SATHYABAMA
INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)
Accredited "A" Grade by NAAC | 12B Status by UGC | Approved by AICTE
www.sathyabama.ac.in

SCHOOL OF SCIENCE AND HUMANITIES

DEPARTMENT OF MATHEMATICS

UNIT – I – NUMBER THOERY – SMT1554

Unit I

Euclidian Algorithm and Diophantine Equation

Theorem 1.1 (Division Algorithm)

Given integers *a* and *b,* with $b > 0$, there exist unique integers *q* and *r* satisfying $a = qb + r$. The integers *q* and *r* are called, respectively, the *quotient* and *remainder* in the division of *a* by *b*.

Proof:

Claim I (Existence) Consider the set $S = \{a - xb | \ x \in \mathbb{Z} \text{ and } a - xb \geq 0\}$. The set S so defined is non-empty, as $x = -|a| \in \mathbb{Z}$ such that $a - (-|a|b) = a + |a|b \geq 0$. By applying Well-Ordering Principle, we can assure that the set S contains a smallest integer, say, *r.* By the definition of *S,* there exists an integer *q* satisfying $r = a - qb \geq 0$. The choice of *r* satisfies the inequality $r < b$. If not, suppose that $r > b$. Then for $x = q + 1 \in \mathbb{Z}$, $a - (q + 1)b = (a - qb) - b = r - b \geq 0$. Hence, $r - b < r \in S$ a contradiction, as r is the smallest element of S. This guarantees that $r < b$.

Claim II (Uniqueness) Suppose that *a* has two distinct representations, say, $qb + r = a = q'b + r'$ where $0 < r < b$ and $0 < r' < b$. Then $r' - r = b(q - q')$ implies $|r' - r| = b|q - q'|$. $0 < r < b \Longrightarrow -b < -r < 0$. This results in the inequality $-b < r' - r < b$ equivalently, $|r - r'| < b$. Thus, $b|q - q'| < b \Longrightarrow 0 < |q - q'| < 1$. But as $|q - q'|$ is a nonnegative integer, the only possibility is that $|q - q'| = 0$ whence $q = q'$; this, in turn, gives $r = r'$, Hence the uniqueness of the integers *q* and *r* is proved. The statement of division algorithm follows.

Corollary 1.1

If *a* and *b* are integers, with $b \neq 0$, then there exist unique integers *q* and *r* such that $a = qb + r$, $0 \leq r < |b|$.

Proof:

The statement follows for the positive values of *b* from the division algorithm. Consider the case in which *b* is negative. Then $|b| > 0$, and by division algorithm there exists unique integers q' and *r* for which $a = q'|b| + r$. As *b* is negative, $a = q'(-b) + r = (-q')b + r = qb + r$, where $q = -q'$ and $0 \leq r < |b|$. Hence proved.

Greatest Common Divisor

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

Theorem 1.2

For integers *a, b,* c, the following hold:

(a) $a|0, 1|a, a|a$

(b) $a|1$if and only if $a = \pm 1$.

(c) If $a|b$ and $c|d$, then $ac|bd$.

(d) If $a|b$ and $b|c$, then $a|c$.

(e) $a|b$ and $b|a$ if and only if $a = \pm b$.

(f) If $a|b$ and $b \neq 0$, then $|a| \leq |b|$.

(g) If $a|b$ and $a|c$, then $a|(bx + cy)$ for arbitrary integers x and y.

Proof:

(a) We know that if$a = b(k)$ for some integer k, then $b|a$.

$0 = a(0) \Longrightarrow a|0$

$a = 1(a) \Longrightarrow 1|a$

$a = a(1) \Longrightarrow a|a$

(b) if $a|b$, then $b = a(k)$. Hence if $a|1$, then $1 = a(k)$ for some integer value k. But $k = \frac{1}{a} \Longrightarrow a = \pm 1$ Conversely, if $a = \pm 1$ then $a|1$ follows obviously.

(c) If $a|b$ and $c|d$, then $b = k_1 a$ and $d = k_2 c$. Hence, $bd = k_1 k_2 ac \Longrightarrow ac|bd$.

(d) If $a|b$ and $b|c$ then $b = k_1 a$ and $c = k_2 b = k_2(k_1 a) = ka$ where $k = k_1 k_2$. Hence $a|c$.

(e) If $a|b$ and $b|a$ then $b = k_1 a$ and $a = k_2 b \Longrightarrow a = k_1 k_2 a \Longrightarrow k_1 k_2 = 1 \Longrightarrow k_1 = \frac{1}{k_2}$, where k_1 and k_2 are integers. Hence, $k_1 = k_2 = \pm 1$. It follows that $a = \pm b$. Conversely, if $a = \pm b$, then it obviously follows that $a|b$ and $b|a$.

(f) If $a|b$, then $b = a(k)$ for some integer k. Hence, $|b| = |ak| = |a||k|$. As k is an integer, $|k| \geq 1 \Longrightarrow |a| \leq |a||k| \Longrightarrow |a| \leq |b|$.

(g) If $a|b$ and $a|c$, then $b = k_1 a$ and $c = k_2 a \Longrightarrow bx + cy = a(k_1 x + k_2 y) \Longrightarrow a|(bx + cy)$, for some integer values of x and y.

Definition 1.1

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 the following:

(a) $d|a$ and $d|b$

(b) If $c|a$ and $c|b$, then $c \leq d$.

Theorem 1.3

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:

Let S be a set of all positive linear combinations of a and b. $S = \{au + bv | au + bv > 0, u \text{ and } v \text{ are integers }\}$. The set S is non-empty, as $0 \leq |a| = a(\pm 1) + b(0) \in S$. Hence, by well-ordering principle, a smallest element d in S the form $ax + by$. From Division Algorithm, there exists unique integers q and r such that $a = qd + r$, where $0 \leq r < d$. Then r is an element of S, as $r = a - qd = a - q(ax + by) = a(1 - qx) + b(-qy)$. But $r < d$ contradicts the fact that d is the smallest element of S. Hence, $r = 0$. This proves that $d|a$. Similarly, $d|b$ follows. Let c be an arbitrary positive common divisor of the integers a and b, then $c|(ax + by)$; that is, $c|d$. This guarantees that $c = |c| \leq |d| = d$. Which proves that d is the greatest common divisor of a and b.

Corollary 1.2

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

Given $d = \gcd(a, b)$. Hence $d \mid a$ and $d \mid b$. It follows from the theorem that $d|(ax + by)$ for all integers x, y. Thus, every member of T is a multiple of d. Conversely, let x_0 and y_0 be integers such that $d = ax_0 + by_0$, 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.

Definition 1.2

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

Theorem 1.4

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

Let a and b be two integers that are relatively prime so that $\gcd(a, b) = 1$, then there exists integers x and y such that $d = 1 = ax + by$. Conversely, suppose that $1 = ax + by$ for some integers x and y, and $d = \gcd(a, b)$. Hence $d \mid a$ and $d \mid b$, this yields $d|(ax + by)$, or $d|1$. It follows that $d = \pm 1$.

Corollary 1.3

If $\gcd(a, b) = d$, then $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$

Proof

Given $\gcd(a, b) = d$. Then it follows that $d = ax + by$. Dividing by d on both sides, $1 = \frac{a}{d}x + \frac{b}{d}y$. Also, $d|a$ and $d|b$ guarantees that $\frac{a}{d}$ and $\frac{b}{d}$ are integers. From the theorem 1.4, $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Corollary 1.4

If $a|c$ and $b|c$, with gcd(a, b)= 1, then $ab|c$.

Proof

Given $a|c$ and $b|c$. Hence, $c = ar = bs$. As $\gcd(a,b) = 1$, $1 = ax + by$ for some integer values of x and y. Multiplying both sides by c, $c = c(ax + by) = acx + bcy$. 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, $ab|c$.

Theorem 1.5 (Euclid's lemma)

If $a|bc$, with gcd(a, b)= 1, then $a|c$.

Proof:

Given $\gcd(a,b) = 1$. From theorem 1.4, there exists integers x and y such that

$$ax + by = 1 \rightarrow (1)$$

For any two integers a and c, $a|ac$. Given $a|bc$. Hence from theorem 1.2, there exists integers x and y such that

$$a|(acx + bcy) \Rightarrow a|c(ax + by) \Rightarrow a|c$$

Theorem 1.6

For any two integers a and b, not both zero, a positive integer d is $\gcd(a,b)$ if and only if

(a) d I a and d I b.

(b) Whenever cIa and c I b, then c I d.

Proof:

Case (i) Suppose that $d = \gcd(a,b)$. Since d is a common divisor of a and b, d I a and d I b, so that (a) holds. From theorem 1.3, there exists integers x and y such that $d = ax + by$. If there exists an integer $c \neq d$ such that $c|a$ and $c|b$, then by theorem 1.2 $c|(ax + by)$. Hence $c|d$. (b) holds.

Case (ii) let d be any positive integer such that d I a and d I b. c be any other integer such that cIa and c I b, then c I d. Hence any other common divisor of a and b, divides d. It follows that $c \leq d$. This proves that d is the greatest common divisor of a and b.

Euclid's Division Algorithm

Given any two integers, the process of obtaining their greatest common divisor by recurrent application of division algorithm is called Euclid's division algorithm.

Lemma 1.1

If $a = qb + r$, then gcd(a, b)= gcd(b, r).

Proof:

Let $d = \gcd(a, b) \Rightarrow d|a$ and $d|b$. Hence $d|\big(a + b(-q)\big) \Rightarrow d|r$. It follows that *d* is a common divisor of *b* and *r*. Suppose *c* is any other common divisor of *b* and *r*, then $c|b$ and $c|r \Rightarrow c|(bq + r)$. i.e., $c|a$. Which proves *c* to be a common divisor of *a* and *b*. This ascertains $c \leq d$. Hence, *d* is the $\gcd(b, r)$. This proves the statement.

Practice Problems

1. Prove that if a and b are integers, with b > 0, then there exist unique integers q and r satisfying $a = qb + r$, where $2b \leq r < 3b$.
2. Show that cube of any integer is of the form $7k$ or $7k \pm 1$.
3. For any positive integer n, prove that $\frac{n(n+1)}{2}$ is an integer.
4. For any positive integer n, prove that $\frac{n(n+1)(2n+1)}{6}$ is an integer.
5. Prove that no member of the sequence $11,111,1111, \ldots \ldots$ is a perfect square.
6. Prove that any integer that can be expressed both as a square and cube of two different numbers is of the form $7k$ or $7k \pm 1$.
7. If $a|b$, then show that $a|(-b)$, $(-a)|b$ and $(-a)|(-b)$.
8. If *a* and *b* are any two integers not both zero, then prove that $\gcd(a, b) = \gcd(a, -b) = \gcd(-a, b) = \gcd(-a, -b)$.
9. Prove that, for a positive integer *n* and any integer *a*, gcd(*a*, *a*+ *n*) divides *n*; hence, gcd(*a*, *a*+ 1) = 1.
10. If *a* and *b* are integers, not both of which are zero, prove that gcd(2*a* - 3*b* , 4*a* - 5*b*) divides *b*; hence, gcd(2*a* + 3 , 4*a* + 5) = 1.
11. Prove the following properties of greatest common divisor.
    (a) If gcd(*a*, *b*)= 1, and gcd(*a*, *c*)= 1, then gcd(*a*, *bc*)= 1.
    (b) If gcd(*a*, *b*) = 1, and *c*I*a*, then gcd(*b*, *c*)= 1.
    (c) If gcd(*a*, *b*)= 1, then gcd(*ac*, *b*)= gcd(*c*, *b*).
    (d) If gcd(*a*, *b*)= 1, and *c*I*a*+ *b*, then gcd(*a*, *c*)= gcd(*b*, *c*)= 1.
    (e) If gcd(*a*, *b*)= 1, *d* I *ac*, and *d* I *bc*, then *d* I *c*.
    (f) If gcd(*a*, *b*)= 1, then gcd(a^2 , b^2) = 1.
12. If *a* I *bc*, show that *a* I gcd(*a*, *b*) gcd(*a*, *c*).

SATHYABAMA
INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)
Accredited "A" Grade by NAAC | 12B Status by UGC | Approved by AICTE
www.sathyabama.ac.in

SCHOOL OF SCIENCE AND HUMANITIES

DEPARTMENT OF MATHEMATICS

UNIT – II – NUMBER THEORY– SMT1554

Unit – II

Fundamental Theorem of Arithmetic

In this section we establish that an integer should be either prime or could be broken down into product of primes in a unique way. The preliminary concepts required to prove the fundamental theorem of arithmetic or the unique factorization theorem are introduced and the detailed proof of the theorem is established.

Definition 2.1

An integer $p > 1$ is called a prime number if its only divisors are 1 and the number itself. Any positive integer that is not prime is called composite.

Theorem 2.1

If p is any prime number and $p|ab$, then $p|a$ or $p|b$.

Proof

Given p is prime and $p|ab$. If $p|a$, then the statement follows. Suppose $p \nmid a$. Since p is prime, $\gcd(p, a) = 1$. By theorem we have proved in chapter 1, if $a|bc$ and $\gcd(a, b) = 1$, then $a|c$. It follows that $p|b$. This gives the desired result.

Corollary 1.

If p is a prime and $p|a_1a_2 \cdots a_n$, then $p|a_k$ for some k, where $1 \leq k \leq n$.

Proof.

Let us prove this theorem by method of induction, by indexing the factors of n. The statement is holds good when n = 1,2. Suppose, that $n > 2$ and assume that the statement 'whenever p divides a product of less than n factors, it divides at least one of the factors' is true.

Now let $p|a_1a_2 \cdots a_n$. From the previous theorem either $p|a_n$, from which the statement follows or $p|a_1a_2 \cdots a_{n-1}$. By the induction hypotheses, p divides at least one of the integers a_k for some $k = 1,2,3 \cdots, n-1$. This completes the proof of the statement.

Corollary 2

If $p, q_1, q_2, \ldots, q_n$ are all primes and $p|q_1q_2 \cdots q_n$, then $p = q_k$ for some k, where $1 \leq k \leq n$.

Proof.

From Corollary 1, if $p|q_1q_2 \cdots q_n$ then $p|q_k$ for some $k = 1,2,3 \cdots, n$. Since each q_k is prime, its only factors are 1 and q_k. Because $p > 1$, we are forced to conclude that $p = q_k$.

Theorem 3.2 Fundamental Theorem of Arithmetic. Every positive integer $n > 1$ can be expressed as a product of primes; this representation is unique, apart from the order in which the factors occur.

Proof. Either n is a prime or it is composite; in the former case, there is nothing more to prove. If n is composite, then there exists an integer d satisfying $d \mid n$ and $1 < d < n$. Among all such integers d, choose p_1 to be the smallest (this is possible by the Well-Ordering Principle). Then p_1 must be a prime number. Otherwise it too would have a divisor q with $1 < q < p_1$; but then $q \mid p_1$ and $p_1 \mid n$ imply that $q \mid n$, which contradicts the choice of p_1 as the smallest positive divisor, not equal to 1, of n.

We therefore may write $n = p_1 n_1$, where p_1 is prime and $1 < n_1 < n$. If n_1 happens to be a prime, then we have our representation. In the contrary case, the argument is repeated to produce a second prime number p_2 such that $n_1 = p_2 n_2$; that is,

$$n = p_1 p_2 n_2 \qquad 1 < n_2 < n_1$$

If n_2 is a prime, then it is not necessary to go further. Otherwise, write $n_2 = p_3 n_3$, with p_3 a prime:

$$n = p_1 p_2 p_3 n_3 \qquad 1 < n_3 < n_2$$

The decreasing sequence

$$n > n_1 > n_2 > \cdots > 1$$

cannot continue indefinitely, so that after a finite number of steps n_{k-1} is a prime, call it, p_k. This leads to the prime factorization

$$n = p_1 p_2 \cdots p_k$$

To establish the second part of the proof—the uniqueness of the prime factorization—let us suppose that the integer n can be represented as a product of primes in two ways; say,

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s \qquad r \leq s$$

where the p_i and q_j are all primes, written in increasing magnitude so that

$$p_1 \leq p_2 \leq \cdots \leq p_r \qquad q_1 \leq q_2 \leq \cdots \leq q_s$$

Because $p_1 \mid q_1 q_2 \cdots q_s$, Corollary 2 of Theorem 3.1 tells us that $p_1 = q_k$ for some k; but then $p_1 \geq q_1$. Similar reasoning gives $q_1 \geq p_1$, whence $p_1 = q_1$. We may cancel this common factor and obtain

$$p_2 p_3 \cdots p_r = q_2 q_3 \cdots q_s$$

Now repeat the process to get $p_2 = q_2$ and, in turn,

$$p_3 p_4 \cdots p_r = q_3 q_4 \cdots q_s$$

Continue in this fashion. If the inequality $r < s$ were to hold, we would eventually arrive at

$$1 = q_{r+1} q_{r+2} \cdots q_s$$

which is absurd, because each $q_j > 1$. Hence, $r = s$ and

$$p_1 = q_1 \qquad p_2 = q_2, \ldots, p_r = q_r$$

making the two factorizations of n identical. The proof is now complete.

Of course, several of the primes that appear in the factorization of a given positive integer may be repeated, as is the case with $360 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5$. By collecting like primes and replacing them by a single factor, we can rephrase Theorem 3.2 as a corollary.

Corollary. Any positive integer $n > 1$ can be written uniquely in a *canonical form*

$$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$$

where, for $i = 1, 2, \ldots, r$, each k_i is a positive integer and each p_i is a prime, with $p_1 < p_2 < \cdots < p_r$.

To illustrate, the canonical form of the integer 360 is $360 = 2^3 \cdot 3^2 \cdot 5$. As further examples we cite

$$4725 = 3^3 \cdot 5^2 \cdot 7 \qquad \text{and} \qquad 17460 = 2^3 \cdot 3^2 \cdot 5 \cdot 7^2$$

Theorem 3.2 should not be taken lightly because number systems do exist in which the factorization into "primes" is not unique. Perhaps the most elemental example is the set E of all positive even integers. Let us agree to call an even integer an e-prime if it is not the product of two other even integers. Thus, 2, 6, 10, 14, ... all are e-primes, whereas 4, 8, 12, 16, ... are not. It is not difficult to see that the integer 60 can be factored into e-primes in two distinct ways; namely,

$$60 = 2 \cdot 30 = 6 \cdot 10$$

Part of the difficulty arises from the fact that Theorem 3.1 is lacking in the set E; that is, $6 \mid 2 \cdot 30$, but $6 \nmid 2$ and $6 \nmid 30$.

This is an opportune moment to insert a famous result of Pythagoras. Mathematics as a science began with Pythagoras (569–500 B.C.), and much of the content of Euclid's *Elements* is due to Pythagoras and his School. The Pythagoreans deserve the credit for being the first to classify numbers into odd and even, prime and composite.

Theorem 3.3 Pythagoras. The number $\sqrt{2}$ is irrational.

Proof. Suppose, to the contrary, that $\sqrt{2}$ is a rational number, say, $\sqrt{2} = a/b$, where a and b are both integers with $\gcd(a, b) = 1$. Squaring, we get $a^2 = 2b^2$, so that $b \mid a^2$. If $b > 1$, then the Fundamental Theorem of Arithmetic guarantees the existence of a prime p such that $p \mid b$. It follows that $p \mid a^2$ and, by Theorem 3.1, that $p \mid a$; hence, $\gcd(a, b) \geq p$. We therefore arrive at a contradiction, unless $b = 1$. But if this happens, then $a^2 = 2$, which is impossible (we assume that the reader is willing to grant that no integer can be multiplied by itself to give 2). Our supposition that $\sqrt{2}$ is a rational number is untenable, and so $\sqrt{2}$ must be irrational.

There is an interesting variation on the proof of Theorem 3.3. If $\sqrt{2} = a/b$ with $\gcd(a, b) = 1$, there must exist integers r and s satisfying $ar + bs = 1$. As a result,

$$\sqrt{2} = \sqrt{2}(ar + bs) = (\sqrt{2}a)r + (\sqrt{2}b)s = 2br + as$$

This representation of $\sqrt{2}$ leads us to conclude that $\sqrt{2}$ is an integer, an obvious impossibility.

PROBLEMS 3.1

1. It has been conjectured that there are infinitely many primes of the form $n^2 - 2$. Exhibit five such primes.
2. Give an example to show that the following conjecture is not true: Every positive integer can be written in the form $p + a^2$, where p is either a prime or 1, and $a \geq 0$.
3. Prove each of the assertions below:
   (a) Any prime of the form $3n + 1$ is also of the form $6m + 1$.
   (b) Each integer of the form $3n + 2$ has a prime factor of this form.
   (c) The only prime of the form $n^3 - 1$ is 7.
   [*Hint:* Write $n^3 - 1$ as $(n - 1)(n^2 + n + 1)$.]
   (d) The only prime p for which $3p + 1$ is a perfect square is $p = 5$.
   (e) The only prime of the form $n^2 - 4$ is 5.
4. If $p \geq 5$ is a prime number, show that $p^2 + 2$ is composite.
   [*Hint:* p takes one of the forms $6k + 1$ or $6k + 5$.]
5. (a) Given that p is a prime and $p \mid a^n$, prove that $p^n \mid a^n$.
   (b) If $\gcd(a, b) = p$, a prime, what are the possible values of $\gcd(a^2, b^2)$, $\gcd(a^2, b)$ and $\gcd(a^3, b^2)$?
6. Establish each of the following statements:
   (a) Every integer of the form $n^4 + 4$, with $n > 1$, is composite.
   [*Hint:* Write $n^4 + 4$ as a product of two quadratic factors.]
   (b) If $n > 4$ is composite, then n divides $(n - 1)!$.
   (c) Any integer of the form $8^n + 1$, where $n \geq 1$, is composite.
   [*Hint:* $2^n + 1 \mid 2^{3n} + 1$.]
   (d) Each integer $n > 11$ can be written as the sum of two composite numbers.
   [*Hint:* If n is even, say $n = 2k$, then $n - 6 = 2(k - 3)$; for n odd, consider the integer $n - 9$.]
7. Find all prime numbers that divide 50!.
8. If $p \geq q \geq 5$ and p and q are both primes, prove that $24 \mid p^2 - q^2$.
9. (a) An unanswered question is whether there are infinitely many primes that are 1 more than a power of 2, such as $5 = 2^2 + 1$. Find two more of these primes.
   (b) A more general conjecture is that there exist infinitely many primes of the form $n^2 + 1$; for example, $257 = 16^2 + 1$. Exhibit five more primes of this type.
10. If $p \neq 5$ is an odd prime, prove that either $p^2 - 1$ or $p^2 + 1$ is divisible by 10.
11. Another unproven conjecture is that there are an infinitude of primes that are 1 less than a power of 2, such as $3 = 2^2 - 1$.
    (a) Find four more of these primes.
    (b) If $p = 2^k - 1$ is prime, show that k is an odd integer, except when $k = 2$.
    [*Hint:* $3 \mid 4^n - 1$ for all $n \geq 1$.]
12. Find the prime factorization of the integers 1234, 10140, and 36000.
13. If $n > 1$ is an integer not of the form $6k + 3$, prove that $n^2 + 2^n$ is composite.
    [*Hint:* Show that either 2 or 3 divides $n^2 + 2^n$.]
14. It has been conjectured that every even integer can be written as the difference of two consecutive primes in infinitely many ways. For example,

$$6 = 29 - 23 = 137 - 131 = 599 - 593 = 1019 - 1013 = \cdots$$

    Express the integer 10 as the difference of two consecutive primes in 15 ways.
15. Prove that a positive integer $a > 1$ is a square if and only if in the canonical form of a all the exponents of the primes are even integers.

16. An integer is said to be *square-free* if it is not divisible by the square of any integer greater than 1. Prove the following:
   (a) An integer $n > 1$ is square-free if and only if n can be factored into a product of distinct primes.
   (b) Every integer $n > 1$ is the product of a square-free integer and a perfect square. [*Hint:* If $n = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$ is the canonical factorization of n, then write $k_i = 2q_i + r_i$ where $r_i = 0$ or 1 according as k_i is even or odd.]

17. Verify that any integer n can be expressed as $n = 2^k m$, where $k \geq 0$ and m is an odd integer.

18. Numerical evidence makes it plausible that there are infinitely many primes p such that $p + 50$ is also prime. List 15 of these primes.

19. A positive integer n is called *square-full*, or *powerful*, if $p^2 \mid n$ for every prime factor p of n (there are 992 square-full numbers less than 250,000). If n is square-full, show that it can be written in the form $n = a^2 b^3$, with a and b positive integers.

3.2 THE SIEVE OF ERATOSTHENES

Given a particular integer, how can we determine whether it is prime or composite and, in the latter case, how can we actually find a nontrivial divisor? The most obvious approach consists of successively dividing the integer in question by each of the numbers preceding it; if none of them (except 1) serves as a divisor, then the integer must be prime. Although this method is very simple to describe, it cannot be regarded as useful in practice. For even if one is undaunted by large calculations, the amount of time and work involved may be prohibitive.

There is a property of composite numbers that allows us to reduce materially the necessary computations—but still the process remains cumbersome. If an integer $a > 1$ is composite, then it may be written as $a = bc$, where $1 < b < a$ and $1 < c < a$. Assuming that $b \leq c$, we get $b^2 \leq bc = a$, and so $b \leq \sqrt{a}$. Because $b > 1$, Theorem 3.2 ensures that b has at least one prime factor p. Then $p \leq b \leq \sqrt{a}$; furthermore, because $p \mid b$ and $b \mid a$, it follows that $p \mid a$. The point is simply this: A composite number a will always possess a prime divisor p satisfying $p \leq \sqrt{a}$.

In testing the primality of a specific integer $a > 1$, it therefore suffices to divide a by those primes not exceeding $\sqrt{a}$ (presuming, of course, the availability of a list of primes up to $\sqrt{a}$). This may be clarified by considering the integer $a = 509$. Inasmuch as $22 < \sqrt{509} < 23$, we need only try out the primes that are not larger than 22 as possible divisors, namely, the primes 2, 3, 5, 7, 11, 13, 17, 19. Dividing 509 by each of these, in turn, we find that none serves as a divisor of 509. The conclusion is that 509 must be a prime number.

Example 3.1. The foregoing technique provides a practical means for determining the canonical form of an integer, say $a = 2093$. Because $45 < \sqrt{2093} < 46$, it is enough to examine the primes 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43. By trial, the first of these to divide 2093 is 7, and $2093 = 7 \cdot 299$. As regards the integer 299, the seven primes that are less than 18 (note that $17 < \sqrt{299} < 18$) are 2, 3, 5, 7, 11, 13, 17. The first prime divisor of 299 is 13 and, carrying out the required division, we obtain $299 = 13 \cdot 23$. But 23 is itself a prime, whence 2093 has exactly three prime factors, 7, 13, and 23:

$$2093 = 7 \cdot 13 \cdot 23$$

Another Greek mathematician whose work in number theory remains significant is Eratosthenes of Cyrene (276–194 B.C.). Although posterity remembers him mainly as the director of the world-famous library at Alexandria, Eratosthenes was gifted in all branches of learning, if not of first rank in any; in his own day, he was nicknamed "Beta" because, it was said, he stood at least second in every field. Perhaps the most impressive feat of Eratosthenes was the accurate measurement of the earth's circumference by a simple application of Euclidean geometry.

We have seen that if an integer $a > 1$ is not divisible by any prime $p \leq \sqrt{a}$, then a is of necessity a prime. Eratosthenes used this fact as the basis of a clever technique, called the *Sieve of Eratosthenes*, for finding all primes below a given integer n. The scheme calls for writing down the integers from 2 to n in their natural order and then systematically eliminating all the composite numbers by striking out all multiples $2p, 3p, 4p, 5p, \ldots$ of the primes $p \leq \sqrt{n}$. The integers that are left on the list—those that do not fall through the "sieve"—are primes.

To see an example of how this works, suppose that we wish to find all primes not exceeding 100. Consider the sequence of consecutive integers 2, 3, 4, . . . ,100. Recognizing that 2 is a prime, we begin by crossing out all even integers from our listing, except 2 itself. The first of the remaining integers is 3, which must be a prime. We keep 3, but strike out all higher multiples of 3, so that 9, 15, 21, . . . are now removed (the even multiples of 3 having been removed in the previous step). The smallest integer after 3 that has not yet been deleted is 5. It is not divisible by either 2 or 3—otherwise it would have been crossed out—hence, it is also a prime. All proper multiples of 5 being composite numbers, we next remove 10, 15, 20, . . . (some of these are, of course, already missing), while retaining 5 itself. The first surviving integer 7 is a prime, for it is not divisible by 2, 3, or 5, the only primes that precede it. After eliminating the proper multiples of 7, the largest prime less than $\sqrt{100} = 10$, all composite integers in the sequence 2, 3, 4, . . . ,100 have fallen through the sieve. The positive integers that remain, to wit, 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, are all of the primes less than 100.

The following table represents the result of the completed sieve. The multiples of 2 are crossed out by \; the multiples of 3 are crossed out by /; the multiples of 5 are crossed out by —; the multiples of 7 are crossed out by ∼.

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

By this point, an obvious question must have occurred to the reader. Is there a largest prime number, or do the primes go on forever? The answer is to be found in a remarkably simple proof given by Euclid in Book IX of his *Elements*. Euclid's argument is universally regarded as a model of mathematical elegance. Loosely

speaking, it goes like this: Given any finite list of prime numbers, one can always find a prime not on the list; hence, the number of primes is infinite. The actual details appear below.

Theorem 3.4 Euclid. There is an infinite number of primes.

Proof. Euclid's proof is by contradiction. Let $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7, \ldots$ be the primes in ascending order, and suppose that there is a last prime, called p_n. Now consider the positive integer

$$P = p_1 p_2 \cdots p_n + 1$$

Because $P > 1$, we may put Theorem 3.2 to work once again and conclude that P is divisible by some prime p. But $p_1, p_2, \ldots, p_n$ are the only prime numbers, so that p must be equal to one of $p_1, p_2, \ldots, p_n$. Combining the divisibility relation $p \mid p_1 p_2 \cdots p_n$ with $p \mid P$, we arrive at $p \mid P - p_1 p_2 \cdots p_n$ or, equivalently, $p \mid 1$. The only positive divisor of the integer 1 is 1 itself and, because $p > 1$, a contradiction arises. Thus, no finite list of primes is complete, whence the number of primes is infinite.

For a prime p, define $p^{\#}$ to be the product of all primes that are less than or equal to p. Numbers of the form $p^{\#} + 1$ might be termed *Euclidean numbers*, because they appear in Euclid's scheme for proving the infinitude of primes. It is interesting to note that in forming these integers, the first five, namely,

$$\begin{aligned}
2^{\#} + 1 &= 2 + 1 = 3 \\
3^{\#} + 1 &= 2 \cdot 3 + 1 = 7 \\
5^{\#} + 1 &= 2 \cdot 3 \cdot 5 + 1 = 31 \\
7^{\#} + 1 &= 2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211 \\
11^{\#} + 1 &= 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 = 2311
\end{aligned}$$

are all prime numbers. However,

$$\begin{aligned}
13^{\#} + 1 &= 59 \cdot 509 \\
17^{\#} + 1 &= 19 \cdot 97 \cdot 277 \\
19^{\#} + 1 &= 347 \cdot 27953
\end{aligned}$$

are not prime. A question whose answer is not known is whether there are infinitely many primes p for which $p^{\#} + 1$ is also prime. For that matter, are there infinitely many composite $p^{\#} + 1$?

At present, 19 primes of the form $p^{\#} + 1$ have been identified. These correspond to the values $p = 2, 3, 5, 7, 11, 31, 379, 1019, 1021, 2657, 3229, 4547, 4787, 11549, 13649, 18523, 23801, 24029$, and 42209; the largest of these, a number consisting of 18241 digits, was discovered in 2000. The integer $p^{\#} + 1$ is composite for all other $p \leq 120000$.

Euclid's theorem is too important for us to be content with a single proof. Here is a variation in the reasoning: Form the infinite sequence of positive integers

$$\begin{aligned} n_1 &= 2 \\ n_2 &= n_1 + 1 \\ n_3 &= n_1 n_2 + 1 \\ n_4 &= n_1 n_2 n_3 + 1 \\ &\vdots \\ n_k &= n_1 n_2 \cdots n_{k-1} + 1 \\ &\vdots \end{aligned}$$

Because each $n_k > 1$, each of these integers is divisible by a prime. But no two n_k can have the same prime divisor. To see this, let $d = \gcd(n_i, n_k)$ and suppose that $i < k$. Then d divides n_i and, hence, must divide $n_1 n_2 \cdots n_{k-1}$. Because $d \mid n_k$, Theorem 2.2 (g) tells us that $d \mid n_k - n_1 n_2 \cdots n_{k-1}$ or $d \mid 1$. The implication is that $d = 1$, and so the integers $n_k (k = 1, 2, \ldots)$ are pairwise relatively prime. The point we wish to make is that there are as many distinct primes as there are integers n_k, namely, infinitely many of them.

Let p_n denote the nth of the prime numbers in their natural order. Euclid's proof shows that the expression $p_1 p_2 \cdots p_n + 1$ is divisible by at least one prime. If there are several such prime divisors, then p_{n+1} cannot exceed the smallest of these so that $p_{n+1} \leq p_1 p_2 \cdots p_n + 1$ for $n \geq 1$. Another way of saying the same thing is that

$$p_n \leq p_1 p_2 \cdots p_{n-1} + 1 \qquad n \geq 2$$

With a slight modification of Euclid's reasoning, this inequality can be improved to give

$$p_n \leq p_1 p_2 \cdots p_{n-1} - 1 \qquad n \geq 3$$

For instance, when $n = 5$, this tells us that

$$11 = p_5 \leq 2 \cdot 3 \cdot 5 \cdot 7 - 1 = 209$$

We can see that the estimate is rather extravagant. A sharper limitation on the size of p_n is given by *Bonse's inequality*, which states that

$$p_n^2 < p_1 p_2 \cdots p_{n-1} \qquad n \geq 5$$

This inequality yields $p_5^2 < 210$, or $p_5 \leq 14$. A somewhat better size-estimate for p_5 comes from the inequality

$$p_{2n} \leq p_2 p_3 \cdots p_n - 2 \qquad n \geq 3$$

Here, we obtain

$$p_5 < p_6 \leq p_2 p_3 - 2 = 3 \cdot 5 - 2 = 13$$

To approximate the size of p_n from these formulas, it is necessary to know the values of $p_1, p_2, \ldots, p_{n-1}$. For a bound in which the preceding primes do not enter the picture, we have the following theorem.

Theorem 3.5. If p_n is the nth prime number, then $p_n \leq 2^{2^{n-1}}$.

Proof. Let us proceed by induction on n, the asserted inequality being clearly true when $n = 1$. As the hypothesis of the induction, we assume that $n > 1$ and that the result holds for all integers up to n. Then

$$\begin{aligned} p_{n+1} &\leq p_1 p_2 \cdots p_n + 1 \\ &\leq 2 \cdot 2^2 \cdots 2^{2^{n-1}} + 1 = 2^{1+2+2^2+\cdots+2^{n-1}} + 1 \end{aligned}$$

Recalling the identity $1 + 2 + 2^2 + \cdots + 2^{n-1} = 2^n - 1$, we obtain

$$p_{n+1} \leq 2^{2^n - 1} + 1$$

However, $1 \leq 2^{2^n - 1}$ for all n; whence

$$\begin{aligned} p_{n+1} &\leq 2^{2^n - 1} + 2^{2^n - 1} \\ &= 2 \cdot 2^{2^n - 1} = 2^{2^n} \end{aligned}$$

completing the induction step, and the argument.

There is a corollary to Theorem 3.5 that is of interest.

Corollary. For $n \geq 1$, there are at least $n + 1$ primes less than 2^{2^n}.

Proof. From the theorem, we know that $p_1, p_2, \ldots, p_{n+1}$ are all less than 2^{2^n}.

We can do considerably better than is indicated by Theorem 3.5. In 1845, Joseph Bertrand conjectured that the prime numbers are well-distributed in the sense that between $n \geq 2$ and $2n$ there is at least one prime. He was unable to establish his conjecture, but verified it for all $n \leq 3{,}000{,}000$. (One way of achieving this is to consider a sequence of primes 3, 5, 7, 13, 23, 43, 83, 163, 317, 631, 1259, 2503, 5003, 9973, 19937, 39869, 79699, 159389, ... each of which is less than twice the preceding.) Because it takes some real effort to substantiate this famous conjecture, let us content ourselves with saying that the first proof was carried out by the Russian mathematician P. L. Tchebycheff in 1852. Granting the result, it is not difficult to show that

$$p_n < 2^n \qquad n \geq 2$$

and as a direct consequence, $p_{n+1} < 2p_n$ for $n \geq 2$. In particular,

$$11 = p_5 < 2 \cdot p_4 = 14$$

To see that $p_n < 2^n$, we argue by induction on n. Clearly, $p_2 = 3 < 2^2$, so that the inequality is true here. Now assume that the inequality holds for an integer n, whence $p_n < 2^n$. Invoking Bertrand's conjecture, there exists a prime number p satisfying $2^n < p < 2^{n+1}$; that is, $p_n < p$. This immediately leads to the conclusion that $p_{n+1} \leq p < 2^{n+1}$, which completes the induction and the proof.

Primes of special form have been of perennial interest. Among these, the repunit primes are outstanding in their simplicity. A *repunit* is an integer written (in decimal notation) as a string of 1's, such as 11, 111, or 1111. Each such integer must have the form $(10^n - 1)/9$. We use the symbol R_n to denote the repunit consisting of n consecutive 1's. A peculiar feature of these numbers is the apparent scarcity of primes among them. So far, only R_2, R_{19}, R_{23}, R_{317}, R_{1031}, R_{49081}, and R_{86453}

have been identified as primes (the last one in 2001). It is known that the only possible repunit primes R_n for all $n \leq 45000$ are the seven numbers just indicated. No conjecture has been made as to the existence of any others. For a repunit R_n to be prime, the subscript n must be a prime; that this is not a sufficient condition is shown by

$$R_5 = 11111 = 41 \cdot 271 \qquad R_7 = 1111111 = 239 \cdot 4649$$

PROBLEMS 3.2

1. Determine whether the integer 701 is prime by testing all primes $p \leq \sqrt{701}$ as possible divisors. Do the same for the integer 1009.
2. Employing the Sieve of Eratosthenes, obtain all the primes between 100 and 200.
3. Given that $p \nmid n$ for all primes $p \leq \sqrt[3]{n}$, show that $n > 1$ is either a prime or the product of two primes.
   [*Hint:* Assume to the contrary that n contains at least three prime factors.]
4. Establish the following facts:
   (a) $\sqrt{p}$ is irrational for any prime p.
   (b) If $a > 0$ and $\sqrt[n]{a}$ is rational, then $\sqrt[n]{a}$ must be an integer.
   (c) For $n \geq 2$, $\sqrt[n]{n}$ is irrational.
   [*Hint:* Use the fact that $2^n > n$.]
5. Show that any composite three-digit number must have a prime factor less than or equal to 31.
6. Fill in any missing details in this sketch of a proof of the infinitude of primes: Assume that there are only finitely many primes, say $p_1, p_2, \ldots, p_n$. Let A be the product of any r of these primes and put $B = p_1 p_2 \cdots p_n / A$. Then each p_k divides either A or B, but not both. Because $A + B > 1$, $A + B$ has a prime divisor different from any of the p_k, which is a contradiction.
7. Modify Euclid's proof that there are infinitely many primes by assuming the existence of a largest prime p and using the integer $N = p! + 1$ to arrive at a contradiction.
8. Give another proof of the infinitude of primes by assuming that there are only finitely many primes, say $p_1, p_2, \ldots, p_n$, and using the following integer to arrive at a contradiction:

$$N = p_2 p_3 \cdots p_n + p_1 p_3 \cdots p_n + \cdots + p_1 p_2 \cdots p_{n-1}$$

9. (a) Prove that if $n > 2$, then there exists a prime p satisfying $n < p < n!$.
   [*Hint:* If $n! - 1$ is not prime, then it has a prime divisor p; and $p \leq n$ implies $p \mid n!$, leading to a contradiction.]
   (b) For $n > 1$, show that every prime divisor of $n! + 1$ is an odd integer that is greater than n.
10. Let q_n be the smallest prime that is strictly greater than $P_n = p_1 p_2 \cdots p_n + 1$. It has been conjectured that the difference $q_n - (p_1 p_2 \cdots p_n)$ is always a prime. Confirm this for the first five values of n.
11. If p_n denotes the nth prime number, put $d_n = p_{n+1} - p_n$. An open question is whether the equation $d_n = d_{n+1}$ has infinitely many solutions. Give five solutions.
12. Assuming that p_n is the nth prime number, establish each of the following statements:
   (a) $p_n > 2n - 1$ for $n \geq 5$.
   (b) None of the integers $P_n = p_1 p_2 \cdots p_n + 1$ is a perfect square.
   [*Hint:* Each P_n is of the form $4k + 3$ for $n > 1$.]

(c) The sum

$$\frac{1}{p_1} + \frac{1}{p_2} + \cdots + \frac{1}{p_n}$$

is never an integer.

13. For the repunits R_n, verify the assertions below:

(a) If $n \mid m$, then $R_n \mid R_m$.

[*Hint:* If $m = kn$, consider the identity

$$x^m - 1 = (x^n - 1)(x^{(k-1)n} + x^{(k-2)n} + \cdots + x^n + 1).]$$

(b) If $d \mid R_n$ and $d \mid R_m$, then $d \mid R_{n+m}$.

[*Hint:* Show that $R_{m+n} = R_n 10^m + R_m$.]

(c) If $\gcd(n, m) = 1$, then $\gcd(R_n, R_m) = 1$.

14. Use the previous problem to obtain the prime factors of the repunit R_{10}.

3.3 THE GOLDBACH CONJECTURE

Although there is an infinitude of primes, their distribution within the positive integers is most mystifying. Repeatedly in their distribution we find hints or, as it were, shadows of a pattern; yet an actual pattern amenable to precise description remains elusive. The difference between consecutive primes can be small, as with the pairs 11 and 13, 17 and 19, or for that matter 1000000000061 and 1000000000063. At the same time there exist arbitrarily long intervals in the sequence of integers that 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 $p + 2$ that are both primes. Numerical evidence leads us to suspect an affirmative conclusion. Electronic computers have discovered 152892 pairs of twin primes less than 30000000 and 20 pairs between 10^{12} and $10^{12} + 10000$, which hints at their growing scarcity as the positive integers increase in magnitude. Many examples of immense twins are known. The largest twins to date, each 51090 digits long,

$$33218925 \cdot 2^{169690} \pm 1$$

were discovered in 2002.

Consecutive primes cannot only be close together, but also can 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 simply need to 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. Indeed, $(n + 1)! + 2$ 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 previous argument 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, we can find other sets of four consecutive composites, such as 24, 25, 26, 27 or 32, 33, 34, 35.

As this example suggests, our procedure for constructing gaps between two consecutive primes gives a gross overestimate of where they occur among the integers. The first occurrences of prime gaps of specific lengths, where all the intervening integers are composite, have been the subject of computer searches. For instance, there is a gap of length 778 (that is, $p_{n+1} - p_n = 778$) following the prime 42842283925351. No gap of this size exists between two smaller primes. The largest effectively calculated gap between consecutive prime numbers has length 1132, with a string of 1131 composites immediately after the prime

$$1693182318746371$$

Interestingly, computer researchers have not identified gaps of every possible width up to 1132. The smallest missing gap size is 796. The conjecture is that there is a prime gap (a string of $2k - 1$ consecutive composites between two primes) for every even integer $2k$.

This brings us to another unsolved problem concerning the primes, the Goldbach conjecture. In a letter to Leonhard Euler in the year 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:

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

Although it seems that Euler never tried to prove the result, upon writing to Goldbach at a later date, Euler 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 a prime of the form $4n + 1$ or 1.

The numerical data suggesting the truth of Goldbach's conjecture are overwhelming. It has been verified by computers for all even integers less than $4 \cdot 10^{14}$.

As the integers become larger, the number of different ways in which $2n$ can be expressed as the sum of two primes increases. For example, there are 219400 such representations for the even integer 100000000. Although this supports the feeling that Goldbach was correct in his conjecture, it is far from a mathematical proof, and all attempts to obtain a proof have been completely unsuccessful. One of the most famous number theorists of the last century, G. H. Hardy, in his address to the Mathematical Society of Copenhagen in 1921, stated that the Goldbach conjecture appeared "... probably as difficult as any of the unsolved problems in mathematics." It is currently known that every even integer is the sum of six or fewer primes.

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. To see this, 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.

The first real progress on the conjecture in nearly 200 years was made by Hardy and Littlewood in 1922. On the basis of a certain unproved hypothesis, the so-called generalized Riemann hypothesis, they showed that every sufficiently large odd number is the sum of three odd primes. In 1937, the Russian mathematician I. M. Vinogradov was able to remove the dependence on the generalized Riemann hypothesis, thereby giving an unconditional proof of this result; that is to say, he established that all odd integers greater than some effectively computable n_0 can be written as the sum of three odd primes.

$$n = p_1 + p_2 + p_3 \qquad (n \text{ odd}, n \text{ sufficiently large})$$

Vinogradov was unable to decide how large n_0 should be, but Borozdkin (1956) proved that $n_0 < 3^{3^{15}}$. In 2002, the bound on n_0 was reduced to 10^{1346}. It follows immediately that every even integer from some point on is the sum of either two or four primes. Thus, it is enough to answer the question for every odd integer n in the range $9 \leq n \leq n_0$, which, for a given integer, becomes a matter of tedious computation (unfortunately, n_0 is so large that this exceeds the capabilities of the most modern electronic computers).

Because of the strong evidence in favor of the famous Goldbach conjecture, we readily become convinced that it is true. Nevertheless, it might be false. Vinogradov showed that if $A(x)$ is the number of even integers $n \leq x$ that are not the sum of two primes, then

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

This allows us to say that "almost all" even integers satisfy the conjecture. As Edmund 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."

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

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

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 $4n + 1$, and the other containing integers of the form $4n + 3$.

The question arises as to how these two types of primes are distributed within the set of positive integers. Let us display the first few odd prime numbers in consecutive order, putting the $4n + 3$ primes in the top row and the $4n + 1$ primes under them:

3	7	11	19	23	31	43	47	59	67	71	79	83
5	13	17	29	37	41	53	61	73	89			

At this point, one might have the general impression that primes of the form $4n + 3$ are more abundant than are those of the form $4n + 1$. To obtain more precise information, we require the help of the function $\pi_{a,b}(x)$, which counts the number of primes of the form $p = an + b$ not exceeding x. Our small table, for instance, indicates that $\pi_{4,1}(89) = 10$ and $\pi_{4,3}(89) = 13$.

In a famous letter written in 1853, Tchebycheff remarked that $\pi_{4,1}(x) \leq \pi_{4,3}(x)$ for small values of x. He also implied that he had a proof that the inequality always held. In 1914, J. E. Littlewood showed that the inequality fails infinitely often, but his method gave no indication of the value of x for which this first happens. It turned out to be quite difficult to find. Not until 1957 did a computer search reveal that $x = 26861$ is the smallest prime for which $\pi_{4,1}(x) > \pi_{4,3}(x)$; here, $\pi_{4,1}(x) = 1473$ and $\pi_{4,3}(x) = 1472$. This is an isolated situation, because the next prime at which a reversal occurs is $x = 616{,}841$. Remarkably, $\pi_{4,1}(x) > \pi_{4,3}(x)$ for the 410 million successive integers x lying between 18540000000 and 18950000000.

The behavior of primes of the form $3n \pm 1$ provided more of a computational challenge: the inequality $\pi_{3,1}(x) \leq \pi_{3,2}(x)$ holds for all x until one reaches $x = 608981813029$.

This furnishes 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 is 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 us take $k = 4n + 1$ 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.

Theorem 3.6. There are 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

$$N = 4q_1q_2 \cdots q_s - 1 = 4(q_1q_2 \cdots q_s - 1) + 3$$

and let $N = r_1r_2 \cdots r_t$ be its prime factorization. Because 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 $4n + 3$, we 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 P. G. L. Dirichlet on primes in arithmetic progressions, established in 1837. The proof is much too difficult for inclusion here, so that we must 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.

Dirichlet's theorem tells us, for instance, that there are infinitely many prime numbers ending in 999, such as 1999, 100999, 1000999, ... for these appear in the arithmetic progression determined by $1000n + 999$, where $\gcd(1000, 999) = 1$.

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

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

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

It is an old, but still unsolved question of whether there exist arbitrarily long but finite arithmetic progressions consisting only of prime numbers (not necessarily consecutive primes). The longest progression found to date is composed of the 22 primes:

$$11410337850553 + 4609098694200n \qquad 0 \leq n \leq 21$$

The prime factorization of the common difference between the terms is

$$2^3 \cdot 3 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 1033$$

which is divisible by 9699690, the product of the primes less than 22. This takes place according to Theorem 3.8.

Theorem 3.8. If all the $n > 2$ terms of the arithmetic progression

$$p, p + d, p + 2d, \ldots, p + (n - 1)d$$

are prime numbers, then the common difference d is divisible by every prime $q < n$.

Proof. Consider a prime number $q < n$ and assume to the contrary that $q \nmid d$. We claim that the first q terms of the progression

$$p, p + d, p + 2d, \ldots, p + (q - 1)d \tag{1}$$

will leave different remainders when divided by q. Otherwise there exist integers j and k, with $0 \leq j < k \leq q - 1$, such that the numbers $p + jd$ and $p + kd$ yield the same remainder upon division by q. Then q divides their difference $(k - j)d$. But $\gcd(q, d) = 1$, and so Euclid's lemma leads to $q \mid k - j$, which is nonsense in light of the inequality $k - j \leq q - 1$.

Because the q different remainders produced from Eq. (1) are drawn from the q integers $0, 1, \ldots, q - 1$, one of these remainders must be zero. This means that $q \mid p + td$ for some t satisfying $0 \leq t \leq q - 1$. Because of the inequality $q < n \leq p \leq p + td$, we are forced to conclude that $p + td$ is composite. (If p were less than n, one of the terms of the progression would be $p + pd = p(1 + d)$.) With this contradiction, the proof that $q \mid d$ is complete.

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 47, 53, 59, and 251, 257, 263, 269.

Most recently a sequence of 10 consecutive primes was discovered in which each term exceeds its predecessor by just 210; the smallest of these primes has 93 digits. Finding an arithmetic progression consisting of 11 consecutive primes is likely to be out of reach for some time. Absent the restriction that the primes involved be consecutive, strings of 11-term arithmetic progressions are easily located. One such is

$$110437 + 13860n \qquad 0 \leq n \leq 10$$

In the interest 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 years ago that the quadratic polynomial

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

assumed only prime values. This was shown to be false by Euler, in 1772. 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 $f(42) = 1847$ turns out to be prime once again. In fact, for the first 100 integer values of n, the so-called Euler polynomial represents 86 primes. Although it starts off very well in the production of primes, there are other quadratics such as

$$g(n) = n^2 + n + 27941$$

that begin to best $f(n)$ as the values of n become larger. For example, $g(n)$ is prime for 286129 values of $0 \leq n \leq 10^6$, whereas its famous rival yields 261081 primes in this range.

It has been shown that no polynomial of the form $n^2 + n + q$, with q a prime, can do better than the Euler polynomial in giving primes for successive values of n. Indeed, until fairly recently no other quadratic polynomial of any kind was known to produce more than 40 successive prime values. The polynomial

$$h(n) = 103n^2 - 3945n + 34381$$

found in 1988, produces 43 distinct prime values for $n = 0, 1, 2, \ldots, 42$. The current record holder in this regard

$$k(n) = 36n^2 - 810n + 2753$$

does slightly better by giving a string of 45 prime values.

The failure of the previous functions to be prime-producing is no accident, for it is easy to prove that there is no nonconstant polynomial $f(n)$ with integral

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

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

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. Because 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 brackets indicate the greatest integer function). Needless to say, this is strictly an existence theorem and nothing is known about the actual value of r. Mills's function does not produce all the primes.

PROBLEMS 3.3

1. Verify that the integers 1949 and 1951 are twin primes.
2. (a) If 1 is added to a product of twin primes, prove that a perfect square is always obtained.
   (b) Show that the sum of twin primes p and $p + 2$ is divisible by 12, provided that $p > 3$.
3. Find all pairs of primes p and q satisfying $p - q = 3$.
4. Sylvester (1896) rephrased the Goldbach conjecture: Every even integer $2n$ greater than 4 is the sum of two primes, one larger than $n/2$ and the other less than $3n/2$. Verify this version of the conjecture for all even integers between 6 and 76.
5. In 1752, Goldbach submitted the following conjecture to Euler: Every odd integer can be written in the form $p + 2a^2$, where p is either a prime or 1 and $a \geq 0$. Show that the integer 5777 refutes this conjecture.
6. Prove that the Goldbach conjecture that every even integer greater than 2 is the sum of two primes is equivalent to the statement that every integer greater than 5 is the sum of three primes.
   [*Hint:* If $2n - 2 = p_1 + p_2$, then $2n = p_1 + p_2 + 2$ and $2n + 1 = p_1 + p_2 + 3$.]
7. A conjecture of Lagrange (1775) asserts that every odd integer greater than 5 can be written as a sum $p_1 + 2p_2$, where p_1, p_2 are both primes. Confirm this for all odd integers through 75.
8. Given a positive integer n, it can be shown that there exists an even integer a that is representable as the sum of two odd primes in n different ways. Confirm that the integers

60, 78, and 84 can be written as the sum of two primes in six, seven, and eight ways, respectively.

9. (a) For $n > 3$, show that the integers n, $n+2$, $n+4$ cannot all be prime.
(b) Three integers p, $p+2$, $p+6$, which are all prime, are called a *prime-triplet*. Find five sets of prime-triplets.

10. Establish that the sequence

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

produces n consecutive composite integers for $n > 2$.

11. Find the smallest positive integer n for which the function $f(n) = n^2 + n + 17$ is composite. Do the same for the functions $g(n) = n^2 + 21n + 1$ and $h(n) = 3n^2 + 3n + 23$.

12. Let p_n denote the nth prime number. For $n \geq 3$, prove that $p_{n+3}^2 < p_n p_{n+1} p_{n+2}$.
[*Hint:* Note that $p_{n+3}^2 < 4p_{n+2}^2 < 8p_{n+1}p_{n+2}$.]

13. Apply the same method of proof as in Theorem 3.6 to show that there are infinitely many primes of the form $6n+5$.

14. Find a prime divisor of the integer $N = 4(3 \cdot 7 \cdot 11) - 1$ of the form $4n+3$. Do the same for $N = 4(3 \cdot 7 \cdot 11 \cdot 15) - 1$.

15. Another unanswered question is whether there exist an infinite number of sets of five consecutive odd integers of which four are primes. Find five such sets of integers.

16. Let the sequence of primes, with 1 adjoined, be denoted by $p_0 = 1$, $p_1 = 2$, $p_2 = 3$, $p_3 = 5, \ldots$. For each $n \geq 1$, it is known that there exists a suitable choice of coefficients $\epsilon_k = \pm 1$ such that

$$p_{2n} = p_{2n-1} + \sum_{k=0}^{2n-2} \epsilon_k p_k \qquad p_{2n+1} = 2p_{2n} + \sum_{k=0}^{2n-1} \epsilon_k p_k$$

To illustrate:

$$13 = 1 + 2 - 3 - 5 + 7 + 11$$

and

$$17 = 1 + 2 - 3 - 5 + 7 - 11 + 2 \cdot 13$$

Determine similar representations for the primes 23, 29, 31, and 37.

17. In 1848, de Polignac claimed that every odd integer is the sum of a prime and a power of 2. For example, $55 = 47 + 2^3 = 23 + 2^5$. Show that the integers 509 and 877 discredit this claim.

18. (a) If p is a prime and $p \nmid b$, prove that in the arithmetic progression

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

every pth term is divisible by p.
[*Hint:* Because $\gcd(p, b) = 1$, there exist integers r and s satisfying $pr + bs = 1$. Put $n_k = kp - as$ for $k = 1, 2, \ldots$ and show that $p \mid (a + n_k b)$.]
(b) From part (a), conclude that if b is an odd integer, then every other term in the indicated progression is even.

19. In 1950, it was proved that any integer $n > 9$ can be written as a sum of distinct odd primes. Express the integers 25, 69, 81, and 125 in this fashion.

20. If p and $p^2 + 8$ are both prime numbers, prove that $p^3 + 4$ is also prime.

21. (a) For any integer $k > 0$, establish that the arithmetic progression

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

where $\gcd(a, b) = 1$, contains k consecutive terms that are composite.
[*Hint:* Put $n = (a + b)(a + 2b) \cdots (a + kb)$ and consider the k terms $a + (n + 1)b$, $a + (n + 2)b, \ldots, a + (n + k)b$.]

(b) Find five consecutive composite terms in the arithmetic progression

$$6, 11, 16, 21, 26, 31, 36, \ldots$$

22. Show that 13 is the largest prime that can divide two successive integers of the form $n^2 + 3$.

23. (a) The arithmetic mean of the twin primes 5 and 7 is the triangular number 6. Are there any other twin primes with a triangular mean?

(b) The arithmetic mean of the twin primes 3 and 5 is the perfect square 4. Are there any other twin primes with a square mean?

24. Determine all twin primes p and $q = p + 2$ for which $pq - 2$ is also prime.

25. Let p_n denote the nth prime. For $n > 3$, show that

$$p_n < p_1 + p_2 + \cdots + p_{n-1}$$

[*Hint:* Use induction and the Bertrand conjecture.]

26. Verify the following:

(a) There exist infinitely many primes ending in 33, such as 233, 433, 733, 1033, ...
[*Hint:* Apply Dirichlet's theorem.]

(b) There exist infinitely many primes that do not belong to any pair of twin primes.
[*Hint:* Consider the arithmetic progression $21k + 5$ for $k = 1, 2, \ldots$.]

(c) There exists a prime ending in as many consecutive 1's as desired.
[*Hint:* To obtain a prime ending in n consecutive 1's, consider the arithmetic progression $10^n k + R_n$ for $k = 1, 2, \ldots$.]

(d) There exist infinitely many primes that contain but do not end in the block of digits 123456789.
[*Hint:* Consider the arithmetic progression $10^{11}k + 1234567891$ for $k = 1, 2, \ldots$.]

27. Prove that for every $n \geq 2$ there exists a prime p with $p \leq n < 2p$.
[*Hint:* In the case where $n = 2k + 1$, then by the Bertrand conjecture there exists a prime p such that $k < p < 2k$.]

28. (a) If $n > 1$, show that $n!$ is never a perfect square.

(b) Find the values of $n \geq 1$ for which

$$n! + (n + 1)! + (n + 2)!$$

is a perfect square.
[*Hint:* Note that $n! + (n + 1)! + (n + 2)! = n!(n + 2)^2$.]

Carl Friedrich Gauss
(1777–1855)

(*Dover Publications, Inc.*)

Gauss was one of those remarkable infant prodigies whose natural aptitude for mathematics soon becomes apparent. As a child of age three, according to a well-authenticated story, he corrected an error in his father's payroll calculations. His arithmetical powers so overwhelmed his schoolmasters that, by the time Gauss was 7 years old, they admitted that there was nothing more they could teach the boy. It is said that in his first arithmetic class Gauss astonished his teacher by instantly solving what was intended to be a "busy work" problem: Find the sum of all the numbers from 1 to 100. The young Gauss later confessed to having recognized the pattern

$$1 + 100 = 101, 2 + 99 = 101, 3 + 98 = 101, \ldots, 50 + 51 = 101$$

Because there are 50 pairs of numbers, each of which adds up to 101, the sum of all the numbers must be $50 \cdot 101 = 5050$. This technique provides another way of deriving the formula

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$$

for the sum of the first n positive integers. One need only display the consecutive integers 1 through n in two rows as follows:

$$\begin{array}{ccccccc} 1 & 2 & 3 & \cdots & n-1 & n \\ n & n-1 & n-2 & \cdots & 2 & 1 \end{array}$$

Addition of the vertical columns produces n terms, each of which is equal to $n + 1$; when these terms are added, we get the value $n(n + 1)$. Because the same sum is obtained on adding the two rows horizontally, what occurs is the formula $n(n + 1) = 2(1 + 2 + 3 + \cdots + n)$.

Gauss went on to a succession of triumphs, each new discovery following on the heels of a previous one. The problem of constructing regular polygons with only "Euclidean tools," that is to say, with ruler and compass alone, had long been laid aside in the belief that the ancients had exhausted all the possible constructions. In 1796, Gauss showed that the 17-sided regular polygon is so constructible, the first

advance in this area since Euclid's time. Gauss' doctoral thesis of 1799 provided a rigorous proof of the Fundamental Theorem of Algebra, which had been stated first by Girard in 1629 and then proved imperfectly by d'Alembert (1746), and later by Euler (1749). The theorem (it asserts that a polynomial equation of degree n has exactly n complex roots) was always a favorite of Gauss', and he gave, in all, four distinct demonstrations of it. The publication of *Disquisitiones Arithmeticae* in 1801 at once placed Gauss in the front rank of mathematicians.

The most extraordinary achievement of Gauss was more in the realm of theoretical astronomy than of mathematics. On the opening night of the 19th century, January 1, 1801, the Italian astronomer Piazzi discovered the first of the so-called minor planets (planetoids or asteroids), later called Ceres. But after the course of this newly found body—visible only by telescope—passed the sun, neither Piazzi nor any other astronomer could locate it again. Piazzi's observations extended over a period of 41 days, during which the orbit swept out an angle of only nine degrees. From the scanty data available, Gauss was able to calculate the orbit of Ceres with amazing accuracy, and the elusive planet was rediscovered at the end of the year in almost exactly the position he had forecasted. This success brought Gauss worldwide fame, and led to his appointment as director of Göttingen Observatory.

By the middle of the 19th century, mathematics had grown into an enormous and unwieldy structure, divided into a large number of fields in which only the specialist knew his way. Gauss was the last complete mathematician, and it is no exaggeration to say that he was in some degree connected with nearly every aspect of the subject. His contemporaries regarded him as Princeps Mathematicorum (Prince of Mathematicians), on a par with Archimedes and Isaac Newton. This is revealed in a small incident: On being asked who was the greatest mathematician in Germany, Laplace answered, "Why, Pfaff." When the questioner indicated that he would have thought Gauss was, Laplace replied, "Pfaff is by far the greatest in Germany, but Gauss is the greatest in all Europe."

Although Gauss adorned every branch of mathematics, he always held number theory in high esteem and affection. He insisted that, "Mathematics is the Queen of the Sciences, and the theory of numbers is the Queen of Mathematics."

4.2 BASIC PROPERTIES OF CONGRUENCE

In the first chapter of *Disquisitiones Arithmeticae*, Gauss introduces the concept of congruence and the notation that makes it such a powerful technique (he explains that he was induced to adopt the symbol $\equiv$ because of the close analogy with algebraic equality). According to Gauss, "If a number n measures the difference between two numbers a and b, then a and b are said to be congruent with respect to n; if not, incongruent." Putting this into the form of a definition, we have Definition 4.1.

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

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

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

It is to be noted that any two integers are congruent modulo 1, whereas two integers are congruent modulo 2 when they are both even or both odd. Inasmuch as congruence modulo 1 is not particularly interesting, the usual practice is to assume that $n > 1$.

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

$$a = qn + r \qquad 0 \le r < n$$

Then, by definition of congruence, $a \equiv r \pmod n$. Because 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 nonnegative 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

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

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. We shall need this fact later.

Our first theorem provides a useful characterization of congruence modulo n in terms of remainders upon division by 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; that is, $b = qn + r$, where $0 \le r < n$. 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 $(0 \le r < n)$. 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, we have $a \equiv b \pmod n$.

Example 4.1. Because the integers -56 and -11 can be expressed in the form

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

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

$$-31 = (-5)7 + 4 \qquad 11 = 1 \cdot 7 + 4$$

Congruence may be viewed as a generalized form of equality, in the sense that its behavior with respect to addition and multiplication is reminiscent of ordinary equality. Some of the elementary properties of equality that carry over to congruences appear in the next theorem.

Theorem 4.2. Let $n > 1$ be fixed and a, b, c, d be arbitrary integers. Then the following properties hold:

(a) $a \equiv a \pmod n$.
(b) If $a \equiv b \pmod n$, then $b \equiv a \pmod n$.
(c) If $a \equiv b \pmod n$ and $b \equiv c \pmod n$, then $a \equiv c \pmod n$.
(d) If $a \equiv b \pmod n$ and $c \equiv d \pmod n$, then $a + c \equiv b + d \pmod n$ and $ac \equiv bd \pmod n$.
(e) If $a \equiv b \pmod n$, then $a + c \equiv b + c \pmod n$ and $ac \equiv bc \pmod n$.
(f) 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 because $-k$ is an integer, this yields property (b).

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

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

which is $a \equiv c \pmod n$ in congruence notation.

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, we obtain

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

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

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

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

The proof of property (e) is covered by (d) and the fact that $c \equiv c \pmod n$. Finally, we obtain property (f) by making an induction argument. The statement certainly holds for $k = 1$, and we will assume it is true for some fixed k. From (d), 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 $k+1$, and so the induction step is complete.

Before going further, we should illustrate that congruences can be a great help in carrying out certain types of computations.

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(f); 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 (b) and (e) 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.

Example 4.3. For another example in the same spirit, suppose that we are asked to find the remainder obtained upon dividing the sum

$$1! + 2! + 3! + 4! + \cdots + 99! + 100!$$

by 12. Without the aid of congruences this would be an awesome calculation. The observation that starts us off is that $4! \equiv 24 \equiv 0 \pmod{12}$; thus, for $k \geq 4$,

$$k! \equiv 4! \cdot 5 \cdot 6 \cdots k \equiv 0 \cdot 5 \cdot 6 \cdots k \equiv 0 \pmod{12}$$

In this way, we find that

$$\begin{aligned} 1! + 2! + 3! + 4! + \cdots + 100! \\ \equiv 1! + 2! + 3! + 0 + \cdots + 0 \equiv 9 \pmod{12} \end{aligned}$$

Accordingly, the sum in question leaves a remainder of 9 when divided by 12.

In Theorem 4.1 we saw that if $a \equiv b \pmod{n}$, then $ca \equiv cb \pmod{n}$ for any integer c. The converse, however, fails to hold. As an example, perhaps as simple as any, note that $2 \cdot 4 \equiv 2 \cdot 1 \pmod{6}$, whereas $4 \not\equiv 1 \pmod{6}$. In brief: One cannot unrestrictedly cancel a common factor in the arithmetic of congruences.

With suitable precautions, cancellation can be allowed; one step in this direction, and an important one, is provided by the following theorem.

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 canceled, the net result is

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

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

Theorem 4.3 gets its maximum force when the requirement that $\gcd(c, n) = 1$ is added, for then the cancellation may be accomplished without a change in modulus.

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

We take a moment to record a special case of Corollary 1 that we shall have frequent occasion to use, namely, Corollary 2.

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, $3 \cdot 11 \equiv 3 \cdot 5 \pmod{9}$. Because $\gcd(3, 9) = 3$, Theorem 4.3 leads to the conclusion that $11 \equiv 5 \pmod{3}$. A further illustration is given 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 the factor 5 to obtain a correct congruence $-7 \equiv 9 \pmod{8}$.

Let us call attention to the fact that, in Theorem 4.3, it is unnecessary to stipulate that $c \not\equiv 0 \pmod{n}$. Indeed, if $c \equiv 0 \pmod{n}$, then $\gcd(c, n) = n$ and the conclusion of the theorem would state that $a \equiv b \pmod{1}$; but, as we remarked earlier, this holds trivially for all integers a and b.

There is another curious situation that can arise with congruences: The product of two integers, neither of which is congruent to zero, may turn out to be congruent to zero. For instance, $4 \cdot 3 \equiv 0 \pmod{12}$, but $4 \not\equiv 0 \pmod{12}$ and $3 \not\equiv 0 \pmod{12}$. It is a simple matter to show that if $ab \equiv 0 \pmod{n}$ and $\gcd(a, n) = 1$, then $b \equiv 0 \pmod{n}$: Corollary 1 permits us legitimately to cancel the factor a from both sides of the congruence $ab \equiv a \cdot 0 \pmod{n}$. A variation on this is that when $ab \equiv 0 \pmod{p}$, with p a prime, then either $a \equiv 0 \pmod{p}$ or $b \equiv 0 \pmod{p}$.

PROBLEMS 4.2

1. Prove each of the following assertions:
   (a) If $a \equiv b \pmod{n}$ and $m \mid n$, then $a \equiv b \pmod{m}$.
   (b) If $a \equiv b \pmod{n}$ and $c > 0$, then $ca \equiv cb \pmod{cn}$.
   (c) If $a \equiv b \pmod{n}$ and the integers a, b, n are all divisible by $d > 0$, then $a/d \equiv b/d \pmod{n/d}$.
2. Give an example to show that $a^2 \equiv b^2 \pmod{n}$ need not imply that $a \equiv b \pmod{n}$.
3. If $a \equiv b \pmod{n}$, prove that $\gcd(a, n) = \gcd(b, n)$.
4. (a) Find the remainders when 2^{50} and 41^{65} are divided by 7.
   (b) What is the remainder when the following sum is divided by 4?

$$1^5 + 2^5 + 3^5 + \cdots + 99^5 + 100^5$$

5. Prove that the integer $53^{103} + 103^{53}$ is divisible by 39, and that $111^{333} + 333^{111}$ is divisible by 7.

6. For $n \geq 1$, use congruence theory to establish each of the following divisibility statements:
   (a) $7 \mid 5^{2n} + 3 \cdot 2^{5n-2}$.
   (b) $13 \mid 3^{n+2} + 4^{2n+1}$.
   (c) $27 \mid 2^{5n+1} + 5^{n+2}$.
   (d) $43 \mid 6^{n+2} + 7^{2n+1}$.
7. For $n \geq 1$, show that

$$(-13)^{n+1} \equiv (-13)^n + (-13)^{n-1} \pmod{181}$$

   [*Hint:* Notice that $(-13)^2 \equiv -13 + 1 \pmod{181}$; use induction on n.]
8. Prove the assertions below:
   (a) If a is an odd integer, then $a^2 \equiv 1 \pmod 8$.
   (b) For any integer a, $a^3 \equiv 0$, 1, or 6 (mod 7).
   (c) For any integer a, $a^4 \equiv 0$ or 1 (mod 5).
   (d) If the integer a is not divisible by 2 or 3, then $a^2 \equiv 1 \pmod{24}$.
9. If p is a prime satisfying $n < p < 2n$, show that

$$\binom{2n}{n} \equiv 0 \pmod p$$

10. If $a_1, a_2, \ldots, a_n$ is a complete set of residues modulo n and $\gcd(a, n) = 1$, prove that $aa_1, aa_2, \ldots, aa_n$ is also a complete set of residues modulo n.
    [*Hint:* It suffices to show that the numbers in question are incongruent modulo n.]
11. Verify that $0, 1, 2, 2^2, 2^3, \ldots, 2^9$ form a complete set of residues modulo 11, but that $0, 1^2, 2^2, 3^2, \ldots, 10^2$ do not.
12. Prove the following statements:
    (a) If $\gcd(a, n) = 1$, then the integers

$$c, c + a, c + 2a, c + 3a, \ldots, c + (n - 1)a$$

    form a complete set of residues modulo n for any c.
    (b) Any n consecutive integers form a complete set of residues modulo n.
    [*Hint:* Use part (a).]
    (c) The product of any set of n consecutive integers is divisible by n.
13. Verify that if $a \equiv b \pmod{n_1}$ and $a \equiv b \pmod{n_2}$, then $a \equiv b \pmod n$, where the integer $n = \text{lcm}(n_1, n_2)$. Hence, whenever n_1 and n_2 are relatively prime, $a \equiv b \pmod{n_1 n_2}$.
14. Give an example to show that $a^k \equiv b^k \pmod n$ and $k \equiv j \pmod n$ need not imply that $a^j \equiv b^j \pmod n$.
15. Establish that if a is an odd integer, then for any $n \geq 1$

$$a^{2^n} \equiv 1 \pmod{2^{n+2}}$$

    [*Hint:* Proceed by induction on n.]
16. Use the theory of congruences to verify that

$$89 \mid 2^{44} - 1 \qquad \text{and} \qquad 97 \mid 2^{48} - 1$$

17. Prove that whenever $ab \equiv cd \pmod n$ and $b \equiv d \pmod n$, with $\gcd(b, n) = 1$, then $a \equiv c \pmod n$.
18. If $a \equiv b \pmod{n_1}$ and $a \equiv c \pmod{n_2}$, prove that $b \equiv c \pmod n$, where the integer $n = \gcd(n_1, n_2)$.

SATHYABAMA
INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)
Accredited "A" Grade by NAAC | 12B Status by UGC | Approved by AICTE
www.sathyabama.ac.in

SCHOOL OF SCIENCE AND HUMANITIES
DEPARTMENT OF MATHEMATICS

UNIT – III – NUMBER THEORY – SMT1554

UNIT III

FERMAT'S THEOREM

In this unit we would arrive at the divisibility tests for few integers and the statement of proof of Fermat's little theorem, Wilson's theorem and few examples that illustrate, their applications is discussed.

Any integer `*N* to a base *b* could be expressed uniquely in the form.

$$N = a_m b^m + a_{m-1} b^{m-1} + \cdots + a_2 b^2 + a_1 b + a_0$$

where the coefficients a_k can take on the b different values 0, 1, 2, ... , $b-1$. By division algorithm, $N = q_1 b + a_0, 0 \le a_0 < b$. If $q_1 \ge b$, then $q_1 = q_2 b + a_1, 0 \le a_1 < b$. On sbustituting for q_1 in the earlier equation to get

$$N = (q_2 b + a_1) b + a_0 = q_2 b^2 + a_1 b + a_0$$

Applying the process repeatedly until $q_m < b$ for some m and back substituting in the older equations we get the desired result.

$$N = a_m b^m + a_{m-1} b^{m-1} + \cdots + a_2 b^2 + a_1 b + a_0$$

To show uniqueness, let us suppose that *N* has two distinct representations, say,

$$N = a_m b^m + a_{m-1} b^{m-1} + \cdots + a_2 b^2 + a_1 b + a_0$$
$$= c_m b^m + c_{m-1} b^{m-1} + \cdots + c_2 b^2 + c_1 b + c_0$$

with $0 \le a_i < b$ for each *i* and $0 \le c_j < b$ for each *j*. Subtracting the second representation from the first gives the equation

$$d_m b^m + d_{m-1} b^{m-1} + \cdots + d_2 b^2 + d_1 b + d_0 = 0$$

where $d_i = a_i - c_i$; for $i = 0, 1, \ldots, m$. Because the two representations for *N* are assumed to be different, we must have $d_i \neq 0$ for some value of *i*. Take *k* to be the smallest subscript for which $d_k \neq 0$. Then $d_k b^k + d_{k+1} b^{k+1} + \cdots + d_m b^m = 0$and so, after dividing by b^k,

$$d_k = -b(d_m b^{m-k-1} + \cdots + d_{k+1}$$

Hence, $b|d_k$. But, $0 \le a_k < b$ and $0 \le c_k < b$ implies $-b < -c_k \le 0$. Combining the two inequalities we get $-b < a_k - c_k < b$, or $|d_k| < b$. As $b|d_k$ the only possibility is that $d_k = 0$, which is impossible. This contradiction, guaranties that the representation of *N* is unique.

From the above theorem it is evident that the integer *N* is completely determined by the ordered array $a_m, a_{m-1}, \ldots, a_1, a_0$ of coefficients, with the plus signs and the powers of b being superfluous. Thus, the number $N = a_m b^m + a_{m-1} b^{m-1} + \cdots + a_2 b^2 + a_1 b + a_0$ may be denoted by $N(a_m a_{m-1} \ldots a_1 a_0)_b$ and is known as the *base b place-value notation for N*. When the base b = 2, and the resulting system of enumeration is called the *binary number system*.

Theorem 3.1.

Let $P(x) = \sum_{k=0}^{m} c_k x^k$ be a polynomial function of *x* with integral coefficients c_k. If $a \equiv b (mod\ n)$, then $P(a) \equiv P(b)\ (mod\ n)$.

Proof.

Given $a \equiv b(mod\ n)$. Hence $a^k \equiv b^k(mod\ n)$ for $k = 0,1,\dots,m$. Multiplying both sides by c_k and adding these *m*+1 congruences, we get $\sum_{k=0}^{m} c_k a^k \equiv \sum_{k=0}^{m} c_k b^k\ (mod\ n)$.
This proves that, $P(a) \equiv P(b)\ (mod\ n)$.

Definition:
If *P(x)* is a polynomial with integral coefficients, we say that *a* is a solution of the congruence $P(x) \equiv 0\ (mod\ n)$ if $P(a) \equiv 0(mod\ n)$.

Corollary
If *a* is a solution of $P(x) \equiv 0\ (mod\ n)$ and $a \equiv b\ (mod\ n)$, then *b* also is a solution.

Proof.
From the last theorem, we infer that whenever $a \equiv b(mod\ n)$ then $P(a) \equiv P(b)\ (mod\ n)$. Since, if a is a solution of $P(x) \equiv 0\ (mod\ n)$, $P(a) \equiv 0(mod\ n)$.By property of congruencies $P(b) \equiv P(a) \equiv 0\ (mod\ n)$, making *b* also a solution.
and only if the sum of the digits in its decimal representation is divisible by 9.
Theorem 3.2.
Let $N = a_m 10^m + a_{m-1}10^{m-1} + \cdots + a_0$, be the decimal expansion of the positive integer *N*, $0 \le a_k < 10$, and let $S = a_0 + a_1 + \cdots + a_m$. Then $9|N$ if and only if $9|S$.

Proof.
Let $P(x) = \sum_{k=0}^{m} a_k x^k$ be a polynomial with integral coefficients. We know that $10 \equiv 1(mod\ 9)$. By theorem 3.1, $P(10) \equiv P(1)(mod\ 9)$. From the definition of $P(x)$, $P(10) = N$ and $P(1) = S$. The above congruence reduces to the form $N \equiv S(mod\ 9)$. Hence it follows that, $N \equiv 0(mod\ 9)$ if and only if $S \equiv 0(mod\ 9)$. This proves the statement of the theorem.

Theorem 3.3
Let $N = a_m 10^m + a_{m-1}10^{m-1} + \cdots + a_0$be the decimal expansion of the positive integer *N*, $0 \le a_k < 10$, and let $T = a_0 - a_1 + \cdots + (-1)^m a_m$. Then $11|N$ if and only if $11|T$.

Proof.
Let $P(x) = \sum_{k=0}^{m} a_k x^k$ be a polynomial with integral coefficients. We know that $10 \equiv -1(mod\ 11)$. By theorem 3.1, $P(11) \equiv P(-1)(mod\ 11)$. From the definition of $P(x)$, $P(10) = N$ and $P(-1) = T$. The above congruence reduces to the form $N \equiv T(mod\ 11)$. Hence it follows that, $N \equiv 0(mod\ 11)$ if and only if $T \equiv 0(mod\ 11)$. This proves the statement of the theorem.

Practice Problems:

1. Without performing the divisions, determine whether the integers 176,521,221 and 149,235,678 are divisible by 9 or 11.
2. Give criteria for the divisibility of *N* by 3 and 8 that depend on the digits of *N* when written in the base 9.
3. Is the integer $(447836)_9$ divisible by 3 and 8?
6. Working modulo 9 or 11, find the missing digits in the calculations below:

(a) 51840 · 273581 = 1418243x040.

(b) 2x99561 = [3(523 + x)]2. (c) 2784x = *x* · 5569.

(d) 512 · 1x53125 = 1000000000.

7. Establish the following divisibility criteria:

(a) An integer is divisible by 2 if and only if its units digit is 0, 2, 4, 6, or 8.

(b) An integer is divisible by 3 if and only if the sum of its digits is divisible by 3.

(c) An integer is divisible by 4 if and only if the number formed by its tens and units digits is divisible by 4.

(d) An integer is divisible by 5 if and only if its units digit is 0 or 5.

8. Prove that no integer whose digits add up to 15 can be a square or a cube. *[Hint:* For any *a, a3* = 0, 1, or 8 (mod 9).]
9. Assuming that 495 divides *273x49y5,* obtain the digits *x* andy.

LINEAR CONGRUENCES

In this section, we would define linear congruence and obtain the solution set to the linear congruencies.

Definition.

An equation of the form $ax \equiv b\ (mod\ n)$ is called a *linear congruence,* and a solution of the congruence is an integer x_0 such that $ax_0 \equiv b(mod\ n)$.

Theorem 3.4

The linear congruence $ax \equiv b\ (mod\ n)$ has a solution if and only if *d* I *b,* where *d* = gcd(a, *n).* If *d* I *b,* then it has *d* mutually incongruent solutions modulo *n.*

Proof.

By the definition of linear congruence it is equivalent to the linear Diophantine equation *ax- ny =b.* which can be solved if and only if *d* I *b;* moreover, if it is solvable and x_0, y_0 is one specific solution, then any other solution has the form $x_0 + \frac{n}{d}t$ and $y_0 + \frac{a}{d}t$ for some integer values of t. Consider *t* = 0, 1, 2, ... , *d*- 1. The corresponding solutions to the congruencies are $x_0 + \frac{n}{d}, x_0 + \frac{2n}{d}, \dots, x_0 + \frac{(d-1)n}{d}$.

Claim (i): These solutions are incongruent modulo *n*.

Suppose that any two of the above solutions are congruent modulo *n*.

Say, $x_0 + \frac{n}{d}t_1 \equiv x_0 + \frac{n}{d}t_2(mod\ n) \Rightarrow \frac{n}{d}t_1 \equiv \frac{n}{d}t_2(mod\ n) \Rightarrow t_1 \equiv t_2(mod\ d)$.

From the above congruence it follows that $d|(t_1 - t_2)$, a contradiction as each of t_i lies between 0 and $d - 1$. Hence the d solutions above are incongruent modulo n.

Claim (ii): All other such integers *x* are congruent to some one of them.

Let $x_0 + \frac{n}{d}t, t \geq d$ be any other solution to the congruence. By division algorithm, there exists unique integers q and r such that $t = qd + r, 0 \leq r < d$. Hence, the solution takes the form $x_0 + \frac{n}{d}(qd + r) = x_0 + nq + \frac{n}{d}r$.

It follows that $x_0 + \frac{n}{d}t \equiv x_0 + \frac{n}{d}r(mod\ n)$, where $x_0 + \frac{n}{d}r$ is one of the d solutions.

This proves the statement of the theorem.

Corollary.

If gcd(a , n) = 1, then the linear congruence *ax* = *b* (mod *n*) has a unique solution modulo n.

The proof of the above statement follows obviously from the above theorem.

Note: Given relatively prime integers *a* and *n*, the congruence $ax \equiv 1(mod\ n)$ has a unique solution. This solution is called the (multiplicative) inverse of *a* modulo *n*.

FERMAT'S LITTLE THEOREM

Fermat's theorem. Let *p* be a prime and suppose that $p \nmid a$. Then $a^{P-1} \equiv 1\ (mod\ p)$.

Proof.

Considering the first $p - 1$ positive multiples $a, 2a, 3a, \ldots, (p - 1)a$ of a. These integers are mutually incongruent modulo p and incongruent to zero. On contrary, if it is true that $ra \equiv sa\ (mod\ p) 1 \leq r < s \leq p - 1$ then the common factor a could be cancelled to give $r \equiv s\ (mod\ p\ )$, which is not true as $|r - s| < p$ and hence $p \nmid (r - s)$. Therefore, the set of integers $a, 2a, 3a, \ldots, (p - 1)a$ must be congruent modulo p to $1, 2, 3, \ldots, p - 1$, taken in some order. Multiplying all these congruences together, results in

$$a \cdot 2a \cdot 3a \cdots (p - 1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p - 1)(mod\ p)$$

$$a^{P-1}(p - 1)! \equiv (p - 1)!\ (mod\ p)$$

Cancelling $(p - 1)!$ from both the sides we get

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

This proves the Fermat's theorem.

Corollary. If p is a prime, then $a^p \equiv a(mod\ p)$ for any integer a.

Proof. If $p|a$, then $p|a^p$ implies $a^p \equiv 0 \equiv a\ (mod\ p)$. If $p \nmid a$ then by Fermat's theorem, we have $a^{p-1} \equiv 1(mod\ p)$. Multiplying this congruence by a we get the desired result $a^p \equiv a(mod\ p)$.

Lemma.

If *p* and *q* are distinct primes with $a^p \equiv a\ (mod\ q)$ and $a^q \equiv a\ (mod\ p)$, then $a^{pq} \equiv a\ (mod\ pq)$.

Proof:

From the previous corollary it follows that for any integer a^q, $(a^q)^p \equiv a^q (mod\ p)$. It is given that $a^q \equiv a(mod\ p)$. By property of congruencies $a^{pq} \equiv a(mod\ p)$. From this we infer that $p|(a^{pq} - a)$. Similarly it could be proved that $q|(a^{pq} - a)$. It clearly follows that $pq|(a^{pq} - a)$. This could be equivalently expressed as $a^{pq} \equiv a\ (mod\ pq)$.

Definition

A composite integer n is called pseudoprime whenever $n|2^n - 2$. In general, a composite integer n for which $a^n \equiv a\ (mod\ n)$ is called a pseudoprime to the base a.

Theorem:

If n is an odd pseudoprime, then $M_n \equiv 2^n - 1$ is a larger one.

Proof.

As n is a composite number, it could be expressed as $n = rs$, with $1 < r \leq s < n$. Hence, $2^r - 1|2^n - 1 \Rightarrow 2^r - 1|M_n$. This guarantees that M_n composite. Since n is pseudo prime, $2^n \equiv 2\ (mod\ n) \Rightarrow 2^n - 2 = kn$ for some integer k.

Hence, $2^{M_n - 1} = 2^{(2^n - 1) - 1} = 2^{2^n - 2} = 2^{kn}$.

It follows that $2^{M_n - 1} - 1 = 2^{kn} - 1 = (2^n - 1)\left(2^{n(k-1)} + 2^{n(k-2)} + \cdots + 2^n + 1\right) \Rightarrow 2^{M_n - 1} - 1 = M_n\left(2^{n(k-1)} + 2^{n(k-2)} + \cdots + 2^n + 1\right)$ and hence $2^{M_n - 1} \equiv 0(mod\ M_n) \Rightarrow M_n|(2^{M_n} - 2)$. This proves that M_n is a pseudoprime.

Definition:

Composite numbers n that are pseudoprimes to every base a are called absolute pseudo primes or Carmichael numbers.

Theorem

Let *n* be a composite square-free integer, say, $n = p_1 p_2 \cdots p_r$ where the p_i are distinct primes. If $P_i - 1|n - 1$ for *i* = 1, 2, ... , *r,* then *n* is an absolute pseudoprime.

Proof.

Suppose that *a* is an integer satisfying gcd(a, *n)* = 1, so that gcd(a, P_i)= 1 for each *i.* Then by Fermat's theorem $P_i|a^{p_i - 1} - 1$. From the divisibility hypothesis $P_i - 1|n - 1$, we have $P_i|a^{n-1} - 1$, and therefore $P_i|a^n - a$ for all a and *i* = 1, 2, ... , *r.* Hence, $n|a^n - a$, which makes *n* an absolute pseudo prime.

WILSON'S THEOREM

If p is a prime, then $(p - 1)! \equiv -1(mod\ p)$.

Proof.

The statement can be easily observed to be true for the cases $p = 2$ and $p = 3$. Consider $p > 3$. Suppose that a is any one of the $p - 1$ positive integers $1, 2, 3, \ldots, p - 1$.

Consider the linear congruence $ax \equiv 1(mod\ p)$. As $gcd(a, p) = 1$, the congruence has a unique solution modulo p; hence, there is a unique integer a', with $1 \leq a' \leq p - 1$, satisfying $aa' \equiv 1(mod\ p)$.

Because p is prime, $a = a' \Rightarrow a^2 = 1(mod\ p)$ is equivalent to $(a - 1)(a + 1) = 0(mod\ p)$. Therefore, either $a - 1 \equiv (mod\ p)$, in which case $a = 1$, or $a + 1 \equiv 0(mod\ p)$, in which case $a = p - 1$.

Omitting 1 and $p - 1$, and grouping the remaining integers $2, 3, \ldots, p - 2$ into pairs a, a', where $a \neq a'$, such that their product $aa' \equiv 1\ (mod\ p\ )$. Multiplying these $\frac{p-3}{2}$ congruencies together and rearranging the factors, we get

$$2 \cdot 3 \cdots (p - 2) \equiv 1(mod\ p)$$

$$(p - 2)! \equiv 1\ (mod\ p)$$

Now multiply by $p - 1$ from both sides

$$(p - 1)! \equiv p - 1 \equiv -1\ (mod\ p)$$

Hence the Wilson's theorem is proved.

SATHYABAMA
INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)
Accredited "A" Grade by NAAC | 12B Status by UGC | Approved by AICTE
www.sathyabama.ac.in

SCHOOL OF SCIENCE AND HUMANITIES

DEPARTMENT OF MATHEMATICS

UNIT – IV – NUMBER THEORY – SMT1554

SMT1554 - NUMBER THEORY

UNIT-4 Number Theoretic Functions

THE SUM AND NUMBER OF DIVISORS

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*. Although 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, and 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 $n = 12$. Because 12 has the positive divisors 1, 2, 3, 4, 6, 12, we find that

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

For the first few integers,

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

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, $\sigma(n) = n + 1$ if and only if n is a prime.

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

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

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

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

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

$$\tau(n) = \sum_{d \mid n} 1 \qquad \sigma(n) = \sum_{d \mid n} d$$

The notation $\sum_{d \mid n} 1$, 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

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

and

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

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 $d = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ $(0 \le a_i \le k_i)$ 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 $k_i - a_i \ge 0$ 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 $0 \le a_i \le k_i$. There are $k_1 + 1$ choices for the exponent a_1; $k_2 + 1$ choices for $a_2, \ldots$; and $k_r + 1$ choices for a_r. Hence, there are

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

possible divisors of n.

To evaluate $\sigma(n)$, consider the product

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

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, the notation for products may be defined using $\prod$, 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

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

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

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

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 $a_1 = 0, 1, 2$; $a_2 = 0, 1, 2$; and $a_3 = 0, 1$. 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 $\tau(n)$ positive divisors of n, $\tau(n)$ such equations occur. Multiplying these together, we get

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

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

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

or equivalently

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

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, Section 6.1), 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

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

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

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

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.

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, we 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 that 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; because 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 that 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 canceled 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. Because the result is trivially true if either m or n is equal to 1, we may assume that $m > 1$ and $n > 1$. If

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

are the prime factorizations of m and n, then because $\gcd(m, n) = 1$, 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_1d_2, where $d_1 \mid m$, $d_2 \mid n$ 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

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

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. Because no p_i is equal to any q_j, we surely must have $\gcd(d_1, d_2) = 1$.

A keystone in much of our subsequent work is Theorem 6.4.

Theorem 6.4. If f is a multiplicative function and F is defined by

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

then F is also multiplicative.

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

$$\begin{aligned} F(mn) &= \sum_{d \mid mn} f(d) \\ &= \sum_{\substack{d_1 \mid m \\ d_2 \mid n}} f(d_1 d_2) \end{aligned}$$

because 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

$$\begin{aligned} F(mn) &= \sum_{\substack{d_1 \mid m \\ d_2 \mid n}} f(d_1) f(d_2) \\ &= \left(\sum_{d_1 \mid m} f(d_1) \right) \left(\sum_{d_2 \mid n} f(d_2) \right) \\ &= F(m) F(n) \end{aligned}$$

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

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

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 that the constant function $f(n) = 1$ is multiplicative, as is the identity function $f(n) = n$. Because τ and σ may be represented in the form

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

the stated result follows immediately from Theorem 6.4.

PROBLEMS 6.1

1. Let m and n be positive integers and $p_1, p_2, \ldots, p_r$ be the distinct primes that 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

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

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 the result of Problem 1 to calculate $\gcd(12378, 3054)$ and $\operatorname{lcm}(12378, 3054)$.

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

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

5. (a) Verify that $\tau(n) = \tau(n+1) = \tau(n+2) = \tau(n+3)$ holds for $n = 3655$ and 4503.
(b) When $n = 14$, 206, and 957, show that $\sigma(n) = \sigma(n+1)$.

6. For any integer $n \geq 1$, establish the inequality $\tau(n) \leq 2\sqrt{n}$.
[*Hint:* If $d \mid n$, then one of d or n/d is less than or equal to $\sqrt{n}$.]

7. Prove the following.
(a) $\tau(n)$ is an odd integer if and only if n is a perfect square.
(b) $\sigma(n)$ is an odd integer if and only if n is a perfect square or twice a perfect square.
[*Hint:* If p is an odd prime, then $1 + p + p^2 + \cdots + p^k$ is odd only when k is even.]

8. Show that $\sum_{d \mid n} 1/d = \sigma(n)/n$ for every positive integer n.

9. If n is a square-free integer, prove that $\tau(n) = 2^r$, where r is the number of prime divisors of n.

10. Establish the assertions below:
(a) If $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ is the prime factorization of $n > 1$, then

$$1 > \frac{n}{\sigma(n)} > \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right)$$

(b) For any positive integer n,

$$\frac{\sigma(n!)}{n!} \geq 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$$

[*Hint:* See Problem 8.]
(c) If $n > 1$ is a composite number, then $\sigma(n) > n + \sqrt{n}$.
[*Hint:* Let $d \mid n$, where $1 < d < n$, so $1 < n/d < n$. If $d \leq \sqrt{n}$, then $n/d \geq \sqrt{n}$.]

11. Given a positive integer $k > 1$, show that there are infinitely many integers n for which $\tau(n) = k$, but at most finitely many n with $\sigma(n) = k$.
[*Hint:* Use Problem 10(a).]

12. (a) Find the form of all positive integers n satisfying $\tau(n) = 10$. What is the smallest positive integer for which this is true?
(b) Show that there are no positive integers n satisfying $\sigma(n) = 10$.
[*Hint:* Note that for $n > 1$, $\sigma(n) > n$.]

13. Prove that there are infinitely many pairs of integers m and n with $\sigma(m^2) = \sigma(n^2)$.
[*Hint:* Choose k such that $\gcd(k\,, 10) = 1$ and consider the integers $m = 5k$, $n = 4k$.]

14. For $k \geq 2$, show each of the following:
(a) $n = 2^{k-1}$ satisfies the equation $\sigma(n) = 2n - 1$.
(b) If $2^k - 1$ is prime, then $n = 2^{k-1}(2^k - 1)$ satisfies the equation $\sigma(n) = 2n$.
(c) If $2^k - 3$ is prime, then $n = 2^{k-1}(2^k - 3)$ satisfies the equation $\sigma(n) = 2n + 2$.
It is not known if there are any positive integers n for which $\sigma(n) = 2n + 1$.

15. If n and $n + 2$ are a pair of twin primes, establish that $\sigma(n + 2) = \sigma(n) + 2$; this also holds for $n = 434$ and 8575.

16. (a) For any integer $n > 1$, prove that there exist integers n_1 and n_2 for which $\tau(n_1) + \tau(n_2) = n$.
(b) Prove that the Goldbach conjecture implies that for each even integer $2n$ there exist integers n_1 and n_2 with $\sigma(n_1) + \sigma(n_2) = 2n$.

17. For a fixed integer k, show that the function f defined by $f(n) = n^k$ is multiplicative.

18. Let f and g be multiplicative functions that are not identically zero and such that $f(p^k) = g(p^k)$ for each prime p and $k \geq 1$. Prove that $f = g$.

19. Prove that if f and g are multiplicative functions, then so is their product fg and quotient f/g (whenever the latter function is defined).

20. Let $\omega(n)$ denote the number of distinct prime divisors of $n > 1$, with $\omega(1) = 0$. For instance, $\omega(360) = \omega(2^3 \cdot 3^2 \cdot 5) = 3$.
(a) Show that $2^{\omega(n)}$ is a multiplicative function.
(b) For a positive integer n, establish the formula

$$\tau(n^2) = \sum_{d \mid n} 2^{\omega(d)}$$

21. For any positive integer n, prove that $\sum_{d \mid n} \tau(d)^3 = (\sum_{d \mid n} \tau(d))^2$.
[*Hint:* Both sides of the equation in question are multiplicative functions of n, so that it suffices to consider the case $n = p^k$, where p is a prime.]

22. Given $n \geq 1$, let $\sigma_s(n)$ denote the sum of the sth powers of the positive divisors of n; that is,

$$\sigma_s(n) = \sum_{d \mid n} d^s$$

Verify the following:
(a) $\sigma_0 = \tau$ and $\sigma_1 = \sigma$.
(b) σ_s is a multiplicative function.
[*Hint:* The function f, defined by $f(n) = n^s$, is multiplicative.]
(c) If $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ is the prime factorization of n, then

$$\sigma_s(n) = \left(\frac{p_1^{s(k_1+1)} - 1}{p_1^s - 1}\right)\left(\frac{p_2^{s(k_2+1)} - 1}{p_2^s - 1}\right) \cdots \left(\frac{p_r^{s(k_r+1)} - 1}{p_r^s - 1}\right)$$

23. For any positive integer n, show the following:
(a) $\sum_{d \mid n} \sigma(d) = \sum_{d \mid n} (n/d)\tau(d)$.
(b) $\sum_{d \mid n} (n/d)\sigma(d) = \sum_{d \mid n} d\tau(d)$.
[*Hint:* Because the functions

$$F(n) = \sum_{d \mid n} \sigma(d) \qquad \text{and} \qquad G(n) = \sum_{d \mid n} \frac{n}{d}\tau(d)$$

are both multiplicative, it suffices to prove that $F(p^k) = G(p^k)$ for any prime p.]

6.2 THE MÖBIUS INVERSION FORMULA

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

Definition 6.3. For a positive integer n, define μ by the rules

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

Put somewhat differently, Definition 6.3 states that $\mu(n) = 0$ if n is not a square-free integer, whereas $\mu(n) = (-1)^r$ if n is square-free with r prime factors. For example: $\mu(30) = \mu(2 \cdot 3 \cdot 5) = (-1)^3 = -1$. The first few values of μ are

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

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

As the reader may have guessed already, the Möbius μ-function is multiplicative. This is the content of Theorem 6.5.

Theorem 6.5. The function μ is a multiplicative function.

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

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

which completes the proof.

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

$$\sum_{d \mid 1} \mu(d) = \mu(1) = 1$$

Suppose that $n > 1$ and put

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

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

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

Because μ is known to be a multiplicative function, an appeal to Theorem 6.4 is legitimate; this result guarantees that F also is multiplicative. Thus, if the canonical factorization of n is $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, then $F(n)$ is the product of the values assigned to F for the prime powers in this representation:

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

We record this result as Theorem 6.6.

Theorem 6.6. For each positive integer $n \geq 1$,

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

where d runs through the positive divisors of n.

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

$$\begin{aligned} \sum_{d \mid 10} \mu(d) &= \mu(1) + \mu(2) + \mu(5) + \mu(10) \\ &= 1 + (-1) + (-1) + 1 = 0 \end{aligned}$$

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

Theorem 6.7 Möbius inversion formula. Let F and f be two number-theoretic functions related by the formula

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

Then

$$f(n) = \sum_{d \mid n} \mu(d) F\left(\frac{n}{d}\right) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) F(d)$$

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

Carrying out the required computation, we get

$$\begin{aligned}\sum_{d\mid n}\mu(d)F\left(\frac{n}{d}\right) &= \sum_{d\mid n}\left(\mu(d)\sum_{c\mid(n/d)}f(c)\right)\\ &= \sum_{d\mid n}\left(\sum_{c\mid(n/d)}\mu(d)f(c)\right)\end{aligned} \tag{1}$$

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

$$\begin{aligned}\sum_{d\mid n}\left(\sum_{c\mid(n/d)}\mu(d)f(c)\right) &= \sum_{c\mid n}\left(\sum_{d\mid(n/c)}f(c)\mu(d)\right)\\ &= \sum_{c\mid n}\left(f(c)\sum_{d\mid(n/c)}\mu(d)\right)\end{aligned} \tag{2}$$

In compliance with Theorem 6.6, the sum $\sum_{d\mid(n/c)}\mu(d)$ must vanish except when $n/c = 1$ (that is, when $n = c$), in which case it is equal to 1; the upshot is that the right-hand side of Eq. (2) simplifies to

$$\begin{aligned}\sum_{c\mid n}\left(f(c)\sum_{d\mid(n/c)}\mu(d)\right) &= \sum_{c=n}f(c)\cdot 1\\ &= f(n)\end{aligned}$$

giving us the stated result.

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

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

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

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

Theorem 6.7 tells us that these formulas may be inverted to give

$$1 = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) \tau(d) \qquad \text{and} \qquad n = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) \sigma(d)$$

which are valid for all $n \geq 1$.

Theorem 6.4 ensures that if f is a multiplicative function, then so is $F(n) = \sum_{d \mid n} f(d)$. Turning the situation around, one might ask whether the multiplicative nature of F forces that of f. Surprisingly enough, this is exactly what happens.

Theorem 6.8. If F is a multiplicative function and

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

then f is also multiplicative.

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

$$\begin{aligned} f(mn) &= \sum_{d \mid mn} \mu(d) F\left(\frac{mn}{d}\right) \\ &= \sum_{\substack{d_1 \mid m \\ d_2 \mid n}} \mu(d_1 d_2) F\left(\frac{mn}{d_1 d_2}\right) \\ &= \sum_{\substack{d_1 \mid m \\ d_2 \mid n}} \mu(d_1)\mu(d_2) F\left(\frac{m}{d_1}\right) F\left(\frac{n}{d_2}\right) \\ &= \sum_{d_1 \mid m} \mu(d_1) F\left(\frac{m}{d_1}\right) \sum_{d_2 \mid n} \mu(d_2) F\left(\frac{n}{d_2}\right) \\ &= f(m) f(n) \end{aligned}$$

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

For $n \geq 1$, we define the sum

$$M(n) = \sum_{k=1}^{n} \mu(k)$$

Then $M(n)$ is the difference between the number of square-free positive integers $k \leq n$ with an even number of prime factors and those with an odd number of prime factors. For example, $M(9) = 2 - 4 = -2$. In 1897, Franz Mertens (1840–1927) published a paper with a 50-page table of values of $M(n)$ for $n = 1, 2, \ldots, 10000$. On the basis of the tabular evidence, Mertens concluded that the inequality

$$|M(n)| < \sqrt{n} \qquad n > 1$$

is "very probable." (In the previous example, $|M(9)| = 2 < \sqrt{9}$.) This conclusion later became known as the Mertens conjecture. A computer search carried out in

1963 verified the conjecture for all n up to 10 billion. But in 1984, Andrew Odlyzko and Herman te Riele showed that the Mertens conjecture is false. Their proof, which involved the use of a computer, was indirect and produced no specific value of n for which $|M(n)| \geq \sqrt{n}$; all it demonstrated was that such a number n must exist somewhere. Subsequently, it has been shown that there is a counterexample to the Mertens conjecture for at least one $n \leq (3.21)10^{64}$.

PROBLEMS 6.2

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

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

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

2. The *Mangoldt function* Λ is defined by

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

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

3. Let $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ be the prime factorization of the integer $n > 1$. If f is a multiplicative function that is not identically zero, prove that

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

[*Hint:* By Theorem 6.4, the function F defined by $F(n) = \sum_{d \mid n} \mu(d) f(d)$ is multiplicative; hence, $F(n)$ is the product of the values $F(p_i^{k_i})$.]

4. If the integer $n > 1$ has the prime factorization $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, use Problem 3 to establish the following:
(a) $\sum_{d \mid n} \mu(d)\tau(d) = (-1)^r$.
(b) $\sum_{d \mid n} \mu(d)\sigma(d) = (-1)^r p_1 p_2 \cdots p_r$.
(c) $\sum_{d \mid n} \mu(d)/d = (1 - 1/p_1)(1 - 1/p_2) \cdots (1 - 1/p_r)$.
(d) $\sum_{d \mid n} d\mu(d) = (1 - p_1)(1 - p_2) \cdots (1 - p_r)$.

5. Let $S(n)$ denote the number of square-free divisors of n. Establish that

$$S(n) = \sum_{d \mid n} |\mu(d)| = 2^{\omega(n)}$$

where $\omega(n)$ is the number of distinct prime divisors of n.
[*Hint:* S is a multiplicative function.]

6. Find formulas for $\sum_{d \mid n} \mu^2(d)/\tau(d)$ and $\sum_{d \mid n} \mu^2(d)/\sigma(d)$ in terms of the prime factorization of n.

7. The *Liouville λ-function* is defined by $\lambda(1) = 1$ and $\lambda(n) = (-1)^{k_1 + k_2 + \cdots + k_r}$, if the prime factorization of $n > 1$ is $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$. For instance,

$$\lambda(360) = \lambda(2^3 \cdot 3^2 \cdot 5) = (-1)^{3+2+1} = (-1)^6 = 1$$

(a) Prove that λ is a multiplicative function.

(b) Given a positive integer n, verify that

$$\sum_{d \mid n} \lambda(d) = \begin{cases} 1 & \text{if } n = m^2 \text{ for some integer } m \\ 0 & \text{otherwise} \end{cases}$$

8. For an integer $n \geq 1$, verify the formulas below:
(a) $\sum_{d \mid n} \mu(d)\lambda(d) = 2^{\omega(n)}$.
(b) $\sum_{d \mid n} \lambda(n/d)2^{\omega(d)} = 1$.

6.3 THE GREATEST INTEGER FUNCTION

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

Definition 6.4. For an arbitrary real number x, we denote by $[x]$ the largest integer less than or equal to x; that is, $[x]$ is the unique integer satisfying $x - 1 < [x] \leq x$.

By way of illustration, [ ] assumes the particular values

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

The important observation to be made here is that the equality $[x] = x$ holds if and only if x is an integer. Definition 6.4 also makes plain that any real number x can be written as

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

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

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

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

so that the exact power of 3 that divides 9! is 4. It is desirable to have a formula that will give this count, without the necessity of always writing $n!$ in canonical form. This is accomplished by Theorem 6.9.

Theorem 6.9. If n is a positive integer and p a prime, then the exponent of the highest power of p that divides $n!$ is

$$\sum_{k=1}^{\infty} \left[\frac{n}{p^k} \right]$$

where the series is finite, because $[n/p^k] = 0$ for $p^k > n$.

Proof. Among the first n positive integers, those divisible by p are $p, 2p, \ldots, tp$, where t is the largest integer such that $tp \leq n$; in other words, t is the largest integer

less than or equal to n/p (which is to say $t = [n/p]$). Thus, there are exactly $[n/p]$ multiples of p occurring in the product that defines $n!$, namely,

$$p, 2p, \ldots, \left[\frac{n}{p}\right] p \tag{1}$$

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

$$p^2, 2p^2, \ldots, \left[\frac{n}{p^2}\right] p^2 \tag{2}$$

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

$$p^3, 2p^3, \ldots, \left[\frac{n}{p^3}\right] p^3 \tag{3}$$

After a finite number of repetitions of this process, we are led to conclude that the total number of times p divides $n!$ is

$$\sum_{k=1}^{\infty} \left[\frac{n}{p^k}\right]$$

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

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

Example 6.2. We would like to find the number of zeros with which the decimal representation of 50! terminates. In determining the number of times 10 enters into the product 50!, it is enough to find the exponents of 2 and 5 in the prime factorization of 50!, and then to select the smaller figure.

By direct calculation we see that

$$\begin{aligned} &[50/2] + [50/2^2] + [50/2^3] + [50/2^4] + [50/2^5] \\ &\quad = 25 + 12 + 6 + 3 + 1 \\ &\quad = 47 \end{aligned}$$

Theorem 6.9 tells us that 2^{47} divides 50!, but 2^{48} does not. Similarly,

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

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

We cannot resist using Theorem 6.9 to prove the following fact.

Theorem 6.10. If n and r are positive integers with $1 \leq r < n$, then the binomial coefficient

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

is also an integer.

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

$$\left[\frac{n}{p^k}\right] \geq \left[\frac{r}{p^k}\right] + \left[\frac{(n-r)}{p^k}\right] \qquad k = 1, 2, \ldots$$

Adding these inequalities, we obtain

$$\sum_{k\geq 1}\left[\frac{n}{p^k}\right] \geq \sum_{k\geq 1}\left[\frac{r}{p^k}\right] + \sum_{k\geq 1}\left[\frac{(n-r)}{p^k}\right] \tag{1}$$

The left-hand side of Eq. (1) gives the exponent of the highest power of the prime p that divides $n!$, whereas the right-hand side equals the highest power of this prime contained in $r!(n-r)!$. Hence, p appears in the numerator of $n!/r!(n-r)!$ at least as many times as it occurs in the denominator. Because this holds true for every prime divisor of the denominator, $r!(n-r)!$ must divide $n!$, making $n!/r!(n-r)!$ an integer.

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

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

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

Now we have

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

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

We pick up a few loose threads. Having introduced the greatest integer function, let us see what it has to do with the study of number-theoretic functions. Their relationship is brought out by Theorem 6.11.

Theorem 6.11. Let f and F be number-theoretic functions such that

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

Then, for any positive integer N,

$$\sum_{n=1}^{N} F(n) = \sum_{k=1}^{N} f(k)\left[\frac{N}{k}\right]$$

Proof. We begin by noting that

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

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

$$k, 2k, 3k, \ldots, \left[\frac{N}{k}\right] k$$

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

$$\sum_{n=1}^{N} \sum_{d \mid n} f(d) = \sum_{k=1}^{N} f(k) \left[\frac{N}{k}\right]$$

and our task is complete.

As an immediate application of Theorem 6.11, we deduce Corollary 1.

Corollary 1. If N is a positive integer, then

$$\sum_{n=1}^{N} \tau(n) = \sum_{n=1}^{N} \left[\frac{N}{n}\right]$$

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

In the same way, the relation $\sigma(n) = \sum_{d \mid n} d$ yields Corollary 2.

Corollary 2. If N is a positive integer, then

$$\sum_{n=1}^{N} \sigma(n) = \sum_{n=1}^{N} n \left[\frac{N}{n}\right]$$

These last two corollaries, can perhaps, be clarified with an example.

Example 6.3. Consider the case $N = 6$. The definition of τ tells us that

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

From Corollary 1,

$$\begin{aligned}\sum_{n=1}^{6}\left[\frac{6}{n}\right] &= [6]+[3]+[2]+[3/2]+[6/5]+[1]\\ &= 6+3+2+1+1+1\\ &= 14\end{aligned}$$

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

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

and a simple calculation leads to

$$\begin{aligned}\sum_{n=1}^{6} n\left[\frac{6}{n}\right] &= 1[6]+2[3]+3[2]+4[3/2]+5[6/5]+6[1]\\ &= 1\cdot 6+2\cdot 3+3\cdot 2+4\cdot 1+5\cdot 1+6\cdot 1\\ &= 33\end{aligned}$$

PROBLEMS 6.3

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

2. Let x and y be real numbers. Prove that the greatest integer function satisfies the following properties:

(a) $[x+n] = [x]+n$ for any integer n.

(b) $[x]+[-x] = 0$ or -1, according as x is an integer or not.
[*Hint:* Write $x = [x]+\theta$, with $0 \le \theta < 1$, so that $-x = -[x]-1+(1-\theta)$.]

(c) $[x]+[y] \le [x+y]$ and, when x and y are positive, $[x][y] \le [xy]$.

(d) $[x/n] = [[x]/n]$ for any positive integer n.
[*Hint:* Let $x/n = [x/n]+\theta$, where $0 \le \theta < 1$; then $[x] = n[x/n]+[n\theta]$.]

(e) $[nm/k] \ge n[m/k]$ for positive integers, n, m, k.

(f) $[x]+[y]+[x+y] \le [2x]+[2y]$.
[*Hint:* Let $x = [x]+\theta$, $0 \le \theta < 1$, and $y = [y]+\theta'$, $0 \le \theta' < 1$. Consider cases in which neither, one, or both of θ and θ' are greater than or equal to $\frac{1}{2}$.]

3. Find the highest power of 5 dividing 1000! and the highest power of 7 dividing 2000!.

4. For an integer $n \ge 0$, show that $[n/2]-[-n/2] = n$.

5. (a) Verify that 1000! terminates in 249 zeros.

(b) For what values of n does $n!$ terminate in 37 zeros?

6. If $n \ge 1$ and p is a prime, prove that

(a) $(2n)!/(n!)^2$ is an even integer.
[*Hint:* Use Theorem 6.10.]

(b) The exponent of the highest power of p that divides $(2n)!/(n!)^2$ is

$$\sum_{k=1}^{\infty}\left(\left[\frac{2n}{p^k}\right]-2\left[\frac{n}{p^k}\right]\right)$$

(c) In the prime factorization of $(2n)!/(n!)^2$ the exponent of any prime p such that $n < p < 2n$ is equal to 1.

7. Let the positive integer n be written in terms of powers of the prime p so that we have $n = a_k p^k + \cdots + a_2 p^2 + a_1 p + a_0$, where $0 \le a_i < p$. Show that the exponent of the highest power of p appearing in the prime factorization of $n!$ is

$$\frac{n - (a_k + \cdots + a_2 + a_1 + a_0)}{p - 1}$$

8. (a) Using Problem 7, show that the exponent of highest power of p dividing $(p^k - 1)!$ is $[p^k - (p-1)k - 1]/(p-1)$.
[*Hint:* Recall the identity $p^k - 1 = (p-1)(p^{k-1} + \cdots + p^2 + p + 1)$.]
(b) Determine the highest power of 3 dividing 80! and the highest power of 7 dividing 2400!.
[*Hint:* $2400 = 7^4 - 1$.]

9. Find an integer $n \ge 1$ such that the highest power of 5 contained in $n!$ is 100.
[*Hint:* Because the sum of coefficients of the powers of 5 needed to express n in the base 5 is at least 1, begin by considering the equation $(n-1)/4 = 100$.]

10. Given a positive integer N, show the following:
(a) $\sum_{n=1}^{N} \mu(n)[N/n] = 1$.
(b) $|\sum_{n=1}^{N} \mu(n)/n| \le 1$.

11. Illustrate Problem 10 in the case where $N = 6$.

12. Verify that the formula

$$\sum_{n=1}^{N} \lambda(n) \left[\frac{N}{n}\right] = \left[\sqrt{N}\right]$$

holds for any positive integer N.
[*Hint:* Apply Theorem 6.11 to the multiplicative function $F(n) = \sum_{d \mid n} \lambda(d)$, noting that there are $[\sqrt{n}]$ perfect squares not exceeding n.]

13. If N is a positive integer, establish the following:
(a) $N = \sum_{n=1}^{2N} \tau(n) - \sum_{n=1}^{N} [2N/n]$.
(b) $\tau(N) = \sum_{n=1}^{N} ([N/n] - [(N-1)/n])$.

6.4 AN APPLICATION TO THE CALENDAR

Our familiar calendar, the Gregorian calendar, goes back as far as the second half of the 16th century. The earlier Julian calendar, introduced by Julius Caesar, was based on a year of $365\frac{1}{4}$ days, with a leap year every fourth year. This was not a precise enough measure, because the length of a solar year—the time required for the earth to complete an orbit about the sun—is apparently 365.2422 days. The small error meant that the Julian calendar receded a day from its astronomical norm every 128 years.

By the 16th century, the accumulating inaccuracy caused the vernal equinox (the first day of Spring) to fall on March 11 instead of its proper day, March 21. The calendar's inaccuracy naturally persisted throughout the year, but at this season it meant that the Easter festival was celebrated at the wrong astronomical time. Pope Gregory XIII rectified the discrepancy in a new calendar, imposed on the predominantly Catholic countries of Europe. He decreed that 10 days were to be omitted from the year 1582, by having October 15 of that year immediately follow

SATHYABAMA
INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)
Accredited "A" Grade by NAAC | 12B Status by UGC | Approved by AICTE
www.sathyabama.ac.in

SCHOOL OF SCIENCE AND HUMANITIES
DEPARTMENT OF MATHEMATICS

UNIT – V – NUMBER THOERY – SMT1554

Unit V

Euler's phi Function

In this chapter, we define and discuss the properties of Euler's phi function. We also state and prove the Euler's Theorem.

Definition

For $n \geq 1$, $\phi(n)$ denotes the number of positive integers not exceeding *n* and relatively prime to *n.* The function $\phi(n)$is usually called the *Euler phi-function* (*indicator* or *totient).*

Note:

If *n* is a prime number, then every integer less than *n* is relatively prime to it; whence, $\phi(n) = n - 1$.

Theorem

If *p* is a prime and *k* > 0, then $\phi(p^k) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right)$

Proof.

Since p is prime, $gcd(n, p^k) = 1$ if and only if $p \nmid n$. There are p^{k-1} integers between 1 and p^k that are divisible by *p*, namely, $p, 2p, 3p, \ldots (p^{k-1})p$. Thus, the set $\{1, 2, \ldots, p^k\}$ contains exactly $p^k - p^{k-1}$integers that are relatively prime to p^k, and so by the definition of the phi-function, $\phi(p^k) = p^k - p^{k-1}$.

Lemma.

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

Proof.

Case (i)

Suppose that $gcd(a, bc) = 1$ and let $d = gcd(a, b)$. Then $d|a$ and $d|b$ hence it follows that $d|a$ and $d|bc$. This implies that $gcd(a, bc) = d$, which forces *d* = 1. Similarly it can be proved that $gcd(a, c) = 1$.

Case (ii)

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

Theorem.

The Euler phi function is a multiplicative function. i.e., if m and n are two positive integers such that $\gcd(m,n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$.

Proof.

We know that $\phi(1) = 1$, hence the result obviously holds if either *m* or *n* equals 1. Let us suppose that *m* > 1 and *n* > 1. Arranging the integers from 1 to *mn* in *m* columns of *n* integers each, as follows:

1	2	$\cdots r \cdots$	m
$m+1$	$(m+1)$	$\cdots (m+r) \cdots$	$2m$
$(2m+2)$	$(2m+2)$	$\cdots (2m+r) \cdots$	3m
.	.	.	.
.	.	.	.
$(n-1)m+1$	$(n-1)m+2$	$\cdots (n-1)m+r \cdots$	mn

From the above array of mn elements we have identify numbers that are relatively prime to mn. From the previous lemma it is the same as the number of integers that are relatively prime to both *m* and *n*. We know that, $gcd(qm + r, m) = gcd(r, m)$, the numbers in the r^{th} column are relatively prime to *m* if and only if *r* itself is relatively prime to *m*. Therefore, only ¢(m) columns contain integers relatively prime to m, and every entry in the column will be relatively prime to *m*. Now the entries in the r^{th} column (where it is assumed that gcd(r, m) = 1) are $r, m + r, 2m + r, \ldots, (n-1)m + r$. The listed n integers are incongruent to modulo n. For if any two integers are congruent modulo n i.e. $km + r \equiv sm + r (mod\ n), 0 \le k < s < n \Rightarrow km \equiv sm (mod\ n) \Rightarrow k \equiv s (mod\ n)$. Thus, the numbers in the *rth* column are congruent modulo *n* to 0, 1, 2, ... , *n*- 1, in some order. But if $s \equiv t\ (mod\ n)$, then $gcd(s,n) = 1$ if and only if $gcd(t, n) = 1$. The implication is that the rth column contains as many integers that are relatively prime to *n* as does the set $\{0, 1, 2, \ldots, n-1\}$, namely, ¢(n) integers. Therefore, the total number of entries in the array that are relatively prime to both *m* and *n* is ¢(m)¢(n). This completes the proof of the theorem.

Theorem.

If the integer n > 1 has the prime factorization $n = p_1^{k_1} p_2^{k_2} p_3^{k_3} \cdots p_r^{k_r}$, then $\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right)$ **Proof**.

Let us prove this theorem by the method of induction, using induction on r, the number of distinct prime factors of n. When $r = 1$, the statement follows from the previous theorem. Since , it is true for $r = 1$, let us assume it is true for $r = i$. i.e., $\phi\left(p_1^{k_1} p_2^{k_2} p_3^{k_3} \cdots p_i^{k_i}\right) = p_1^{k_1} p_2^{k_2} p_3^{k_3} \cdots p_i^{k_i}\left(\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_i}\right)\right)$

For $r = i + 1$, $\phi\left(p_1^{k_1} p_2^{k_2} p_3^{k_3} \cdots p_i^{k_i} p_{i+1}^{k_i+1}\right) = \phi\left(p_1^{k_1} p_2^{k_2} p_3^{k_3} \cdots p_i^{k_i}\right)\phi\left(p_{i+1}^{k_i+1}\right)$

$$= p_1^{k_1} p_2^{k_2} p_3^{k_3} \cdots p_i^{k_i} \left(\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_i}\right) \right) p_{i+1}^{k_i+1} \left(1 - \frac{1}{p_{i+1}^{k_i+1}}\right)$$

Hence, whenever the statement is true for $n = i$, it is true for $n = i + 1$ by principle of mathematical induction the statement is true for all $n > 1$. This proves the theorem.

Theorem.

For n > 2, $\phi(n)$ is an even integer.

Proof.

If $n > 2$, is prime then $\phi(n) = n - 1$ is even. As every prime number greater than 2 is odd. If n is an even composite number with the prime factorisation $n = p_1^{k_1} p_2^{k_2} p_3^{k_3} \cdots p_r^{k_r}$ then $\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right)$ which is even as n is even. If n is odd, then the prime factorization of n involves only the odd prime factors. Let $n = p_i^{k_i} m$. Since, Euler's phi function is multiplicative $\phi(n) = \phi\left(p_i^{k_i}\right)\phi(m) = p_i^{k_i - 1}(p_i - 1)\phi(m)$. As $p_i - 1$ is even $\phi(n)$ is even. This proves the theorem

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

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

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

Proof. Observe that no two of the integers $aa_1, aa_2, \ldots, aa_{\phi(n)}$ are congruent modulo n. For if $aa_i \equiv aa_j \pmod{n}$, with $1 \leq i < j \leq \phi(n)$, then the cancellation law yields $a_i \equiv a_j \pmod{n}$, and thus $a_i = a_j$, a contradiction. Furthermore, because $\gcd(a_i, n) = 1$ for all i and $\gcd(a, n) = 1$, the lemma preceding Theorem 7.2 guarantees that each of the aa_i is relatively prime to n.

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

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

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

Theorem 7.5 Euler. If $n \geq 1$ and $\gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$.

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

$$\begin{aligned} aa_1 &\equiv a_1' \pmod{n} \\ aa_2 &\equiv a_2' \pmod{n} \\ &\vdots \qquad\qquad \vdots \\ aa_{\phi(n)} &\equiv a_{\phi(n)}' \pmod{n} \end{aligned}$$

where $a_1', a_2', \ldots, a_{\phi(n)}'$ are the integers $a_1, a_2, \ldots, a_{\phi(n)}$ in some order. On taking the product of these $\phi(n)$ congruences, we get

$$\begin{aligned} (aa_1)(aa_2)\cdots(aa_{\phi(n)}) &\equiv a_1'a_2'\cdots a_{\phi(n)}' \pmod{n} \\ &\equiv a_1a_2\cdots a_{\phi(n)} \pmod{n} \end{aligned}$$

and so

$$a^{\phi(n)}(a_1a_2\cdots a_{\phi(n)}) \equiv a_1a_2\cdots a_{\phi(n)} \pmod{n}$$

Because $\gcd(a_i, n) = 1$ for each i, the lemma preceding Theorem 7.2 implies that $\gcd(a_1a_2\cdots a_{\phi(n)}, n) = 1$. Therefore, we may divide both sides of the foregoing congruence by the common factor $a_1a_2\cdots a_{\phi(n)}$, leaving us with

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

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

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