = 3$ in the year 1770; the reasoning was incomplete at one stage, but Legendre later supplied the missing steps. Using the method of infinite descent, Dirichlet and Legendre independently settled the case $p = 5$ around 1825. Not long thereafter, in 1839, Lamé proved the conjecture for seventh powers. With the increasing complexity of the arguments came the realization that a successful resolution of the general case called for different techniques. The best hope seemed to lie in extending the meaning of "integer" to include a wider class of numbers and, by attacking the problem within this enlarged system, obtaining more information than was possible by using ordinary integers only.

The German mathematician Kummer made the major breakthrough. In 1843, he submitted to Dirichlet a purported proof of the Fermat Conjecture based upon an extension of the integers to include the so-called "algebraic numbers" (that is, complex numbers satisfying polynomials with rational coefficients). Having spent considerable time on the problem himself, Dirichlet was immediately able to detect the flaw in the reasoning: Kummer had taken for granted that algebraic numbers admit a unique factorization similar to that of the ordinary integers, and this is not always true.

But Kummer was undeterred by this perplexing situation and returned to his investigations with redoubled effort. In order to restore unique factorization to the algebraic numbers, he was led to invent the concept of *ideal numbers*. By adjoining these new entities to the algebraic numbers, Kummer successfully proved the Fermat Conjecture for a large class of primes which he termed "regular primes" (that this represented an enormous achievement is reflected in the fact that the only irregular primes less than 100 are 37, 59, and 67.). Unfortunately, it is still not known whether there are an infinite number of regular primes, while, in the other direction, Jensen (1915) established that there exist infinitely many irregular ones. Almost all the subsequent progress on the problem has been within the framework suggested by Kummer.

To round out our historical digression, we might mention that in 1908 a prize of 100,000 marks was bequeathed to the Academy of Science at Göttingen to be paid for the first complete proof of Fermat's Conjecture. The immediate result was a deluge of incorrect demonstrations by amateur mathematicians. Since only printed solutions were eligible, Fermat's Conjecture is reputed to be the mathematical problem for which the greatest number of false proofs have been published; indeed, between 1908 and 1912 over 1000 alleged proofs appeared, mostly printed as private pamphlets. Suffice it to say, interest declined as the German inflation of the 1920's wiped out the monetary value of the prize.

From $x^4 + y^4 = z^2$, we move on to a closely related Diophantine equation, namely, $x^4 - y^4 = z^2$. The proof of its insolubility parallels that of Theorem 11-3, but we give a slight variation in the method of infinite descent.

THEOREM 11-4 (Fermat). *The Diophantine equation $x^4 - y^4 = z^2$ has no solution in positive integers x, y, z.*

Proof: The proof proceeds by contradiction. Let us assume that the equation admits a solution in the positive integers and among these solutions x_0, y_0, z_0 is one with a least value of x; in particular, this supposition forces x_0 to be odd (Why?). Were $\gcd(x_0, y_0) = d > 1$,

then putting $x_0 = dx_1, y_0 = dy_1$, we would have $d^4(x_1^4 - y_1^4) = z_0^2$, whence $d^2 \mid z_0$ or $z_0 = d^2 z_1$ for some $z_1 > 0$. It follows that x_1, y_1, z_1 provides a solution to the equation under consideration with $0 < x_1 < x_0$, an impossible situation. Thus, we are free to assume a solution x_0, y_0, z_0 in which $\gcd(x_0, y_0) = 1$. The ensuing argument falls into two stages, depending on whether y_0 is odd or even.

First, consider the case of an odd integer y_0. If the equation $x_0^4 - y_0^4 = z_0^2$ is written in the form $z_0^2 + (y_0^2)^2 = (x_0^2)^2$, one sees that z_0, y_0^2, x_0^2 constitute a primitive Pythagorean triple. Theorem 11-1 asserts the existence of relatively prime integers $s > t > 0$ for which

$$z_0 = 2st,$$
$$y_0^2 = s^2 - t^2,$$
$$x_0^2 = s^2 + t^2.$$

It thus appears that

$$s^4 - t^4 = (s^2 + t^2)(s^2 - t^2) = x_0^2 y_0^2 = (x_0 y_0)^2,$$

making s, t, $x_0 y_0$ a (positive) solution to the equation $x^4 - y^4 = z^2$. Since

$$0 < s < \sqrt{s^2 + t^2} = x_0,$$

we arrive at a contradiction to the minimal nature of x_0.

For the second part of the proof, assume that y_0 is an even integer. Using the formulas for primitive Pythagorean triples, we now write

$$y_0^2 = 2st,$$
$$z_0 = s^2 - t^2,$$
$$x_0^2 = s^2 + t^2,$$

It thus appears that

$$s^4 - t^4 = (s^2 + t^2)(s^2 - t^2) = x_0^2 y_0^2 = (x_0 y_0)^2,$$

making s, t, $x_0 y_0$ a (positive) solution to the equation $x^4 - y^4 = z^2$.

Since

$$0 < s < \sqrt{s^2 + t^2} = x_0,$$

we arrive at a contradiction to the minimal nature of x_0.

For the second part of the proof, assume that y_0 is an even integer. Using the formulas for primitive Pythagorean triples, we now write

$$y_0^2 = 2st,$$
$$z_0 = s^2 - t^2,$$
$$x_0^2 = s^2 + t^2,$$

where s may be taken to be even and t to be odd. Then, in the relation $y_0^2 = 2st$, we have gcd $(2s, t) = 1$. The by-now-customary Lemma 2 tells us that $2s$ and t are each squares of positive integers; say, $2s = w^2$, $t = v^2$. Since w must of necessity be an even integer, set $w = 2u$ to get $s = 2u^2$. Therefore,

$$x_0^2 = s^2 + t^2 = 4u^4 + v^4$$

and so $2u^2$, v^2, x_0 forms a primitive Pythagorean triple. Falling back on Theorem 11-1 again, there exist integers $a > b > 0$ for which

$$2u^2 = 2ab,$$
$$v^2 = a^2 - b^2,$$
$$x_0 = a^2 + b^2,$$

where gcd $(a, b) = 1$. The equality $u^2 = ab$ ensures that a and b are perfect squares, so that $a = c^2$ and $b = d^2$. Knowing this, the rest of the proof is easy; for, upon substituting,

$$v^2 = a^2 - b^2 = c^4 - d^4.$$

The result is a new solution c, d, v of the given equation $x^4 - y^4 = z^2$ and what's more, a solution in which

$$0 < c = \sqrt{a} < a^2 + b^2 = x_0,$$

contrary to our assumption regarding x_0.

The only resolution of these contradictions is that the equation $x^4 - y^4 = z^2$ cannot be satisfied in the positive integers.

THEOREM 11-5. *The area of a Pythagorean triangle can never be equal to a perfect (integral) square.*

Proof: Consider a Pythagorean triangle whose hypotenuse has length z and other two sides have lengths x and y, so that $x^2 + y^2 = z^2$. The area of the triangle in question is $\frac{1}{2}xy$ and if this were a square, say u^2, it would follow that $2xy = 4u^2$. By adding and subtracting the last-written equation from $x^2 + y^2 = z^2$, we are led to

$$(x + y)^2 = z^2 + 4u^2 \quad \text{and} \quad (x - y)^2 = z^2 - 4u^2.$$

When these last two equations are multiplied together, the outcome is that two fourth powers have as their difference a square:

$$(x^2 - y^2)^2 = z^4 - 16u^4 = z^4 - (2u)^4.$$

Since this amounts to an infringement of Theorem 11-4, there can be no Pythagorean triangle whose area is a square.

There are a number of simple problems pertaining to Pythagorean triangles that still await solution. The Corollary to Theorem 11-3 may be expressed by saying that there exists no Pythagorean triangle all the sides of which are squares. However, it is not difficult to produce Pythagorean triangles whose sides, if increased by 1, are squares; for instance, the triangles associated with the triples $13^2 - 1$, $10^2 - 1$, $14^2 - 1$, and $287^2 - 1$, $265^2 - 1$, $329^2 - 1$. An obvious—and as yet unanswered—question is whether there are an infinite number of such triangles. One can find Pythagorean triangles each side of which is a triangular number. [By a triangular number, we mean an integer of the form $t_n = n(n + 1)/2$.] An example of such is the triangle corresponding to $t_{132}, t_{143}, t_{164}$. It is not known if there exist infinitely many Pythagorean triangles of this type.

As a closing comment, we should observe that all the effort expended on attempting to prove Fermat's Conjecture has been far from wasted. The new mathematics that was developed as a by-product laid the foundations for algebraic number theory, as well as the ideal theory of modern abstract algebra. It seems fair to say that the value of these far exceeds that of the conjecture itself.

PROBLEMS

1. Show that the equation $x^2+y^2=z^3$ has infinitely many solutions for x, y, z positive integers. [*Hint:* For any $n>3$, let $x=n(n^2-3)$ and $y=3n^2-1$.]
2. Prove the theorem: The only solutions in nonnegative integers of the equation $x^2+2y^2=z^2$, with gcd $(x, y, z)=1$, are given by

$$x=\pm(2s^2-t^2),\ y=2st,\ z=2s^2+t^2$$

where s, t are arbitrary nonnegative integers. [*Hint:* If u, v, w are such that $y=2w$, $z+x=2u$, $z-x=2v$, then the equation becomes $2w^2=uv$.]

POSSIBLE QUESTIONS

2 Mark Questions:

1. Evaluate the Legendre symbol $(71/73)$.
2. Evaluate the Legendre symbol $(-219/383)$.
3. Solve the congruence $x^2 \equiv 31 (\mathrm{mod}\, 11^4)$.
4. What is Hash function.
5. Define Pythagorean triple.
6. If x, y, z is a primitive Pythagorean triple, then prove one of the integers x and y is even, while the other is odd.
7. Give an example of Pythagorean triple.

8 Mark Questions:

1. State and prove Gauss Quadratic Reciprocity Law.
2. If p is an odd prime and $\gcd(a, p) = 1,$ then prove that e congruence
$$x^2 \equiv a (\mathrm{mod}\, p^n), \qquad n \geq 1$$
has a solution if and only if $(a/p) = 1$.
3. Let a be an odd integer. then prove
   (i) $x^2 \equiv a (\mathrm{mod}\, 2)$ always has a solution.
   (ii) $x^2 \equiv a (\mathrm{mod}\, 4)$ has a solution if and only if $a \equiv 1 (\mathrm{mod}\, 4)$.
   (iii) $x^2 \equiv a (\mathrm{mod}\, 2^n)$, for $n \geq 3,$ has a solution if and only if $a \equiv 1 (\mathrm{mod}\, 8)$.
4. Explain about Public key encryption.
5. Describe RSA encryption and decryption.
6. If $ab = c^n$, where $\gcd(a, b) = 1,$ then prove a and b are n^{th} power. this is, there exist positive integers a_1, b_1 for which $a = a_1^n, b = b_1^n$.
7. Find all the solution of the Pythagorean equation
$$x^2 + y^2 = z^2$$
Satisfying the conditions
$$\gcd(x, y, z) = 1, \quad 2 | x, \; x > 0, y > 0, z > 0$$
are given by the formulas
$$x = 2st, y = s^2 - t^2, z = s^2 + t^2$$
for integers $s > t > 0$ such that $\gcd(s, t) = 1$ and $s \not\equiv t (\mathrm{mod}\, 2)$.

8. Find all primitive solution of $x^2 + y^2 = z^2$ having $0 < z < 30$.
9. Prove that the area of a Pythagorean triangle can never be equal to a perfect (integral) square.
10. Prove that the Diophantine equation $x^4 + y^4 = z^4$ has no solution in positive integer $x, y, z.$
11. Prove that the Diophantine equation $x^4 - y^4 = z^4$ has no solution in positive integer $x, y, z.$