Semester – III

18MMP302 **NUMBER THEORY** **4H – 4C**

Instruction Hours / week: L: 4 T: 0 P: 0 **Marks:** Internal: **40** External: **60** Total: **100**

End Semester Exam: 3 Hours

Course Objectives

This course enables the students to learn

- Mathematical concepts and principles to perform numerical and symbolic computations.
- To investigate and solve mathematical and statistical problems.
- To write clear and precise proofs.
- To communicate effectively in both written and oral form.
- To demonstrate the ability to read and learn mathematics and/or statistics independently.

Course Outcomes (COs)

On successful completion of this course, students will be able to

1. Identify and apply various properties of and relating to the integers including the Well-Ordering Principle, primes, unique factorization, the division algorithm, and greatest common divisors.
2. Identify certain number theoretic functions and their properties.
3. Understand the concept of a congruence and use various results related to congruences including the Chinese Remainder Theorem.
4. Solve certain types of Diophantine equations.
5. Identify how number theory is related to and used in cryptography

UNIT I

DIVISIBILITY

Introduction - Divisibility - Primes - The Bionomial Theorem

UNIT II

CONGRUENCES

Congruences - Solutions of Congruences - The Chinese Remainder Theorem - Techniques of Numerical Calculation - Public-Key Cryptography - Prime Power Moduli - Prime Modulus

UNIT III

CONGRUENCES (CONTINUITY)

Primitive Roots and Power Residues - Congruences of Degree Two, Prime Modulus - Number Theory from an Algebraic Viewpoint - Groups, Rings, and Fields

UNIT IV

QUADRATIC RECIPROCITY AND QUADRATIC FORMS

Quadratic Residues - Quadratic Reciprocity - The Jacobi Symbol - Binary Quadratic Forms - Equivalence and Reduction of Binary Quadratic Forms - Sums of Two Squares - Positive Definite Binary Quadratic Forms

UNIT V

SOME FUNCTIONS OF NUMBER THEORY

Greatest Integer Function - Arithmetic Functions - The Mobius Inversion Formula - Recurrence Functions - Combinatorial Number Theory

SUGGESTED READINGS

1. Ivan Nivan and HerbertsZucherman., (1972), An Introduction to Theory of Numbers third Edition, Wiley Eastern Limited, New Delhi.
2. ApostolT.M., (1976), Introduction to Analytic Number Theory, Springer Verlag,.
3. Kennath and Rosan, (1968).,Elementary Number Theory and its Applications, Addison Wesley Publishing Company.
4. George E. Andrews., (1989) Number Theory, Hindustan Publishing, 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:18MMP302**
Semester: III **Class: II M. Sc Mathematics**

S.No	Lecture Duration Period	Topics to be Covered	Support Material/ Page Nos
UNIT-I			
1.	1	Introduction	S_1: Chap 1: P.No:1-4
2.	1	Divisibility –definition and theorems	S_1: Chap 1: P.No:4-6
3.	1	Greatest common divisor –Definition and theorem	S_1: Chap 1: P.No:7-11
4.	1	Euclidean algorithm with problems	S_1: Chap 1: P.No:11-15
5.	1	Continuation of problems on Euclidean algorithm	S_2: Chap 1: P.No:21-22
6.	1	Least common multiple – definition and theorems	S_1: Chap 1: P.No:16
7.	1	Prime number –definition and theorems	S_1: Chap 1: P.No:20-23
8.	1	Fundamental theorem of arithmetic and Euclid theorem	S_1: Chap 1: P.No:23-28
9.	1	Problems on fundamental theorem of arithmetic	S_4: Chap 1: P.No:21-23
10.	1	Binomial theorem –definition and theorems	S_1: Chap 1: P.No:35-40
11.	1	Recapitulation and discussion on possible questions	
	Total no. of hours planned for unit-1 is 11		
UNIT-II			
1.	1	Congruence-definition and theorem	S_1: Chap 2: P.No:48-50
2.	1	Continuation of theorem on congruence	S_1: Chap 2: P.No:50-56

3.	1	Solution of congruence-definition and theorem	S_1: Chap 2: P.No:61-62
4.	1	The Chinese remainder theorem	S_1: Chap 2: P.No:64-69
5.	1	Problems on The Chinese remainder theorem	S_3: Chap 3: P.No:113-114
6.	1	Continuation of the problems on Chinese remainder theorem	S_1: Chap 2: P.No:69-71
7.	1	Techniques of Numerical Calculation	S_1: Chap 2: P.No:74-81
8.	1	Public-Key Cryptography	S_1: Chap 2: P.No:84-90
9.	1	Prime Power Moduli and Prime Modulu	S_1: Chap 2: P.No:91-96
10.	1	Recapitulation and discussion of possible questions	
	Total no. of hours planned for unit-2 is 10		
UNIT-III			
1.	1	Primitive roots and power residues-definition and theorems	S_1: Chap 2: P.No:97-101
2.	1	Continuation of theorems on Primitive roots and power residues	S_1: Chap 2: P.No:101-106
3.	1	Continuation of theorems on Primitive roots and power residues	S_1: Chap 2: P.No:101-106
4.	1	Congruence of Degree Two, Prime Modulus	S_1: Chap 2: P.No:110-114
5.	1	Number Theory from an Algebraic Viewpoint	S_1: Chap 2: P.No:115-119
6.	1	Groups, Rings, and Fields -theorems	S_1: Chap 2: P.No:121-124
7.	1	Continuation of theorems on groups, rings, and fields	S_1: Chap 2: P.No:124-126
8.	1	Recapitulation and discussion of possible questions	
	Total no. of hours planned for unit 3 is 8		
UNIT-IV			
1.	1	Quadratic Residues- definition and	S_1: Chap 3: P.No:131-135

		theorems	
2.	1	Quadratic Reciprocity-theorems	S_1: Chap 3: P.No:137-140
3.	1	The Jacobi Symbol –definition and theorems	S_1: Chap 3: P.No:142-147
4.	1	Binary Quadratic Forms- definition and theorems	S_1: Chap 3: P.No:150-154
5.	1	Equivalence and Reduction of Binary Quadratic Forms	S_1: Chap 3: P.No:155-161
6.	1	Sums of Two Squares -theorems	S_1: Chap 3: P.No:163-169
7.	1	Sums of Two Squares -theorems	S_1: Chap 3: P.No:163-169
8.	1	Positive Definite Binary Quadratic Forms	S_1: Chap 3: P.No:170-175
9.	1	Recapitulation and discussion of possible questions	
	Total no. of hours planned for unit 4 is 9		
UNIT-V			
1.	1	Greatest Integer function-definition and theorem	S_1: Chap 4: P.No:182-184
2.	1	Arithmetic Functions –definition and theorems	S_1: Chap 4: P.No:188-191
3.	1	The Mobius Inversion Formula-definition and theorems	S_1: Chap 4: P.No:193-195
4.	1	Recurrence Functions-concept and theorems	S_1: Chap 4: P.No:197-201
5.	1	Continuation of theorem on recurrence functions	S_1: Chap 4: P.No:201-204
6.	1	Combinatorial Number Theory	S_1: Chap 4: P.No:206-210
7.	1	Recapitulation and discussion on possible questions	
8.	1	Discuss on previous year ESE question papers	
9.	1	Discuss on previous year ESE question papers	
10.	1	Discuss on previous year ESE question papers	

	Total No of Hours Planned for unit 5 is 10	
	Total Planned Hours-48	

SUGGESTED READINGS

1. Ivan Nivan and HerbertsZucherman., (1972), An Introduction to Theory of Numbers third Edition, Wiley Eastern Limited, New Delhi.
2. ApostolT.M., (1976), Introduction to Analytic Number Theory, Springer Verlag,.
3. Kennath and Rosan, (1968).,Elementary Number Theory and its Applications, Addison Wesley Publishing Company.
4. George E. Andrews., (1989) Number Theory, Hindustan Publishing, New Delhi.

UNIT-I

SYLLABUS

Introduction - Divisibility - Primes - The Binomial 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 $n_k = n + kp$ 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

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

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 $ax \equiv b(\text{mod } n)$ has a unique solution modulo n.
10. State Chinese Remainder theorem.

8 Mark Questions:

1. State and Prove Binomial theorem
2. 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.

3. 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) $84x - 438y = 156.$

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

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

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

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

5. State and prove fundamental theorem of Arithmetic.

6. State and prove Euclid Lemma.

7. Prove that if p_n is the nth prime number, then $p_n \leq 2^{2^{n-1}}$.

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

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

10. State and Prove Chinese Remainder theorem.

11. Solve the following linear congruence:

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

UNIT-II

SYLLABUS

Congruences - Solutions of Congruences - The Chinese Remainder Theorem - Techniques of Numerical Calculation - Public-Key Cryptography - Prime Power Moduli - Prime Modulus

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

$$(p-1)! \equiv 1 \cdot (-1) \cdot 2 \cdot (-2) \cdots \frac{p-1}{2} \cdot \left(-\frac{p-1}{2}\right) \pmod{p}$$

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

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) 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 $n=p_1^{k_1}p_2^{k_2}\ldots p_r^{k_r}$ is the prime factorization of $n>1$, then the positive divisors of n are precisely those integers d of the form

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

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

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

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

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

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_1d_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 $x^2\equiv -1(\text{mod } p)$, p is a prime, has a solution if and only if $p\equiv 1(\text{mod } 4)$.

UNIT-IV

SYLLABUS

Quadratic Residues - Quadratic Reciprocity - The Jacobi Symbol - Binary Quadratic Forms - Equivalence and Reduction of Binary Quadratic Forms - Sums of Two Squares - Positive Definite Binary Quadratic Forms

Definition 3.1 *For all a such that $(a, m) = 1$, a is called a* quadratic residue *modulo m if the congruence $x^2 \equiv a \pmod{m}$ has a solution. If it has no solution, then a is called a* quadratic nonresidue *modulo m.*

Since $a + m$ is a quadratic residue or nonresidue modulo m according as a is or is not, we consider as distinct residues or nonresidues only those that are distinct modulo m. The quadratic residues modulo 5 are 1 and 4, whereas 2 and 3 are the nonresidues.

Theorem 3.1 *Let p be an odd prime. Then*

(1) $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$,

(2) $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$,

(3) $a \equiv b \pmod{p}$ *implies that* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$,

(4) If $(a, p) = 1$ *then* $\left(\frac{a^2}{p}\right) = 1$, $\left(\frac{a^2 b}{p}\right) = \left(\frac{b}{p}\right)$,

(5) $\left(\frac{1}{p}\right) = 1$, $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$.

Remark From our observations in Section 2.9, we see that if p is an odd prime then for any integer a the number of solutions of the congruence $x^2 \equiv a \pmod{p}$ is $1 + \left(\frac{a}{p}\right)$.

Proof If $p|a$, then Part 1 of the theorem is obvious. If $(a, p) = 1$ then Part 1 follows from Euler's criterion (Corollary 2.38). The remaining parts are all simple consequences of Part 1.

Part 1 can also be proved without appealing to Euler's criterion, as follows: If $\left(\frac{a}{p}\right) = 1$, then $x^2 \equiv a \pmod{p}$ has a solution, say x_0. Then, by

Fermat's congruence (Theorem 2.7), $a^{(p-1)/2} \equiv x_0^{p-1} \equiv 1 \equiv \left(\frac{a}{p}\right) \pmod{p}$. On the other hand, if $\left(\frac{a}{p}\right) = -1$, then $x^2 \equiv a \pmod{p}$ has no solution, and we proceed as in the proof of Wilson's congruence (Theorem 2.11). To each j satisfying $1 \leqslant j < p$, choose j', $1 \leqslant j' < p$, so that $jj' \equiv a \pmod{p}$. We pair j with j'. We note that $j \not\equiv j' \pmod{p}$, since the congruence $x^2 \equiv a \pmod{p}$ has no solution. The combined contribution of j and j' to $(p-1)!$ is $jj' \equiv a \pmod{p}$. Since there are $(p-1)/2$ pairs j, j', it follows that $a^{(p-1)/2} \equiv (p-1)! \pmod{p}$, and then Wilson's congruence gives Part 1.

Theorem 3.2 *Lemma of Gauss. For any odd prime p let $(a, p) = 1$. Consider the integers $a, 2a, 3a, \cdots, \{(p-1)/2\}a$ and their least positive residues modulo p. If n denotes the number of these residues that exceed $\frac{p}{2}$, then $\left(\frac{a}{p}\right) = (-1)^n$.*

Proof Let $r_1, r_2, \cdots, r_n$ denote the residues that exceed $p/2$, and let $s_1, s_2, \cdots, s_k$ denote the remaining residues. The r_i and s_i are all distinct, and none is zero. Furthermore, $n + k = (p-1)/2$. Now $0 < p - r_i < p/2$, $i = 1, 2, \cdots, n$, and the numbers $p - r_i$ are distinct. Also no $p - r_i$ is an s_j for if $p - r_i = s_j$ then $r_i \equiv \rho a$, $s_j \equiv \sigma a \pmod{p}$ for some ρ, σ, $1 \leqslant \rho \leqslant (p-1)/2$, $1 \leqslant \sigma \leqslant (p-1)/2$, and $p - \rho a \equiv \sigma a \pmod{p}$. Since $(a, p) = 1$ this implies $a(\rho + \sigma) \equiv 0$, $\rho + \sigma \equiv 0 \pmod{p}$, which is impossible. Thus $p - r_1, p - r_2, \cdots, p - r_n, s_1, s_2, \cdots, s_k$ are all distinct, are all at least 1 and less than $p/2$, and they are $n + k = (p-1)/2$ in number. That is, they are just the integers $1, 2, \cdots, (p-1)/2$ in some order. Multiplying them together we have

$$(p - r_1)(p - r_2) \cdots (p - r_n) s_1 s_2 \cdots s_k = 1 \cdot 2 \cdots \frac{p-1}{2}$$

and then

$$(p-r_1)(p-r_2)\cdots(p-r_n)s_1s_2\cdots s_k = 1\cdot 2\cdots\frac{p-1}{2}$$

and then

$$(-r_1)(-r_2)\cdots(-r_n)s_1s_2\cdots s_k \equiv 1\cdot 2\cdots\frac{p-1}{2} \pmod p,$$

$$(-1)^n r_1r_2\cdots r_n s_1s_2\cdots s_k \equiv 1\cdot 2\cdots\frac{p-1}{2} \pmod p,$$

$$(-1)^n a\cdot 2a\cdot 3a\cdots\frac{p-1}{2}a \equiv 1\cdot 2\cdots\frac{p-1}{2} \pmod p.$$

We can cancel the factors $2, 3, \cdots, (p-1)/2$ to obtain $(-1)^n a^{(p-1)/2} \equiv 1 \pmod p$ which gives us $(-1)^n \equiv a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod p$ by Theorem 3.1, part 1.

Definition 3.3 *For real x, the symbol $[x]$ denotes the greatest integer less than or equal to x.*

This is also called the *integral part* of x, and $x-[x]$ is called the *fractional part*. Such an integer as $[1000/23]$ is the quotient when 1000 is divided by 23 and is also the number of positive multiples of 23 less than 1000. On a hand calculator, its value, 43, is immediately obtained by dividing 1000 by 23 and taking the integer part of the answer only. Here are further examples: $[15/2] = 7$, $[-15/2] = -8$, $[-15] = -15$.

Theorem 3.3 *If p is an odd prime and $(a, 2p) = 1$, then*

$$\left(\frac{a}{p}\right) = (-1)^t \quad \textit{where} \quad t = \sum_{j=1}^{(p-1)/2}\left[\frac{ja}{p}\right]; \quad \textit{also} \quad \left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

Proof We use the same notation as in the proof of Theorem 3.2. The r_i and s_i are just the least positive remainders obtained on dividing the integers ja by p, $j = 1, 2, \cdots, (p-1)/2$. The quotient in this division is easily seen to be $q = [ja/p]$. Then for $(a, p) = 1$, whether a is odd or even, we have

$$\sum_{j=1}^{(p-1)/2} ja = \sum_{j=1}^{(p-1)/2} p\left[\frac{ja}{p}\right] + \sum_{j=1}^{n} r_j + \sum_{j=1}^{k} s_j$$

and

$$\sum_{j=1}^{(p-1)/2} j = \sum_{j=1}^{n} (p - r_j) + \sum_{j=1}^{k} s_j = np - \sum_{j=1}^{n} r_j + \sum_{j=1}^{k} s_j$$

and hence by subtraction,

$$(a-1)\sum_{j=1}^{(p-1)/2} j = p\left(\sum_{j=1}^{(p-1)/2}\left[\frac{ja}{p}\right] - n\right) + 2\sum_{j=1}^{n} r_j.$$

But

$$\sum_{j=1}^{(p-1)/2} j = \frac{p^2-1}{8}$$

so we have

$$(a-1)\frac{p^2-1}{8} \equiv \sum_{j=1}^{(p-1)/2}\left[\frac{ja}{p}\right] - n \pmod 2.$$

If a is odd, this implies $n \equiv \sum_{j=1}^{(p-1)/2}\left[\frac{ja}{p}\right] \pmod 2$. If $a = 2$ it implies $n \equiv (p^2-1)/8 \pmod 2$ since $[2j/p] = 0$ for $1 \leqslant j \leqslant (p-1)/2$. Our theorem now follows by Theorem 3.2.

QUADRATIC RECIPROCITY

Theorem 3.4 *The Gaussian reciprocity law. If p and q are distinct odd primes, then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\{(p-1)/2\}\{(q-1)/2\}}.$$

Another way to state this is: If p and q are distinct odd primes of the form $4k + 3$, then one of the congruences $x^2 \equiv p \pmod{q}$ and $x^2 \equiv q \pmod{p}$ is solvable and the other is not; but if at least one of the primes is of the form $4k + 1$, then both congruences are solvable or both are not.

Proof Let $\mathcal{S}$ be the set of all pairs of integers (x, y) satisfying $1 \leqslant x \leqslant (p-1)/2$, $1 \leqslant y \leqslant (q-1)/2$. The set $\mathcal{S}$ has $(p-1)(q-1)/4$ members. Separate this set into two mutually exclusive subsets $\mathcal{S}_1$ and $\mathcal{S}_2$ according as $qx > py$ or $qx < py$. Note that there are no pairs (x, y) in $\mathcal{S}$ such that $qx = py$. The set $\mathcal{S}_1$ can be described as the set of all pairs (x, y) such that $1 \leqslant x \leqslant (p-1)/2$, $1 \leqslant y < qx/p$. The number of pairs in $\mathcal{S}_1$ is then seen to be $\sum_{x=1}^{(p-1)/2}[qx/p]$. Similarly $\mathcal{S}_2$ consists of the pairs (x, y) such that $1 \leqslant y \leqslant (q-1)/2$, $1 \leqslant x < py/q$, and the number of pairs in $\mathcal{S}_2$ is $\sum_{y=1}^{(q-1)/2}[py/q]$. Thus we have

$$\sum_{j=1}^{(p-1)/2}\left[\frac{qj}{p}\right] + \sum_{j=1}^{(q-1)/2}\left[\frac{pj}{q}\right] = \frac{p-1}{2}\frac{q-1}{2}$$

and hence

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\{(p-1)/2\}\{(q-1)/2\}}$$

by Theorem 3.3.

For Example

$$\left(\frac{-42}{61}\right) = \left(\frac{-1}{61}\right)\left(\frac{2}{61}\right)\left(\frac{3}{61}\right)\left(\frac{7}{61}\right),$$

$$\left(\frac{-1}{61}\right) = (-1)^{60/2} = 1,$$

$$\left(\frac{2}{61}\right) = (-1)^{(61^2-1)/8} = -1,$$

$$\left(\frac{3}{61}\right) = \left(\frac{61}{3}\right)(-1)^{(2/2\times 60/2)} = \left(\frac{1}{3}\right) = 1,$$

$$\left(\frac{7}{61}\right) = \left(\frac{61}{7}\right)(-1)^{(6/2\times 60/2)} = \left(\frac{5}{7}\right) = \left(\frac{7}{5}\right)(-1)^{(4/2\times 6/2)} = \left(\frac{2}{5}\right)$$

$$= (-1)^{24/8} = -1.$$

Hence $\left(\frac{-42}{61}\right) = 1$. This computation demonstrates a number of different sorts of steps; it was chosen for this purpose and is not the shortest possible. A shorter way is

$$\left(\frac{-42}{61}\right) = \left(\frac{19}{61}\right) = \left(\frac{61}{19}\right) \cdot 1 = \left(\frac{4}{19}\right) = 1.$$

One could also obtain the value of $\left(\frac{-42}{61}\right)$ by use of Theorem 3.2 or the first part of Theorem 3.3, but the computation would be considerably longer.

There is another kind of problem that is of some importance. As an example, let us find all odd primes p such that 3 is a quadratic residue modulo p. We have

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)(-1)^{(p-1)/2},$$

$$\left(\frac{p}{3}\right) = \begin{cases} \left(\frac{1}{3}\right) = 1 & \text{if} \quad p \equiv 1 \pmod 3 \\ \left(\frac{2}{3}\right) = -1 & \text{if} \quad p \equiv 2 \pmod 3, \end{cases}$$

and

$$(-1)^{(p-1)/2} = \begin{cases} 1 & \text{if} \quad p \equiv 1 \pmod 4 \\ -1 & \text{if} \quad p \equiv 3 \pmod 4. \end{cases}$$

Thus $\left(\frac{3}{p}\right) = 1$ if and only if $p \equiv 1 \pmod 3$, $p \equiv 1 \pmod 4$, or $p \equiv 2 \pmod 3$, $p \equiv 3 \pmod 4$; that is $p \equiv 1$ or $11 \pmod{12}$.

Just as we determined which primes have 3 as a quadratic residue, so for any odd prime p we can analyze which primes have p as a quadratic residue. This is done in effect in the following result.

Theorem 3.5 *Let p be an odd prime. For any odd prime $q > p$ let r be determined as follows. First if p is of the form $4n + 1$, define r as the least positive remainder when q is divided by p; thus $q = kp + r$, $0 < r < p$. Next if p is of the form $4n + 3$, there is a unique r defined by the relations $q = 4kp \pm r$, $0 < r < 4p$, $r \equiv 1 \pmod 4$. Then in both cases* $\left(\frac{p}{q}\right) = \left(\frac{r}{p}\right)$.

Proof If $p = 4n + 1$, by Theorems 3.4 and 3.1, part 3, we see that $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = \left(\frac{r}{p}\right)$. In case $p = 4n + 3$, we first prove that r exists to satisfy the conditions stated. Let r_0 be the least positive remainder when q is divided by $4p$, so $0 < r_0 < 4p$. If $r_0 \equiv 1 \pmod 4$, take $r = r_0$; if $r_0 \equiv 3 \pmod 4$ take $r = 4p - r_0$. The uniqueness of r is readily established.

If $q = 4kp + r$, then $q \equiv r \equiv 1 \pmod 4$ and again $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = \left(\frac{r}{p}\right)$.

If $q = 4kp - r$, then $q \equiv -r = 3 \pmod 4$ and by Theorems 3.4 and 3.1, Parts 3 and 4, we have

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right) = -\left(\frac{-r}{p}\right) = -\left(\frac{-1}{p}\right)\left(\frac{r}{p}\right) = \left(\frac{r}{p}\right).$$

For example, suppose we want to determine all odd primes q that have 11 as a quadratic residue. A complete set of quadratic residues r of 11 satisfying $0 < r < 44$ and $r \equiv 1 \pmod 4$ is $1, 5, 9, 25, 37$. Hence by Theorem 3.5 the odd primes q having 11 as a quadratic residue are precisely those primes of the form $44k \pm r$ where $r = 1$, 5, 9, 25, or 37.

THE JACOBI SYMBOL

Definition

Let Q be positive and odd, so that $Q = q_1 q_2 \cdots q_s$ where the q_i are odd primes, not necessarily distinct. Then the Jacobi symbol $\left(\frac{P}{Q}\right)$ *is defined by*

$$\left(\frac{P}{Q}\right) = \prod_{j=1}^{s} \left(\frac{P}{q_j}\right)$$

where $\left(\frac{P}{q_j}\right)$ is the Legendre symbol.

Theorem

Suppose that Q and Q' are odd and positive. Then

(1) $\left(\frac{P}{Q}\right)\left(\frac{P}{Q'}\right) = \left(\frac{P}{QQ'}\right)$,

(2) $\left(\frac{P}{Q}\right)\left(\frac{P'}{Q}\right) = \left(\frac{PP'}{Q}\right)$,

(3) *if* $(P, Q) = 1$, *then* $\left(\frac{P^2}{Q}\right) = \left(\frac{P}{Q^2}\right) = 1$,

(4) *if* $(PP', QQ') = 1$, *then* $\left(\frac{P'P^2}{Q'Q^2}\right) = \left(\frac{P'}{Q'}\right)$,

(5) $P' \equiv P \pmod{Q}$ *implies* $\left(\frac{P'}{Q}\right) = \left(\frac{P}{Q}\right)$.

Proof Part 1 is obvious from the definition of $\left(\frac{P}{Q}\right)$, and part 2 follows from the definition and Theorem 3.1, part 2. Then part 3 follows from (2) and (1) and so also does (4). To prove part 5, we write $Q = q_1 q_2 \cdots q_s$. Then $P' \equiv P \pmod{q_j}$ so that $\left(\frac{P'}{q_j}\right) = \left(\frac{P}{q_j}\right)$ by Theorem 3.1, part 3, and then we have part 5 from Definition 3.4.

Theorem

If Q is odd and $Q > 0$, then

$$\left(\frac{-1}{Q}\right) = (-1)^{(Q-1)/2} \qquad \text{and} \qquad \left(\frac{2}{Q}\right) = (-1)^{(Q^2-1)/8}$$

Proof We have

$$\left(\frac{-1}{Q}\right) = \prod_{j=1}^{s}\left(\frac{-1}{q_j}\right) = \prod_{j=1}^{s}(-1)^{(q_j-1)/2} = (-1)^{\sum_{j=1}^{s}(q_j-1)/2}$$

If a and b are odd, then

$$\frac{ab-1}{2} - \left(\frac{a-1}{2} + \frac{b-1}{2}\right) - \frac{(a-1)(b-1)}{2} \equiv 0 \pmod 2$$

and hence

$$\frac{a-1}{2} + \frac{b-1}{2} \equiv \frac{ab-1}{2} \pmod 2.$$

Applying this repeatedly we obtain

$$\sum_{j=1}^{s}\frac{q_j-1}{2} \equiv \frac{1}{2}\left(\prod_{j=1}^{s} q_j - 1\right) \equiv \frac{Q-1}{2} \pmod 2 \qquad (3.1)$$

and thus $\left(\frac{-1}{Q}\right) = (-1)^{(Q-1)/2}$.

Similarly, if a and b are odd, then

$$\frac{a^2b^2-1}{8}-\left(\frac{a^2-1}{8}+\frac{b^2-1}{8}\right)=\frac{(a^2-1)(b^2-1)}{8}\equiv 0\,(\mathrm{mod}\,8)$$

so we have

$$\frac{a^2-1}{8}+\frac{b^2-1}{8}\equiv\frac{a^2b^2-1}{8}\,(\mathrm{mod}\,2),$$

$$\sum_{j=1}^{s}\frac{q_j^2-1}{8}\equiv\frac{Q^2-1}{8}\,(\mathrm{mod}\,2)$$

and hence,

$$\left(\frac{2}{Q}\right)=\prod_{j=1}^{s}\left(\frac{2}{q_j}\right)=(-1)^{\sum_{j=1}^{s}(q_j^2-1)/8}=(-1)^{(Q^2-1)/8}.$$

Theorem

If P and Q are odd and positive and if $(P, Q) = 1$, then

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{\{(P-1)/2\}\{(Q-1)/2\}}.$$

Proof Writing $P = \prod_{i=1}^{r} p_i$ as well as $Q = \prod_{j=1}^{s} q_j$, we have

$$\left(\frac{P}{Q}\right) = \prod_{j=1}^{s}\left(\frac{P}{q_j}\right) = \prod_{j=1}^{s}\prod_{i=1}^{r}\left(\frac{p_i}{q_j}\right) = \prod_{j=1}^{s}\prod_{i=1}^{r}\left(\frac{q_j}{p_i}\right)(-1)^{\{(p_i-1)/2\}\{(q_j-1)/2\}}$$

$$= \left(\frac{Q}{P}\right)(-1)^{\sum_{j=1}^{s}\sum_{i=1}^{r}\{(p_i-1)/2\}\{(q_j-1)/2\}}$$

where we have used Theorem 3.4. But

$$\sum_{j=1}^{s}\sum_{i=1}^{r}\frac{p_i-1}{2}\frac{q_j-1}{2} = \sum_{i=1}^{r}\frac{p_i-1}{2}\sum_{j=1}^{s}\frac{q_j-1}{2}$$

and

$$\sum_{i=1}^{r}\frac{p_i-1}{2} \equiv \frac{P-1}{2}, \qquad \sum_{j=1}^{s}\frac{q_j-1}{2} \equiv \frac{Q-1}{2} \pmod 2$$

as in (3.1) in the proof of Theorem 3.7. Therefore we have

$$\left(\frac{P}{Q}\right) = \left(\frac{Q}{P}\right)(-1)^{\{(P-1)/2\}\{(Q-1)/2\}}$$

which proves the theorem.

BINARY QUADRATIC FORMS

A monomial $ax_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}$ in n variables with coefficient $a \neq 0$ is said to have degree $k_1 + k_2 + \cdots + k_n$. The degree of a polynomial in n variables is the maximum of the degrees of the monomial terms in the polynomial. A polynomial in several variables is called a *form*, or is said to be *homogeneous* if all its monomial terms have the same degree. A form of degree 2 is called a *quadratic* form. Thus the general quadratic form is a sum of the shape

$$\sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}x_i x_j.$$

A form in two variables is called *binary*. The remainder of this chapter is devoted to the study of binary quadratic forms

$$f(x, y) = ax^2 + bxy + cy^2$$

Theorem

Let $f(x, y) = ax^2 + bxy + cy^2$ be a binary quadratic form with integral coefficients and discriminant d. If $d \neq 0$ and d is not a perfect square, then $a \neq 0$, $c \neq 0$, and the only solution of the equation $f(x, y) = 0$ in integers is given by $x = y = 0$.

Proof We may presume that $a \neq 0$ and $c \neq 0$, for if $a = 0$ or $c = 0$ then $ac = 0$ and $d = b^2 - 4ac = b^2$, a perfect square. Suppose that x_0 and y_0 are integers such that $f(x_0, y_0) = 0$. If $y_0 = 0$ then $ax_0^2 = 0$, and hence $x_0 = 0$ because $a \neq 0$. If $x_0 = 0$, a parallel argument gives $y_0 = 0$. Consequently we take $x_0 \neq 0$ and $y_0 \neq 0$. By completing the square we see that

$$4af(x, y) = (2ax + by)^2 - dy^2 \qquad (3.3)$$

and hence $(2ax_0 + by_0)^2 = dy_0^2$ since $f(x_0, y_0) = 0$. But $dy_0^2 \neq 0$, and it follows by unique factorization that d is a perfect square. The proof is now complete.

Definition 3.5 *A form $f(x, y)$ is called* indefinite *if it takes on both positive and negative values. The form is called* positive semidefinite (*or* negative semidefinite) *if $f(x, y) \geqslant 0$ (or $f(x, y) \leqslant 0$) for all integers x, y. A semidefinite form is called* definite *if in addition the only integers x, y for which $f(x, y) = 0$ are $x = 0,\ y = 0$.*

Theorem

Let d be a given integer. There exists at least one binary quadratic form with integral coefficients and discriminant d, if and only if $d \equiv 0$ or $1 \pmod 4$.

Proof Since $b^2 \equiv 0$ or $1 \pmod 4$ for any integer b, it follows that the discriminant $d = b^2 - 4ac \equiv 0$ or $1 \pmod 4$. For the converse, suppose first that $d \equiv 0 \pmod 4$. Then the form $x^2 - (d/4)y^2$ has discriminant d. Similarly, if $d \equiv 1 \pmod 4$ then the form $x^2 + xy - \left(\frac{d-1}{4}\right)y^2$ has discriminant d, and the proof is complete.

Theorem

Let n and d be given integers with $n \neq 0$. There exists a

binary quadratic form of discriminant d that represents n properly if and only if the congruence $x^2 \equiv d \pmod{4|n|}$ has a solution.

Proof Suppose that b is a solution of the congruence, with $b^2 - d = 4nc$, say. Then the form $f(x, y) = nx^2 + bxy + cy^2$ has integral coefficients and discriminant d. Moreover, $f(1, 0) = n$ is a proper representation of n.

Conversely, suppose we have a proper representation $f(x_0, y_0)$ of n by a form $f(x, y) = ax^2 + bxy + cy^2 = n$ with discriminant $b^2 - 4ac = d$. Since g.c.d.$(x_0, y_0) = 1$, we can choose integers m_1, m_2 such that $m_1 m_2 = 4|n|$, g.c.d.$(m_1, y_0) = 1$ and g.c.d.$(m_2, x_0) = 1$. For example, take m_1 to be the product of those prime-power factors p^α of $4n$ for which $p|x_0$, and then put $m_2 = 4|n|/m_1$. From equation (3.3) we see that $4an = (2ax_0 + by_0)^2 - dy_0^2$, and hence $(2ax_0 + by_0)^2 \equiv dy_0^2 \pmod{m_1}$. As $(y_0, m_1) = 1$, there is an integer $\overline{y_0}$ such that $y_0\overline{y_0} \equiv 1 \pmod{m_1}$, and we find that the congruence $u^2 \equiv d \pmod{m_1}$ has a solution, namely $u = u_1 = (2ax_0 + by_0)\overline{y_0}$. We interchange a and c, and also x and y, to see that the parallel congruence $u^2 \equiv d \pmod{m_2}$ also has a solution, say $u = u_2$. Then by the Chinese remainder theorem we find an integer w such that $w \equiv u_1 \pmod{m_1}$ and $w \equiv u_2 \pmod{m_2}$. Thus $w^2 \equiv u_1^2 \equiv d \pmod{m_1}$, and similarly $w^2 \equiv u_2^2 \equiv d \pmod{m_2}$, from which we get $w^2 \equiv d \pmod{m_1 m_2}$. But this last modulus is $4|n|$, so the theorem is proved.

Corollary

Suppose that $d \equiv 0$ or $1 \pmod 4$. If p is an odd prime, then

there is a binary quadratic form of discriminant d that represents p, if and only if $\left(\frac{d}{p}\right) = 1$.

Proof Any representation of p must be proper. Hence if p is represented, then it is properly represented, and thus (by the theorem) d must be a square modulo $4p$, so that $\left(\frac{d}{p}\right) = 1$. Conversely, if $\left(\frac{d}{p}\right) = 1$, then d is a square modulo p. By hypothesis, d is a square modulo 4. Since p is odd, it follows by the Chinese remainder theorem that d is a square modulo $4p$, and hence (by the theorem) p is properly represented by some form of discriminant d, thus completing the proof.

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 $n = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$, then
$$\phi(n) = (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1})\ldots(p_r^{k_r} - p_r^{k_r-1})$$
$$= n(1-1/p_1)(1-1/p_2)\ldots(1-1/p_r).$$
8. Let $n > 1$ and $\gcd(a,n) = 1$. If $a_1, a_2, \ldots, a_{\phi(n)}$ are the positive integer 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.
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-V

SYLLABUS

Greatest Integer Function - Arithmetic Functions - The Mobius Inversion Formula - Recurrence Functions - Combinatorial Number Theory

GREATEST INTEGER FUNCTION

The function $[x]$ was introduced in Section 1.2, and again in Definition 3.3 in Section 3.1. It is defined for all real x and it assumes integral values only. Indeed, $[x]$ is the unique integer such that $[x] \leqslant x < [x] + 1$. For brevity it is useful to put $\{x\} = x - [x]$. This is known as the *fractional part of* x. Many of the basic properties of the function $[x]$ are included in the following theorem.

Theorem 4.1 *Let x and y be real numbers. Then we have*

(1) $[x] \leqslant x < [x] + 1,\ x - 1 < [x] \leqslant x,\ 0 \leqslant x - [x] < 1.$

(2) $[x] = \sum_{1 \leqslant i \leqslant x} 1$ *if* $x \geqslant 0$.

(3) $[x + m] = [x] + m$ *if m is an integer*.

(4) $[x] + [y] \leqslant [x + y] \leqslant [x] + [y] + 1.$

(5) $[x] + [-x] = \begin{cases} 0 \text{ if } x \text{ is an integer}, \\ -1 \text{ otherwise}. \end{cases}$

(6) $\left[\frac{[x]}{m}\right] = \left[\frac{x}{m}\right]$ *if m is a positive integer*.

(7) $-[-x]$ *is the least integer* $\geqslant x$.

(8) $[x + \frac{1}{2}]$ *is the nearest integer to x. If two integers are equally near to x, it is the larger of the two.*

(9) $-[-x + \frac{1}{2}]$ *is the nearest integer to x. If two integers are equally near to x, it is the smaller of the two.*

(10) If n and a are positive integers, $[n/a]$ is the number of integers among $1, 2, 3, \cdots, n$ that are divisible by a.

Proof The first part of (1) is just the definition of $[x]$ in algebraic form. The two other parts are rearrangements of the first part.

In (2) the sum is vacuous if $x < 1$. We adopt the standard convention that a vacuous sum is zero. Then, for $x \geqslant 0$, the sum counts the number of positive integers i that are less than or equal to x. This number is evidently just $[x]$.

Part (3) is obvious from the definition of $[x]$.

To prove (4) we write $x = n + \nu$, $y = m + \mu$, where n and m are integers and $0 \leqslant \nu < 1$, $0 \leqslant \mu < 1$. Then

$$[x] + [y] = n + m \leqslant [n + \nu + m + \mu] = [x + y]$$

$$= n + m + [\nu + \mu] \leqslant n + m + 1 = [x] + [y] + 1.$$

Again writing $x = n + \nu$, we also have $-x = n - 1 + 1 - \nu$, $0 < 1 - \nu \leqslant 1$. Then

$$[x] + [-x] = n + [-n - 1 + 1 - \nu]$$

$$= n - n - 1 + [1 - \nu] = \begin{cases} 0 & \text{if } \nu = 0 \\ -1 & \text{if } \nu > 0 \end{cases}$$

and we have (5).

To prove (6) we write $x = n + \nu$, $n = qm + r$, $0 \leqslant \nu < 1$, $0 \leqslant r \leqslant m - 1$, and have

$$\left[\frac{x}{m}\right] = \left[\frac{qm + r + \nu}{m}\right] = q + \left[\frac{r + \nu}{m}\right] = q$$

since $0 \leqslant r + \nu < m$. Then (6) follows because

$$\left[\frac{[x]}{m}\right] = \left[\frac{n}{m}\right] = \left[q + \frac{r}{m}\right] = q.$$

Replacing x by $-x$ in (1) we get $-x - 1 < [-x] \leqslant -x$ and hence $x \leqslant -[-x] < x + 1$, which proves (7).

To prove (8) we let n be the nearest integer to x, taking the larger one if two are equally distant. Then $n = x + \theta$, $-\frac{1}{2} < \theta \leqslant \frac{1}{2}$, and $[x + \frac{1}{2}] = n + [-\theta + \frac{1}{2}] = n$, since $0 \leqslant -\theta + \frac{1}{2} < 1$.

The proof of (9) is similar to that of (8).

To prove part (10) we note that if $a, 2a, 3a, \cdots, ja$ are all the positive integers $\leqslant n$ that are divisible by a, then we must prove that $[n/a] = j$. But we see that $(j + 1)a$ exceeds n, so

$$ja \leqslant n < (j+1)a, \qquad j \leqslant n/a < j+1; \qquad [n/a] = j.$$

ARITHMETIC FUNCTIONS

Definition 4.1 *For positive integers n we make the following definitions.*

$d(n)$ *is the number of positive divisors of* n.
$\sigma(n)$ *is the sum of the positive divisors of* n.
$\sigma_k(n)$ *is the sum of the kth powers of the positive divisors of* n.
$\omega(n)$ *is the number of distinct primes dividing* n.
$\Omega(n)$ *is the number of primes dividing n, counting multiplicity.*

For example, $d(12) = 6$, $\sigma(12) = 28$, $\sigma_2(12) = 210$, $\omega(12) = 2$, and $\Omega(12) = 3$. These are all arithmetic functions. The value of k can be any real number, positive, negative, or zero. Complex values of k are useful in more advanced investigations. The *divisor function* $d(n)$ is a special case, since $d(n) = \sigma_0(n)$. Similarly, $\sigma(n) = \sigma_1(n)$. It is convenient to use the symbols $\sum_{d|n} f(d)$ and $\prod_{d|n} f(d)$ for the sum and product of $f(d)$ over all positive divisors d of n. Thus we write

$$d(n) = \sum_{d|n} 1, \qquad \sigma(n) = \sum_{d|n} d, \qquad \sigma_k(n) = \sum_{d|n} d^k,$$

and similarly

$$\omega(n) = \sum_{p|n} 1, \qquad \Omega(n) = \sum_{p^\alpha \| n} \alpha = \sum_{p^\beta | n} 1.$$

In the formulae for $\Omega(n)$, the first sum is extended over all prime powers p^α that exactly divide n, while the second sum is over all prime powers p^β dividing n.

Theorem

For each positive integer n, $d(n) = \prod_{p^\alpha \| n} (\alpha + 1)$.

In this notation, $\alpha = \alpha(p)$ depends on the prime being considered, and on n. Those primes p not dividing n may be ignored, since $\alpha = 0$ for such primes, and the factor contributed by such p is 1. If $n = 1$ then this is the case for all p, and we see that this formula gives $d(1) = 1$.

Proof Let $n = \prod p^{\alpha}$ be the canonical factorization of n. A positive integer $d = \prod p^{\beta}$ divides n if and only if $0 \leqslant \beta(p) \leqslant \alpha(p)$ for all prime numbers p. Since $\beta(p)$ may take on any one of the values $0, 1, \cdots, \alpha(p)$, there are $\alpha(p) + 1$ possible values for $\beta(p)$, and hence the number of divisors is $\prod_{p^{\alpha} \| n}(\alpha + 1)$.

From Theorem 4.3 it follows that if $(m, n) = 1$ then $d(mn) = d(m)d(n)$.

Definition 4.2 *If $f(n)$ is an arithmetic function not identically zero such that $f(mn) = f(m)f(n)$ for every pair of positive integers m, n satisfying $(m, n) = 1$, then $f(n)$ is said to be* multiplicative. *If $f(mn) = f(m)f(n)$ whether m and n are relatively prime or not, then $f(n)$ is said to be* totally multiplicative *or* completely multiplicative.

If f is a multiplicative function, $f(n) = f(n)f(1)$ for every positive integer n, and since there is an n for which $f(n) \neq 0$, we see that $f(1) = 1$.

From the definition of a multiplicative function f it follows by mathematical induction that if $m_1, m_2, \cdots, m_r$ are positive integers are relatively prime in pairs, then

$$f(m_1 m_2 \cdots m_r) = f(m_1)f(m_2) \cdots f(m_r).$$

Theorem 4.4 *Let $f(n)$ be a multiplicative function and let $F(n) = \sum_{d|n} f(d)$. Then $F(n)$ is multiplicative.*

Proof Suppose that $m = m_1 m_2$ with $(m_1, m_2) = 1$. If $d|m$, then we set $d_1 = (d, m_1)$ and $d_2 = (d, m_2)$. Thus $d = d_1 d_2$, $d_1|m_1$, and $d_2|m_2$. Conversely, if a pair d_1, d_2 of divisors of m_1 and m_2 are given, then $d = d_1 d_2$ is a divisor of m, and $d_1 = (d, m_1)$, $d_2 = (d, m_2)$. Thus we have established a one-to-one correspondence between the positive divisors d of m and pairs d_1, d_2 of positive divisors of m_1 and m_2. Hence

$$F(m) = \sum_{d|m} f(d) = \sum_{d_1|m_1} \sum_{d_2|m_2} f(d_1 d_2)$$

for any arithmetic function f. Since $(d_1, d_2) = 1$, it follows from the hypothesis that f is multiplicative that the right side is

$$\sum_{d_1|m_1} \sum_{d_2|m_2} f(d_1) f(d_2) = \left(\sum_{d_1|m_1} f(d_1) \right) \left(\sum_{d_2|m_2} f(d_2) \right) = F(m_1) F(m_2).$$

We could have used this theorem and Definition 4.1 to prove that $d(n)$ is multiplicative. Since $d(n) = \sum_{d|n} 1$ is of the form $\sum_{d|n} f(d)$, and since the function $f(n) = 1$ is multiplicative, Theorem 4.4 applies, and we see that $d(n)$ is multiplicative. Then Theorem 4.3 would have been easy to prove. If p is a prime, then $d(p^\alpha) = \alpha + 1$, since p^α has the $\alpha + 1$ positive divisors $1, p, p^2, \cdots, p^\alpha$ and no more. Then, since $d(n)$ is multiplicative,

$$d\left(\prod_{p^\alpha \| n} p^\alpha \right) = \prod_{p^\alpha \| n} d(p^\alpha) = \prod_{p^\alpha \| n} (\alpha + 1).$$

Theorem 4.5 *For every positive integer* n, $\sigma(n) = \prod_{p^\alpha \| n} \left(\frac{p^{\alpha+1} - 1}{p - 1} \right)$.

In case $n = 1$, $\alpha = 0$ for all primes p, so that each factor in the product is 1, and the formula gives $\sigma(1) = 1$.

Proof By definition $\sigma(n) = \sum_{d|n} d$, so we can apply Theorem 4.4 with $f(n) = n$, $F(n) = \sigma(n)$. Thus $\sigma(n)$ is multiplicative and $\sigma(n) = \prod \sigma(p^\alpha)$. But the positive divisors of p^α are just $1, p, p^2, \cdots, p^\alpha$ whose sum is $(p^{\alpha+1} - 1)/(p - 1)$.

THE MOBIUS INVERSION FORMULA

Definition 4.3 *For positive integers* n *put* $\mu(n) = (-1)^{\omega(n)}$ *if* n *is square free, and set* $\mu(n) = 0$ *otherwise. Then* $\mu(n)$ *is the* Möbius mu function.

Theorem 4.7 *The function* $\mu(n)$ *is multiplicative and*

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

Proof It is clear from the definition that $\mu(n)$ is multiplicative. If $F(n) = \sum_{d|n} \mu(d)$, then $F(n)$ is multiplicative by Theorem 4.4. Clearly

$F(1) = \mu(1) = 1$. If $n > 1$, then $\alpha > 0$ for some prime p, and in this case $F(p^\alpha) = \sum_{\beta=0}^{\alpha} \mu(p^\beta) = 1 + (-1) = 0$, and we have the desired result.

Theorem 4.8 *Möbius inversion formula. If* $F(n) = \sum_{d|n} f(d)$ *for every positive integer* n, *then* $f(n) = \sum_{d|n} \mu(d)F(n/d)$.

Proof We see that

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

$$= \sum_{dk|n} \mu(d) f(k)$$

where the last sum is to be taken over all ordered pairs (d, k) such that $dk|n$. This last formulation suggests that we can reverse the roles of d and k to write the sum in the form

$$\sum_{k|n} f(k) \sum_{d|(n/k)} \mu(d)$$

and this is $f(n)$ by Theorem 4.7.

Theorem 4.9 *If* $f(n) = \sum_{d|n} \mu(d)F(n/d)$ *for every positive integer* n, *then* $F(n) = \sum_{d|n} f(d)$.

Proof First we write

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

As k runs through the divisors of d, so does d/k, and hence this sum can be written as

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

In this double sum, $F(k)$ appears for every possible divisor k of n. For each fixed divisor k of n, we collect all the terms involving $F(k)$. The

coefficient is the set of all $\mu(d/k)$, where d/k is a divisor of n/k or, more simply, the set of all $\mu(r)$, where r is a divisor of n/k. It follows that the last sum can be rewritten as

$$\sum_{k|n} \sum_{r|(n/k)} \mu(r) F(k).$$

By Theorem 4.7, we see that the coefficient of $F(k)$ here is zero unless $n/k = 1$, so the entire sum reduces to $F(n)$.

It should be noted that Theorem 4.8 and its converse, Theorem 4.9, do not require that $f(n)$ or $F(n)$ be multiplicative.

On inserting the identity of Theorem 4.6 in the inversion formula of Theorem 4.8, we find that

$$\phi(n) = n \sum_{d|n} \mu(d)/d. \tag{4.1}$$

Here the summand is multiplicative, so that by Theory 4.4 we see once more that $\phi(n)$ is multiplicative. Indeed, if n is a prime power, say $n = p^\alpha$, then

$$\sum_{d|p^\alpha} \mu(d)/d = \sum_{\beta=0}^{\alpha} \mu(p^\beta)/p^\beta = 1 - 1/p.$$

This, with (4.1), gives again the formula for $\phi(n)$ in Theorem 2.15.

Theorem 4.6 *For every positive integer n,* $\sum_{d|n} \phi(d) = n$.

Proof Let $F(n)$ denote the sum on the left side of the proposed identity. From Theorem 2.19 we see that $\phi(n)$ is multiplicative. Thus $F(n)$ is multiplicative, by Theorem 4.4. Since the right side, n, is also a multiplicative function, to establish that $F(n) = n$ for all n it suffices to prove that $F(p^\alpha) = p^\alpha$ for all prime powers p^α. From Theorem 2.15 we see that if $\beta > 0$ then $\phi(p^\beta) = p^\beta - p^{\beta-1}$. Thus

$$F(p^\alpha) = \sum_{d|p^\alpha} \phi(d) = \sum_{\beta=0}^{\alpha} \phi(p^\beta) = 1 + \sum_{\beta=1}^{\alpha} p^\beta - p^{\beta-1} = p^\alpha.$$

Theorem 4.6 can be proved combinatorially, as follows. Let n be given, and put $\mathscr{S} = \{1, 2, \cdots, n\}$. For each divisor d of n, let $\mathscr{S}_d$ be the subset of those members $k \in \mathscr{S}$ for which $(k, n) = d$. Clearly each member of $\mathscr{S}$ lies in exactly one of the subsets $\mathscr{S}_d$. (In such a situation we say that the subsets *partition* the set.) We note that $k \in \mathscr{S}_d$ if and only if k is of the form $k = jd$ where $(j, n/d) = 1$ and $1 \leqslant j \leqslant n/d$. Thus by Theorem 2.5 we deduce that $\mathscr{S}_d$ contains precisely $\phi(n/d)$ numbers. Since $\mathscr{S}$ contains exactly n numbers, it is now evident that $n = \sum_{d|n} \phi(n/d)$. This is an alternative formulation of the stated identity.

COMBINATORIAL NUMBER THEORY

PIGEONHOLE PRINCIPLE

In this section, we treat a few elementary combinatorial problems of number theory, especially those that can be solved by the use of two simple ideas. First, if n sets contain $n + 1$ or more distinct elements in all, at least one of the sets contains two or more elements. This is sometimes familiarly called the *pigeonhole principle*, the idea being that if one places $n + 1$ letters in n slots (called "pigeonholes") then there is a pigeonhole containing more than one letter. The second idea is the one-to-one correspondence procedure, used to pair off elements in a finite set or between two sets to determine the number of elements or to prove the existence of an element of a specified kind.

Example 1 Given any $m + 1$ integers, prove that two can be selected whose difference is divisible by m.

Since there are m residue classes modulo m, two of the integers must be in the same class, and so m is a divisor of their difference.

In this and most other problems in this section, the statement is the best possible of its kind. In Example 1, we could not replace the opening phrase by "Given any m integers," because the integers $1, 2, 3, \cdots, m$ do not have the property that two can be selected whose difference is divisible by m.

Example 2 Given any m integers $a_1, a_2, \cdots, a_m$, prove that a nonempty subset of these can be selected whose sum is a multiple of m.

Solution Consider the $m + 1$ integers

$$0, a_1, a_1 + a_2, a_1 + a_2 + a_3, \cdots, a_1 + a_2 + a_3 + \cdots + a_m$$

consisting of zero and the sums of special subsets of the integers. By Example 1, two of these $m + 1$ integers have a difference that is a multiple of m, and the problem is solved.

Example 3 Let $\mathscr{S}$ be a set of k integers. If $m > 1$ and $2^k > m + 1$, prove that there are two distinct nonempty subsets of $\mathscr{S}$, the sums of whose elements are congruent modulo m. Prove that the conclusion is false if $2^k = m + 1$.

Solution The set $\mathscr{S}$, containing k elements, has 2^k subsets in all, but only $2^k - 1$ nonempty subsets. For each of these nonempty subsets, consider the sum of the elements, so that there are $2^k - 1$ of these sums. Since $2^k - 1 > m$, two of these sums are in the same residue class modulo m, and so are congruent (mod m).

In case $2^k = m + 1$, define $\mathscr{S}$ as the set $\{1, 2, 4, 8, \cdots, 2^{k-1}\}$, with k elements each of a power of 2. It is not difficult to see that the sums of the nonempty subsets of $\mathscr{S}$ are precisely the natural numbers $1, 2, 3, \cdots, 2^k - 1$, each occurring once. One way to see this is to observe that the elements of $\mathscr{S}$, when written to base 2, can be expressed in the form $1, 10, 100, 1000, \cdots, 10^{k-1}$. The sums of the nonempty subsets are then all the integers, in base 2,

$$1, 10, 11, 100, 101, 111, \cdots, 111 \cdots 111$$

where the last integer here contains k digits 1 in a row.

Example 4 If $\mathscr{S}$ is any set of $n + 1$ integers selected from $1, 2, 3, \cdots, 2n$, prove that there are two relatively prime integers in $\mathscr{S}$.

Solution The set $\mathscr{S}$ must contain one of the pairs of consecutive integers 1, 2 or 3, 4 or 5, 6 or $\cdots$ or $2n - 1, 2n$.

Example 5 Find the number of integers in the set $\mathscr{S} = \{1, 2, 3, \cdots, 6300\}$ that are divisible by neither 3 nor 4; also the number divisible by none of 3, 4, or 5.

Solution Of the 6300 integers in $\mathscr{S}$, exactly 2100 are divisible by 3, and 1575 are divisible by 4. The subtraction $6300 - 2100 - 1575$ does not give the correct answer to the first part of the problem, because the sets removed by subtraction are not disjoint. Those integers divisible by 12 have been removed twice. There are 525 such integers, so the answer to the first part of the problem is

$$6300 - 2100 - 1575 + 525 = 3150.$$

Turning to the second part of the problem, we begin by removing from the set $\mathscr{S}$ those integers divisible by 3, in number 2100, those divisible by 4, in number 1575, and those divisible by 5, in number 1260. So we see that

$$6300 - 2100 - 1575 - 1260$$

is a start toward the answer. However, integers divisible by both 3 and 4 have been removed twice; likewise, those divisible by both 3 and 5 and those divisible by both 4 and 5. Hence, we add back in 6300/12 or 525 of the first type, 6300/15 or 420 of the second type, and 6300/20 or 315 of the third type to give

$$6300 - 2100 - 1575 - 1260 + 525 + 420 + 315.$$

This is still not the final answer, because one more adjustment must be made, for the integers $50, 120, 180, \cdots$ that are divisible by 3, 4, and 5. Such integers are counted once in each term of the expression above, and so the net count for each such integer is 1. There are 6300/60 or 105 such integers, so if we subtract this number we get the correct answer,

$$6300 - 2100 - 1575 - 1260 + 525 + 420 + 315 - 105 = 2520.$$

The Inclusion-Exclusion Principle Example 5 illustrates a basic combinatorial argument as follows: Consider a collection of N objects of which $N(\alpha)$ have a certain property α, $N(\beta)$ have property β, and $N(\gamma)$ have property γ. Similarly, let $N(\alpha, \beta)$ be the number having both properties α and β, and $N(\alpha, \beta, \gamma)$ be the number having properties α, β, and γ. Then the number of objects in the collection having none of the properties α, β, γ is

$$N - N(\alpha) - N(\beta) - N(\gamma) + N(\alpha, \beta) + N(\alpha, \gamma) + N(\beta, \gamma) - N(\alpha, \beta, \gamma) \qquad (4.15)$$

This is the inclusion-exclusion principle in the case of three properties.

The proof of (4.15) can be given along the same lines as in Example 5: First, that an object having exactly one of the properties, say β, is counted once by N and once by $N(\beta)$ for a net count of $1 - 1$ or 0; that an object having exactly two of the properties has a net count of $1 - 1 - 1 + 1$, again 0; next, that an object with all three properties has a net count of $1 - 1 - 1 - 1 + 1 + 1 + 1 - 1$, again 0. On the other hand, an object having none of the properties is counted by N once in (4.15), and so a net count of 1.

The extension of (4.15) to a collection of N objects having (variously) k properties is very natural. Where (4.15) has three terms of the type $N(\alpha)$, the general formula has k such terms; where (4.15) has three terms of the type $N(\alpha, \beta)$, the general formula has $k(k - 1)/2$ such terms; and so on.

It may be noted that the inclusion-exclusion principle can be used to give an entirely different proof of the formula for the evaluation of the Euler function $\phi(n)$, as set forth in Theorem 2.15. Because that result has been proved in full detail already, we make the argument in the case of an

integer n having exactly three distinct prime factors, say p, q, and r. The problem is to determine the number of integers in the set $\mathscr{S} = \{1, 2, 3, \cdots, n\}$ having no prime factor in common with n. Let an integer in the set $\mathscr{S}$ have property α if it is divisible by p, property β if it is divisible by q and property γ if it is divisible by r. A direct application of (4.15) gives

$$n - n/p - n/q - n/r + n/pq + n/pr + n/qr - n/pqr$$
$$= n(1 - 1/p)(1 - 1/q)(1 - 1/r)$$

as the number of integers in the set $\mathscr{S}$ divisible by none of p, q, or r.

POSSIBLE QUESTIONS

2 Mark Questions:

1. Evaluate the Legendre symbol $(71/73)$.
2. Evaluate the Legendre symbol $(-219/383)$.
3. Solve the congruence $x^2 \equiv 31 (\text{mod } 11^4)$.
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
$$x^2 \equiv a (\text{mod } p^n), \qquad n \geq 1$$
has a solution if and only if $(a/p) = 1$.
3. Let a be an odd integer. then prove
   (i) $x^2 \equiv a (\text{mod } 2)$ always has a solution.
   (ii) $x^2 \equiv a (\text{mod } 4)$ has a solution if and only if $a \equiv 1 (\text{mod } 4)$.
   (iii) $x^2 \equiv a (\text{mod } 2^n)$, for $n \geq 3,$ has a solution if and only if $a \equiv 1 (\text{mod } 8)$.
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 $s \not\equiv t \pmod 2$.

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.

Reg no----------

(18MMP302)

KARPAGAM ACADEMY OF HIGHER EDUCATION

Coimbatore-21

DEPARTMENT OF MATHEMATICS

Third Semester

I Internal Test – Aug 2019

Number Theory

Date: -08-2019 Time: 2 Hours

Class: II-M. Sc. Mathematics Maximum Marks:50

PART-A(20X1=20 Marks)

Answer all the Questions:

1. If a divides b and b divides c then _____

   (a) a=c (b) a divides c (c) c divides a (d) a not equal to c

2. Suppose d divides a and d divides b then d is _____

   (a)Factor (b) any integer (c) common divisor (d) 1

3. If (a, b)=1then _____

   (a) ax+by=1 (b) ax+by=a (c) ax+by=b (d) ax+by=c

4. How many prime numbers are less than 50 ?

   (a) 16 (b)15 (c) 14 (d) 18

5. If a and b are relatively prime then (a, b) = _____

   (a) 1 (b) a (c) b (d) ab

6. Any positive integer n can be written in the form_____

(a) $p_1^{r_1}.p_2^{r_2}.p_3^{r_3}...p_n^{r_n}$. (b) $p_1.p_2.p_3...p_n$.

(c) $p_1^{r_1}.p_2^{r_2}.p_3^{r_3}...$ (d) $p_1.p_2.p_3...$

7. If a divides b then _____

   (a) b=ac (b) a=bc (c)a=b (d) a>b

8. a and b are co prime if _____

   (a) gcd (a, b) = 1 (b) gcd (a, b) = gcd (b, a)

   (c) gcd (a, b) = d (d) gcd(b, a) = d

9. In Fermat's little theorem $a^{p-1} \equiv 1 (\text{mod } p)$ if _____

   (a) (a, p) = a (b) (p, a) = p (c) (a, p) = p (d) (p, a) = 1

10. The equation $ax \equiv b (\text{mod } n)$ has a solution if _____

    (a) gcd (a, n) divides b (b) gcd (a, b) divides n

    (c) gcd (b, n) divides a (d) gcd (a, x) divides b

11. $(n-1)! \equiv -1 (\text{mod } n)$ is valid only if_____

    (a) n is positive (b) n is prime (c) n is composite (d) n>2

12. Gcd (a, b)=d then (a/d, b/d)=_____

    (a) a (b) b (c) 1 (d) d

13. The arithmetic progression a, a+b, a+2b, … contains infinitely many primes if _____

    (a) a and b are positive co prime (b) a and b are co prime

    (c) negative co prime (d) a=b

14. $p \equiv$ _____$-1 (\text{mod } p)$.

    (a) 0 (b) p (c) p-1 (d) 1

15. _____ is the remainder when 8.8.8….(30 times) divided by 31.

    (a) 0 (b) 1 (c) -1 (d) 30

16. The number 1729 is called _____

    (a) pseudo prime (b) prime

    (c) composite (d) special prime

17. The quadratic congruence $x^2 \equiv -1 (\text{mod } p)$, p is a prime, has a solution if _____

(a) $p \equiv 1 (\text{mod } 4)$ (b) $p \equiv -1 (\text{mod } 4)$

(c) $p \equiv 1 (\text{mod } p)$ (d) $p \equiv -1 (\text{mod } p)$

18. The Euler phi function $\phi(p)$ = _____ for any prime p.

(a) p (b) $p+1$ (c) $p-1$ (d) p^2

19. The integer 701 is _____

(a) composite (b) prime

(c) special prime (d) either prime or composite

20. _____ are all primes is of the form of 4n+3

(a) 2, 3 and 5 (b) 7, 11, 19 (c) 7, 11, 15 (d) 7, 11, 17

PART-B (3X2=6 Marks)

Answer all the Questions:

21. Define primitive root.
22. State Wilson's theorem.
23. Define Legendre symbol.

PART-C (3X8=24 Marks)

Answer all the Questions:

24. (a) State and prove division algorithm.

(OR)

(b) Using Euclidean algorithm and find the greatest common divisor g of 1819 and 3587, and then find integers x and y to satisfy $1819x + 3587y = g$.

25. (a) Prove that the following statements

i. $ax \equiv ay (mod\ m)$ if and only if $x \equiv y\ (mod \frac{m}{(a,b)})$.

ii. If $ax \equiv ay (mod\ m)$ and $(a, m) = 1$, then $x \equiv y\ (mod\ m)$.

iii. $x \equiv y\ (mod\ m_i)$ for $i = 1,2, \dots, r$ if and only if $x \equiv y\ (mod [m_1, m_2, \dots, m_r])$.

(OR)

(b) Prove that the congruence $f(x) \equiv 0 (mod\ p)$ of degree n has at most n solutions.

26. (a) State and prove binomial theorem.

(OR)

(b) State and prove Euler's generalization theorem.

Reg no----------

(18MMU302)

KARPAGAM ACADEMY OF HIGHER EDUCATION

Coimbatore-21

DEPARTMENT OF MATHEMATICS

Third Semester

II Internal Test – Oct'19

Number Theory

Date: -10-2019 **Time: 2 Hours**

Class: II-M. Sc. Mathematics **Maximum Marks:50**

PART-A(20X1=20 Marks)

Answer all the Questions:

1. $\lim_{n\to\infty}\sigma(n) =$ _____

   (a) 0 (b) 1 (c) ∞ (d) not defined

2. The number of divisor function is _____

   (a) Regular (b) irregular

   (c) real valued function (d) onto

3. The order of 2 modulo7 is _____

   (a) 2 (b) 7 (c) 3 (d) 6

4. If $a^k \equiv 1(\text{mod } n)$ and $a \equiv b(\text{mod } n)$ then _____

   (a) k is the order of n (b) n is order of k

   (c) b has order k (d) a has order n

5. For the Legendre symbol, $\left(\frac{ab}{p}\right) =$ _____

   (a) 1 (b) $\left(\frac{a}{p}\right)$ (c) $\left(\frac{ab}{p^2}\right)$ (d) $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

6. If p is odd prime then _____

   (a) $\sum_{n=1}^{p-1}\left(\frac{n}{p}\right)=1$ (b) $\sum_{n=1}^{p-1}\left(\frac{n}{p}\right)=0$ (c) $\sum_{n=1}^{p-1}\left(\frac{a}{p}\right)=1$ (d) $\sum_{n=1}^{p-1}\left(\frac{a}{p}\right)=0$

7. $\phi(p^{k+1}) =$ _____ is the property of Euler phi function.

   (a) $p-1$ (b) p (c) $p\phi(p^k)$ (d) p^k

8. The value of $\sigma(15) =$ _____

   (a) 4 (b) 24 (c) 6 (d) 39

9. $a^k \equiv 1(\text{mod } n)$ and a and b has same order if _____

   (a) $a \equiv b(\text{mod } n)$ (b) $a \equiv b(\text{mod } k)$

   (c) $a \equiv k(\text{mod } n)$ (d) $a \equiv n(\text{mod } k)$

10. If an integer a has order $\phi(n)$ modulo n and $(a,n)=1$ then a is _____

    (a) prime (b) order of n
    (c) a primitive root of n (d) root of n

11. There exists a primitive root for p^k when p is _____

    (a) even prime (b) prime

    (c) odd prime (d) special prime

12. If p is a prime and a is an integer co prime to p then a is called quadratic residue if __

    (a) $x^2 \equiv a(\text{mod } p)$ has a solution
    (b) $x^2 \equiv a(\text{mod } p)$ has no solution
    (c) $x \equiv a(\text{mod } p)$ has a solution
    (d) $x \equiv a(\text{mod } p)$ has no solution

13. If n = 100 then the number of divisor is _____

(a) 9 (b) 10 (c) 8 (d) 11

14. The notation $\sigma(n)$ is denoted by _____

(a) number of divisors (b) number of co primes

(c) sum of co primes (d) sum of divisors

15. The Mobius inversion formula for a positive integer n,

$\mu(n) =$ _____ for n = 1

(a) 1 (b) 0 (c) -1 (d) $(-1)^k$

16. The value of $\phi(15) =$ _____

(a) 5 (b) 8 (c) 3 (d) 1

17. If n is _____ then $\phi(2n) = \phi(n)$.

(a) even integer (b) odd integer

(c) prime (d) composite

18. In the property of Legendre symbol, $\left(\frac{a^2}{p}\right) =$ _____

(a) a (b) 1 (c) $\left(\frac{a}{p}\right)$ (d) $\left(\frac{1}{p}\right)$

19. If p is _____ then $\sum_{n=1}^{p-1}\left(\frac{n}{p}\right) = 0$

(a) any prime (b) odd prime

(c) even prime (d) special prime

20. If $a \equiv b(\text{mod } m)$ then _____

(a) $\left(\frac{a}{p}\right) = 1$ (b) $\left(\frac{b}{p}\right) = 1$

(c) $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = 1$ (d) $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

PART-B (3X2=6 Marks)

Answer all the Questions:

21. Define Legendre symbol
22. Define Congruence.
23. What is the value of $\phi(500)$?

PART-C (3X8=24 Marks)

Answer all the Questions:

24. (a) State and Prove Chinese Remainder theorem.

(OR)

(b) Find the least positive integer x such that $x \equiv 5(mod\ 7)$, $x \equiv 7(mod\ 11)$ and $x \equiv 3(mod\ 13)$.

25. (a) State and prove Gaussian reciprocity law.

(OR)

(b) For any odd prime p let $(a, p) = 1$. Consider the integers $a, 2a, 3a, \ldots, \left\{\frac{p-1}{2}\right\}a$ and their least positive residue modulo p. If n denotes the number of these residues that exceed $\frac{p}{2}$, then prove $\left(\frac{a}{p}\right) = (-1)^n$.

26. (a) If p is a prime then prove there exist $\varphi(p-1)$ primitive roots modulo p.

(OR)

(b) In any group G, $ab = ac$ implies b= c, and likewise $ba = ca$ implies $b = c$. If a is any element of a finite group G with identity element e, then prove that there is a unique smallest positive integer rsuch that $a^r = e$.