CHAPTER 11

Properties of the Integers

11.1 INTRODUCTION

This chapter investigates some basic properties of the *natural numbers* (or *positive integers*), that is, the set

$$\mathbf{N} = \{1, 2, 3, \ldots\}$$

and their "cousins," the integers, that is, the set

$$\mathbf{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$$

(The letter **Z** comes from the word "Zahlen" which means numbers in German.)

The following simple rules concerning the addition and multiplication of these numbers are assumed (where a, b, c are arbitrary integers):

(a) Associative law for multiplication and addition:

$$(a + b) + c = a + (b + c) \quad \text{and} \quad (ab)c = a(bc)$$

(b) Commutative law for multiplication and addition:

$$a + b = b + a \quad \text{and} \quad ab = ba$$

(c) Distributive law:

$$a(b + c) = ab + ac$$

(d) Additive identity 0 and multiplicative identity 1:

$$a + 0 = 0 + a = a \quad \text{and} \quad a \cdot 1 = 1 \cdot a = a$$

(e) Additive inverse $-a$ for any integer a:

$$a + (-a) = (-a) + a = 0$$

Appendix **B** shows that other mathematical structures have the above properties. One fundamental property which distinguishes the integers **Z** from other structures is the Principle of Mathematical Induction (Section 1.8) which we rediscuss here. We also state and prove (Problem 11.30) the following theorem.

Fundamental Theorem of Arithmetic: Every positive integer $n > 1$ can be written uniquely as a product of prime numbers.

This theorem already appeared in Euclid's *Elements*. Here we also develop the concepts and methods which are used to prove this important theorem.

11.2 ORDER AND INEQUALITIES, ABSOLUTE VALUE

This section discusses the elementary properties of order and absolute value.

Order

Observe that we define order in **Z** in terms of the positive integers **N**. All the usual properties of this order relation are a consequence of the following two properties of **N**:

$[\mathbf{P_1}]$ If a and b belong to **N**, then $a + b$ and ab belong to **N**.

$[\mathbf{P_2}]$ For any integer a, either $a \in \mathbf{N}$, $a = 0$, or $-a \in \mathbf{N}$.

The following notation is also used:

$a > b$ means $b < a$;	read: a is greater than b.
$a \leq b$ means $a < b$ or $a = b$;	read: a is less than or equal to b.
$a \geq b$ means $b \geq a$;	read: a is greater than or equal to b.

The relations $<$, $>$, $\leq$ and $\geq$ are called *inequalities* in order to distinguish them from the relation $=$ of equality. The reader is certainly familiar with the representation of the integers as points on a straight line, called the *number line* **R**, as shown in Fig. 11-1.

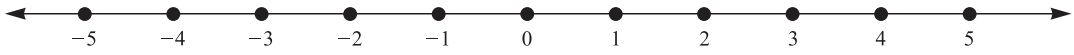

Fig. 11-1

We note that $a < b$ if and only if a lies to the left of b on the number line **R** in Fig. 11-1. For example,

$$2 < 5; \qquad -6 < -3; \qquad 4 \leq 4; \qquad 5 > -8; \qquad 6 \geq 0; \qquad -7 \leq 0$$

We also note that a is positive iff $a > 0$, and a is negative iff $a < 0$. (Recall "iff" means "if and only if.") Basic properties of the inequality relations follow.

Proposition 11.1: The relation $\leq$ in **Z** has the following properties:

(i) $a \leq a$, for any integer a.

(ii) If $a \leq b$ and $b \leq a$, then $a = b$.

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

Proposition 11.2 (Law of Trichotomy): For any integers a and b, exactly one of the following holds:

$$a < b, \quad a = b, \quad \text{or} \quad a > b$$

Proposition 11.3: Suppose $a \leq b$, and let c be any integer. Then:

(i) $a + c \leq b + c$.

(ii) $ac \leq bc$ when $c > 0$; but $ac \leq bc$ when $c < 0$.

(Problem 11.5 proves Proposition 11.3.)

Absolute Value

The *absolute value* of an integer a. written $|a|$, is formally defined by

$$|a| = \begin{cases} a & \text{if } a \geq 0 \\ -a & \text{if } a < 0 \end{cases}$$

Accordingly, $|a| > 0$ except when $a = 0$. Geometrically speaking, $|a|$ may be viewed as the distance between the points a and 0 on the number line $\mathbf{R}$. Also, $|a - b| = |b - a|$ may be viewed as the distance between the points a and b. For example:

(a) $|-3| = 3$; $|7| = 7$; $|-13| = 13$; (b) $|2 - 7| = |-5| = 5$; $|7 - 2| = |5| = 5$

Some properties of the absolute value function follow. (Problems 11.6 and 11.7 prove (iii) and (iv).)

Proposition 11.4: Let a and b be any integers. Then:

(i) $|a| \geq 0$, and $|a| = 0$ iff $a = 0$
(ii) $-|a| \leq a \leq |a|$
(iii) $|ab| = |a||b|$
(iv) $|a \pm b| \leq |a| + |b|$
(v) $||a| - |b|| \leq |a \pm b|$

11.3 MATHEMATICAL INDUCTION

The principle of mathematical induction stated below essentially asserts that the positive integers $\mathbf{N}$ begin with the number 1 and the rest are obtained by successively adding 1. That is, we begin with 1, then $2 = 1 + 1$, then $3 = 2 + 1$, then $4 = 3 + 1$, and so on. The principle makes precise the vague phrase "and so on."

Principle of Mathematical Induction: Let S be a set of positive integers with the following two properties:

(i) 1 belongs to S.

(ii) If k belongs to S, then $k + 1$ belongs to S.

Then S is the set of all positive integers.

We shall not prove this principle. On the contrary, when the set $\mathbf{N}$ of positive integers (natural numbers) is developed axiomatically, this principle is given as one of the axioms.

There is an equivalent form of the above principle which is usually used when proving theorems:

Principle of Mathematical Induction: Let P be a proposition defined on the integers $n \geq 1$ such that:

(i) $P(1)$ is true.

(ii) $P(k + 1)$ is true whenever $P(k)$ is true.

Then P is true for every integer $n \geq 1$.

EXAMPLE 11.1

(a) Let P be the proposition that the sum of the first n odd numbers is n^2; that is:

$$P(n)\colon 1 + 3 + 5 + \cdots + (2n - 1) = n^2$$

(The nth odd number is $2n - 1$ and the next odd number is $2n + 1$.)

Clearly, $P(n)$ is true for $n = 1$; that is:

$$P(1)\colon 1 = 1^2$$

Suppose $P(k)$ is true. (This is called the inductive hypothesis.) Adding $2k + 1$ to both sides of $P(k)$ we obtain

$$1 + 3 + 5 + \cdots + (2k - 1) + (2k + 1) = k^2 + (2k + 1)$$
$$= (2k + 1)^2$$

which is $P(k + 1)$. We have shown that $P(k + 1)$ is true whenever $P(k)$ is true. By the principle of mathematical induction, P is true for all positive integers n.

(b) The symbol $n!$ (read: n factorial) is defined as the product of the first n positive integers; that is:

$$1! = 1, \quad 2! = 2 \cdot 1 = 2, \quad 3! = 3 \cdot 2 \cdot 1 = 6, \qquad \text{and so on.}$$

This may be formally defined as follows:

$$1! = 1 \quad \text{and} \quad (n + 1)! = (n + 1)(n!), \quad \text{for} \quad n > 1$$

Observe that if S is the set of positive integers for which ! is defined, then S satisfies the two properties of mathematical induction. Hence the above definition defines ! for every positive integer.

There is another form of the principle of mathematical induction (proved in Problem 11.13) which is sometimes more convenient to use. Namely:

Theorem 11.5 (Induction: Second Form): Let P be a proposition defined on the integers $n \geq 1$ such that:

(i) $P(1)$ is true.

(ii) $P(k)$ is true whenever $P(j)$ is true for all $1 \leq j < k$.

Then P is true for every integer $n \geq 1$.

Remark: The above theorem is true if we replace 1 by 0 or by any other integer a.

Well-Ordering Principle

A property of the positive integers which is equivalent to the principle of induction, although apparently very dissimilar, is the well-ordering principle (proved in Problem 11.12). Namely:

Theorem 11.6 (Well-Ordering Principle): Let S be a nonempty set of positive integers. Then S contains a *least element*; that is, S contains an element a such that $a \leq s$ for every s in S.

Generally speaking, an ordered set S is said to be *well-ordered* if every subset of S contains a first element. Thus Theorem 11.6 states that **N** is well ordered.

A set S of integers is said to be *bounded from below* if every element of S is greater than some integer m (which may be negative). (The number m is called a *lower bound* of S.) A simple corollary of the above theorem follows:

Corollary 11.7: Let S be a nonempty set of integers which is bounded from below. Then S contains a least element.

11.4 DIVISION ALGORITHM

The following fundamental property of arithmetic (proved in Problems 11.17 and 11.18) is essentially a restatement of the result of long division.

Theorem 11.8 (Division Algorithm): Let a and b be integers with $b \neq 0$. Then there exists integers q and r such that

$$a = bq + r \quad \text{and} \quad 0 \leq r < |b|$$

Also, the integers q and r are unique.

The number q in the above theorem is called the *quotient*, and r is called the *remainder*. We stress the fact that r must be non-negative. The theorem also states that

$$r = a - bq$$

This equation will be used subsequently

If a and b are positive, then q is non negative. If b is positive, then Fig. 11-2 gives a geometrical interpretation of this theorem. That is, the positive and negative multiples of b will be evenly distributed throughout the number line $\mathbf{R}$, and a will fall between some multiples qb and $(q + 1)b$. The distance between qb and a is then the remainder r.

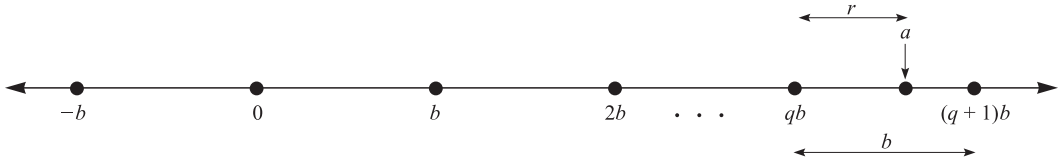

Fig. 11-2

Division Algorithm using a Calculator

Suppose a and b are both positive. Then one can find the quotient q and remainder r using a calculator as follows:

Step 1. Divide a by b using the calculator, that is, find a/b.

Step 2. Let q be the integer part of a/b, that is, let $q = INT(a/b)$.

Step 3. Let r be the difference between a and bq, that is, let $r = a - bq$.

EXAMPLE 11.2

(a) Let $a = 4461$ and $b = 16$. We can find that the quotient $q = 278$ and the remainder $r = 13$ by long division, Alternately, using a calculator, we obtain q and r as follows:

$$a/b = 278.8125\ldots, \quad q = 278, \qquad r = 4461 - 16(278) = 13$$

As expected, $a = bq + r$, namely:

$$4461 = 16(278) + 13$$

(b) Let $a = -262$ and $b = 3$. First we divide $|a| = 262$ by $b = 3$. This yields a quotient $q' = 87$ and a remainder $r' = 1$. Thus

$$262 = 3(87) + 1$$

We need $a = -262$, so we multiply by -1 obtaining

$$-262 = 3(-87) - 1$$

However, -1 is negative and hence cannot be r. We correct this by adding and subtracting the value of b (which is 3) as follows:

$$-262 = 3(-87) - 3 + 3 - 1 = 3(-88) + 2$$

Therefore, $q = -88$ and $r = 2$.

(c) Let $b = 2$. Then any integer a can be written in the form

$$a = 2q + r \quad \text{where} \quad 0 \leq r < 2$$

Thus r can only be 0 or 1. Thus every integer is of the form $2k$ or $2k + 1$. The integers of the form $2k$ are called *even* integers, while those of the form $2k + 1$ are called *odd* integers. (Usually, an even integer is defined as an integer divisible by 2, and all other integers are said to be odd. Thus the division algorithm proves that every odd integer has the form $2k + 1$.)

11.5 DIVISIBILITY, PRIMES

Let a and b be integers with $a \neq 0$. Suppose $ac = b$ for some integer c. We then say that a divides b or b is divisible by a, and we denote this by writing

$$a \mid b$$

We also say that b is a *multiple* of a or that a is a *factor* or *divisor* of b. If a does not divide b, we will write $a \nmid b$.

EXAMPLE 11.3

(a) Clearly, $3 \mid 6$ since $3 \cdot 2 = 6$, and $-4 \mid 28$ since $(-4)(-7) = 28$.

(b) The divisors of 4 are ± 1, ± 2, ± 4 and the divisors of 9 are ± 1, ± 3, ± 9.

(c) If $a \neq 0$, then $a \mid 0$ since $a \cdot 0 = 0$.

(d) Every integer a is divisible by ± 1 and $\pm a$. These are sometimes called the *trivial divisors* of a. The basic properties of divisibility is stated in the next theorem (proved in Problem 11.24).

Theorem 11.9: Suppose a, b, c are integers.

(i) If $a \mid b$ and $b \mid c$, then $a \mid c$.

(ii) If $a \mid b$ then, for any integer x, $a \mid bx$.

(iii) If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$ and $a \mid (b - c)$.

(iv) If $a \mid b$ and $b \neq 0$, then $a = \pm b$ or $|a| < |b|$.

(v) If $a \mid b$ and $b \mid a$, then $|a| = |b|$, i.e., $a = \pm b$.

(vi) If $a \mid 1$, then $a = \pm 1$

Putting (ii) and (iii) together, we obtain the following important result.

Corollary 11.10: Suppose $a \mid b$ and $a \mid c$. Then, for any integers x and y, $a \mid (bx + cy)$. The expression $bx + cy$ will be called a *linear combination* of b and c.

Primes

A positive integer $p > 1$ is called a *prime number* or a *prime* if its only divisors are ± 1 and $\pm p$, that is, if p only has trivial divisors. If $n > 1$ is not prime, then n is said to be *composite*. We note (Problem 11.13) that if $n > 1$ is composite then $n = ab$ where $1 < a, b < n$.

EXAMPLE 11.4

(a) The integers 2 and 7 are primes, whereas $6 = 2 \cdot 3$ and $15 = 3 \cdot 5$ are composite.

(b) The primes less than 50 follow:

$$2, \quad 3, \quad 5, \quad 7, \quad 11, \quad 13, \quad 17, \quad 19, \quad 23, \quad 29, \quad 31, \quad 37, \quad 41, \quad 43, \quad 47$$

(c) Although 21, 24, and 1729 are not primes, each can be written as a product of primes:

$$21 = 3 \cdot 7; \qquad 24 = 2 \cdot 2 \cdot 2 \cdot 3 = 2^3 \cdot 3; \qquad 1729 = 7 \cdot 13 \cdot 19$$

The Fundamental Theorem of Arithmetic states that every integer $n > 1$ can be written as a product of primes in essentially one way; it is a deep and somewhat difficult theorem to prove. However, using induction, it is easy at this point to prove that such a product exists. Namely:

Theorem 11.11: Every integer $n > 1$ can be written as a product of primes.

Note that a product may consist of a single factor so that a prime p is itself a product of primes. We prove Theorem 11.11 here, since its proof is relatively simple.

Proof: The proof is by induction. Let $n = 2$. Since 2 is prime, n is a product of primes. Suppose $n > 2$, and the theorem holds for positive integers less than n. If n is prime, then n is a product of primes. If n is composite, then $n = ab$ where $a, b < n$. By induction, a and b are products of primes; hence $n = ab$ is also a product of primes.

Euclid, who proved the Fundamental Theorem of Arithmetic, also asked whether or not there was a largest prime. He answered the question thus:

Theorem 11.12: There is no largest prime, that is, there exists an infinite number of primes.

Proof: Suppose there is a finite number of primes, say $p_1, p_2, \ldots, p_m$. Consider the integer

$$n = p_1 p_2 \cdots p_m + 1$$

Since n is a product of primes (Theorem 11.11), it is divisible by one of the primes, say p_k. Note that p_k also divides the product $p_1 p_2 \ldots p_m$. Therefore p_k divides

$$n - p_1 p_2 \ldots p_m = 1$$

This is impossible, and so n is divisible by some other prime. This contradicts the assumption that $p_1, p_2, \ldots, p_m$ are the only primes. Thus the number of primes is infinite, and the theorem is proved.

11.6 GREATEST COMMON DIVISOR, EUCLIDEAN ALGORITHM

Suppose a and b are integers, not both 0. An integer d is called a *common divisor* of a and b if d divides both a and b, that is, if $d \mid a$ and $d \mid b$. Note that 1 is a positive common divisor of a and b, and that any common divisor of a and b cannot be greater than $|a|$ or $|b|$. Thus there exists a largest common divisor of a and b; it is denoted by

$$\gcd(a, b)$$

and it is called the *greatest common divisor* of a and b.

EXAMPLE 11.5

(a) The common divisors of 12 and 18 are $\pm 1, \pm 2, \pm 3, \pm 6$. Thus $\gcd(12, 18) = 6$. Similarly:

$$\gcd(12, -18) = 16, \qquad \gcd(12, -16) = 4, \qquad \gcd(29, 15) = 1, \qquad \gcd(14, 49) = 7$$

(b) For any integer a, we have $\gcd(1, a) = 1$.

(c) For any prime p, we have $\gcd(p, a) = p$ or $\gcd(p, a) = 1$ according as p does or does not divide a.

(d) Suppose a is positive. Then $a \mid b$ if and only if $\gcd(a, b) = a$.

The following theorem (proved in Problem 11.26) gives an alternative characterization of the greatest common divisor.

Theorem 11.13: Let d be the smallest positive integer of the form $ax + by$. Then

$$d = \gcd(a, b).$$

Corollary 11.14: Suppose $d = \gcd(a, b)$. Then there exist integers x and y such that $d = ax + by$.

Another way to characterize the greatest common divisor, without using the inequality relation, follows

Theorem 11.15: A positive integer $d = \gcd(a, b)$ if and only if d has the following two properties:

(1) d divides both a and b.

(2) If c divides both a and b, then $c \mid d$.

Simple properties of the greatest common divisor are:

(a) $\gcd(a, b) = \gcd(b, a)$.

(b) If $x > 0$, then $\gcd(ax, bx) = x \cdot \gcd(a, b)$.

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

(d) For any integer x, $\gcd(a, b) = \gcd(a, b + ax)$.

Euclidean Algorithm

Let a and b be integers, and let $d = \gcd(a, b)$. One can always find d by listing all the divisors of a and then all the divisors of b and then choosing the largest common divisor. The complexity of such an algorithm is $f(n) = 0(\sqrt{n})$ where $n = |a| + |b|$. Also, we have given no method to find the integers x and y such that $d = ax + by$.

This subsection gives a very efficient algorithm, called the Euclidean algorithm, with complexity $f(n) = O(\log n)$, for finding $d = \gcd(a, b)$ by applying the division algorithm to a and b and then repeatedly applying it to each new quotient and remainder until obtaining a nonzero remainder. The last nonzero remainder is $d = \gcd(a, b)$.

Then we give an "unraveling" algorithm which reverses the steps in the Euclidean algorithm to find the integers x and y such that $d = xa + yb$.

We illustrate the algorithms with an example.

EXAMPLE 11.6 Let $a = 540$ and $b = 168$. We apply the Euclidean algorithm to a and b. These steps, which repeatedly apply the division algorithm to each quotient and remainder until obtaining a zero remainder, are pictured in Fig. 11-3(a) using long division and also in Fig. 11-3(b) where the arrows indicate the quotient and remainder in the next step. The last nonzero remainder is 12. Thus

$$12 = \gcd(540, 168)$$

This follows from the fact that

$$\gcd(540, 168) = \gcd(168, 36) = \gcd(36, 24) = \gcd(24, 12) = 12$$

Next we find x and y such that $12 = 540x + 168y$ by "unraveling" the above steps in the Euclidean algorithm. Specifically, the first three quotients in Fig. 11-3 yield the following equations:

$$(1)\ 36 = 540 - 3(168), \qquad (2)\ 24 = 168 - 4(36), \qquad (3)\ 12 = 36 - 1(24)$$

Equation (3) tells us that $d = \gcd(a, b) = 12$ is a linear combination of 36 and 24. Now we use the preceding equations in reverse order to eliminate the other remainders. That is, first we use equation (2) to replace 24 in equation (3) so we can write 12 as a linear combination of 168 and 36 as follows:

$$(4)\ 12 = 36 - 1[168 - 4(36)] = 36 - 1(168) + 4(36) = 5(36) - 1(168)$$

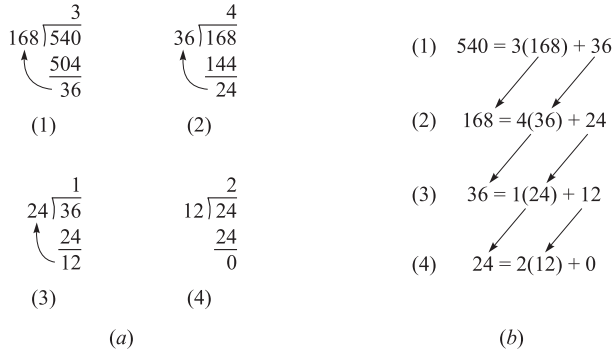

Fig. 11-3

Next we use equation (1) to replace 36 in (4) so we can write 12 as a linear combination of 168 and 540 as follows:

$$12 = 5[540 - 3(168)] - 1(168) = 5(54) - 15(168) - 1(168) = 5(540) - 16(168)$$

This is our desired linear combination. In other words, $x = 5$ and $y = -16$.

Least Common Multiple

Suppose a and b are nonzero integers. Note that $|ab|$ is a positive common multiple of a and b. Thus there exists a smallest positive common multiple of a and b; it is denoted by

$$\text{lcm}(a, b)$$

and it is called the *least common multiple* of a and b.

EXAMPLE 11.7

(a) $\text{lcm}(2, 3) = 6$; $\text{lcm}(4, 6) = 12$; $\text{lcm}(9, 10) = 90$.

(b) For any positive integer a, we have $\text{lcm}(1, a) = a$.

(c) For any prime p and any positive integer a,

$$\text{lcm}(p, a) = a \quad \text{or} \quad \text{lcm}(p, a) = ap$$

according as p does or does not divide a.

(d) Suppose a and b are positive integers. Then $a \mid b$ if and only if $\text{lcm}(a, b) = b$.

The next theorem gives an important relationship between the greatest common divisor and the least common multiple.

Theorem 11.16: Suppose a and b are nonzero integers. Then

$$\text{lcm}(a,b) = \frac{|ab|}{\gcd(a, b)}$$

11.7 FUNDAMENTAL THEOREM OF ARITHMETIC

This section discusses the Fundamental Theorem of Arithmetic. First we define relatively prime integers.

Relatively Prime Integers

Two integers a and b are said to be *relatively prime* or *coprime* if $\gcd(a, b) = 1$. Accordingly, if a and b are relatively prime, then there exist integers x and y such that

$$ax + by = 1$$

Conversely, if $ax + by = 1$, then a and b are relatively prime.

EXAMPLE 11.8

(a) Observe that: $\gcd(12, 35) = 1$, $\gcd(49, 18) = 1$, $\gcd(21, 64) = 1$, $\gcd(-28, 45) = 1$

(b) If p and q are distinct primes, then $\gcd(p, q) = 1$.

(c) For any integer a, we have $\gcd(a, a + 1) = 1$, since any common factor of a and $a + 1$ must divide their difference $(a + 1) - a = 1$.

The relation of being relatively prime is particularly important because of the following results. The first theorem is proved in Problem 11.27, and we will prove the second theorem here.

Theorem 11.17: Suppose $\gcd(a, b) = 1$, and a and b both divide c. Then ab divides c.

Theorem 11.18: Suppose $a \mid bc$, and $\gcd(a, b) = 1$. Then $a \mid c$

Proof: Since $\gcd(a, b) = 1$, there exist x and y such that $ax + by = 1$. Multiplying by c yields:

$$acx + bcy = c$$

We have $a \mid acx$. Also, $a \mid bcy$ since, by hypothesis, $a \mid bc$. Hence a divides the sum $acx + bcy = c$.

Corollary 11.19: Suppose a prime p divides the product ab. Then $p \mid a$ or $p \mid b$.

This corollary (proved in Problem 11.28) dates back to Euclid; it is the basis of his proof of the Fundamental Theorem of Arithmetic.

Fundamental Theorem of Arithmetic

Theorem 11.11 asserts that every positive integer is a product of primes. Can different products of primes yield the same number? Clearly, we can rearrange the order of the prime factors, e.g.,

$$30 = 2 \cdot 3 \cdot 5 = 5 \cdot 2 \cdot 3 = 3 \cdot 2 \cdot 5$$

The Fundamental Theorem of Arithmetic (proved in Problem 11.30) says that this is the only way that two "different" products can give the same number. Namely:

Theorem 11.20 (Fundamental Theorem of Arithmetic): Every integer $n > 1$ can be expressed uniquely (except for order) as a product of primes.

The primes in the factorization of n need not be distinct. Frequently, it is useful to collect together all equal primes. Then n can be expressed uniquely in the form

$$n = p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r}$$

where the m_i are positive and $p_1 < p_2 < \ldots < p_r$. This is called the *canonical factorization* of n.

EXAMPLE 11.9

Given $a = 2^4 \cdot 3^3 \cdot 7 \cdot 13$ and $b = 2^3 \cdot 3^2 \cdot 5^2 \cdot 11 \cdot 17$. Find $d = \gcd(a, b)$ and $m = \text{lcm}(a, b)$.

(a) First we find $d = \gcd(a, b)$. Those primes p, which appear in both a and b, 2, 3, and 11, will also appear in d, and the exponent of p, in d will be the smaller of its exponents in a and b. Thus

$$d = \gcd(a, b) = 2^3 \cdot 3^2 \cdot 11 = 792$$

(b) Next we find $m = \text{lcm}(a, b)$. Those primes p, which appear in either a or b, 2, 3, 5, 7, 11, 13, and 17, will also appear in m, and the exponent of p in m will be the larger of its exponents in a and b. Thus

$$m = \text{lcm}(a, b) = 2^4 \cdot 3^3 \cdot 5^2 \cdot 11 \cdot 13 \cdot 17$$

We are so used to using numbers as if the Fundamental Theorem of Arithmetic were true that it may seem as if it needs no proof. It is a tribute to Euclid, who first proved the theorem, that he recognized that it does require proof. We emphasize the nontriviality of the theorem by giving an example of a system of numbers which does not satisfy this theorem.

EXAMPLE 11.10 Let F be the set of positive integers of the form $3x + 1$. Thus F consists of the numbers:

$$1,\ 4,\ 7,\ 10,\ 13,\ 16,\ 19,\ 22,\ \ldots$$

Note that the product of two numbers in F is again in F since:

$$(3x + 1)(3y + 1) = 9xy + 3x + 3y + 1 = 3(3xy + x + y) + 1$$

Our definition of primes makes perfectly good sense in F. Although $4 = 2 \cdot 2$, the number 2 is not in F. Thus 4 is prime in F since 4 has no factors except 1 and 4. Similarly 10, 22, 25,… are primes in F. We list the first few primes in F:

$$4,\ 7,\ 10,\ 13,\ 19,\ 22,\ 25,\ \ldots$$

Note $100 = 3(33) + 1$ belongs to F. However, 100 has two essentially different factorizations into primes of F; namely,

$$100 = 4 \cdot 25 \qquad \text{and} \qquad 100 = 10 \cdot 10$$

Thus there is no unique factorization into primes in F.

11.8 CONGRUENCE RELATION

Let m be a positive integer. We say that a is *congruent* to b *modulo* m. written

$$a \equiv b \text{ (modulo } m) \qquad \text{or simply} \qquad a \equiv b \text{ (mod } m)$$

if m divides the difference $a - b$. The integer m is called the *modulus*. The negation of $a \equiv b \pmod m$ is written $a \not\equiv b \pmod m$. For example:

(i) $87 \equiv 23 \pmod 4$ since 4 divides $87 - 23 = 64$.

(ii) $67 \equiv 1 \pmod 6$ since 6 divides $67 - 1 = 66$.

(iii) $72 \equiv -5 \pmod 7$ since 7 divides $72 - (-5) = 77$.

(iv) $27 \not\equiv 8 \pmod 9$ since 9 does not divide $27 - 8 = 19$.

Our first theorem (proved in Problem 11.34) states that congruence modulo m is an equivalence relation.

Theorem 11.21: Let m be a positive integer. Then:

(i) For any integer a, we have $a \equiv a \pmod m$.

(ii) If $a \equiv b \pmod m$, then $b \equiv a \pmod m$.

(iii) If $a \equiv b \pmod m$ and $b \equiv c \pmod m$, then $a \equiv c \pmod m$.

Remark: Suppose m is positive, and a is any integer. By the Division Algorithm, there exist integers q and r with $0 = r \leq m$ such that $a = mq + r$. Hence

$$mq = a - r \quad \text{or} \quad m \mid (a - r) \quad \text{or} \quad a \equiv r \pmod{m}$$

Accordingly:

(1) Any integer a is congruent modulo m to a unique integer in the set

$$\{0,\ 1,\ 2, \ldots, m - 1\}$$

The uniqueness comes from the fact that m cannot divide the difference of two such integers.

(2) Any two integers a and b are congruent modulo m if and only if they have the same remainder when divided by m.

Residue Classes

Since congruence modulo m is an equivalence relation, it partitions the set $\mathbf{Z}$ of integers into disjoint equivalence classes called the *residue classes modulo m*. By the above remarks, a residue class consists of all those integers with the same remainder when divided by m. Therefore, there are m such residue classes and each residue class contains exactly one of the integers in the set of possible remainders, that is,

$$\{0,\ 1,\ 2,\ \ldots, m - 1\}$$

Generally speaking, a set of m integers $\{a_1,\ a_2,\ \ldots, a_m\}$ is said to be a *complete residue system modulo m* if each a_i comes from a distinct residue class. (In such a case, each a_i is called a *representative* of its equivalence class.)

Thus the integers from 0 to $m - 1$ form a complete residue system. In fact, any m consecutive integers form a complete residue system modulo m.

The notation $[x]_m$, or simply $[x]$ is used to denote the residue class (modulo m) containing an integer x, that is, those integers which are congruent to x. In other words,

$$[x] = \{a \in \mathbf{Z} \mid a \equiv x \pmod{m}\}$$

Accordingly, the residue classes can be denoted by

$$[0],\ [1],\ [2], \ldots, [m - 1]$$

or by using any other choice of integers in a complete residue system.

EXAMPLE 11.11 The residue classes modulo $m = 6$ follow:

$$\begin{aligned} [0] &= \{\ldots, -18, -12, -6, 0, 6, 12, 18, \ldots\}, \quad |3| = \{\ldots, -15, -9, -3, 3, 9, 15, 21, \ldots\} \\ [1] &= \{\ldots, -17, -11, -5, 1, 7, 13, 19, \ldots\}, \quad |4| = \{\ldots, -14, -8, -2, 4, 10, 16, 22, \ldots\} \\ [2] &= \{\ldots, -16, -10, -4, 2, 8, 14, 20, \ldots\}, \quad |5| = \{\ldots, -13, -7, -1, 5, 11, 17, 23, \ldots\} \end{aligned}$$

Note that $\{-2, -1, 0, 1, 2, 3\}$ is also a complete residue system modulo $m = 6$, and these representatives have minimal absolute values.

Congruence Arithmetic

The next theorem (proved in Problem 11.35) tells us that, under addition and multiplication, the congruence relation behaves very much like the relation of equality. Namely:

Theorem 11.22: Suppose $a \equiv c \pmod{m}$ and $b \equiv d \pmod{m}$. Then:
(i) $a + b \equiv c + d \pmod{m}$; (ii) $a \cdot b \equiv c \cdot d \pmod{m}$

Remark: Suppose $p(x)$ is a polynomial with integral coefficients. If $s \equiv t \pmod{m}$, then using Theorem 11.22 repeatedly we can show that $p(s) \equiv p(t) \pmod{m}$.

EXAMPLE 11.12 Observe that $2 \equiv 8 \pmod 6$ and $5 \equiv 41 \pmod 6$. Then:

(a) $2 + 5 \equiv 8 + 41 \pmod 6$ or $7 \equiv 49 \pmod 6$

(b) $2 \cdot 5 \equiv 8 \cdot 41 \pmod 6$ or $10 \equiv 328 \pmod 6$

(c) Suppose $p(x) = 3x^2 - 7x + 5$. Then

$$p(2) = 12 - 14 + 5 = 3 \qquad \text{and} \qquad p(8) = 192 - 56 + 5 = 141$$

Hence $3 \equiv 141 \pmod 6$.

Arithmetic of Residue Classes

Addition and multiplication are defined for our residue classes modulo m as follows:

$$[a] + [b] = [a + b] \qquad \text{and} \qquad [a] \cdot [b] = [ab]$$

For example, consider the residue classes modulo $m = 6$; that is,

$$[0], [1], [2], [3], [4], [5]$$

Then

$$[2] + [3] = [5], \quad [4] + [5] = [9] = [3], \quad [2]\cdot[2] = [4], \quad [2]\cdot[5] = [10] = [4]$$

The content of Theorem 11.22 tells us that the above definitions are well defined, that is, the sum and product of the residue classes do not depend on the choice of representative of the residue class.

There are only a finite number m of residue classes modulo m. Thus one can easily write down explicitly their addition and multiplication tables when m is small. Figure 11-4 shows the addition and multiplication tables for the residue classes modulo $m = 6$. For notational convenience, we have omitted brackets and simply denoted the residue classes by the numbers 0, 1, 2, 3, 4, 5.

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

×	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Fig. 11-4

Integers Modulo m, $\mathbf{Z_m}$

The *integers modulo m*, denoted by $\mathbf{Z_m}$, refers to the set

$$\mathbf{Z_m} = \{0, 1, 2, 3, \ldots, m - 1\}$$

where addition and multiplication are defined by the arithmetic modulo m or, in other words, the corresponding operations for the residue classes. For example, Fig. 11-4 may also be viewed as the addition and multiplication tables for $\mathbf{Z_6}$, This means:

> There is no essential difference between $\mathbf{Z_m}$ and the arithmetic of the residue classes modulo m, and so they will be used interchangeably.

Cancellation Laws for Congruences

Recall that the integers satisfy the following:

Cancellation law: If $ab = ac$ and $a \neq 0$, then $b = c$.

The critical difference between ordinary arithmetic and arithmetic modulo m is that the above cancellation law is not true for congruences. For example,

$$3 \cdot 1 \equiv 3 \cdot 5 \pmod 6 \quad \text{but} \quad 1 \not\equiv 5 \pmod 6$$

That is, we cannot cancel the 3 even though $3 \not\equiv 0 \pmod 6$. However, we do have the following *Modified Cancellation Law* for our congruence relations.

Theorem 11.23 (Modified Cancellation Law): Suppose $ab \equiv ac \pmod m$ and $\gcd(a, m) = 1$.

Then $b \equiv c \pmod m$.

The above theorem is a consequence of the following more general result (proved in Problem 11.37).

Theorem 11.24: Suppose $ab \equiv ac \pmod m$ and $d = \gcd(a, m)$. Then $b \equiv c \pmod{m/d}$.

EXAMPLE 11.13 Consider the following congruence:

$$6 \equiv 36 \pmod{10} \tag{11.1}$$

Since $\gcd(3, 10) = 1$ but $\gcd(6, 10) \neq 1$, we can divide both sides of (11.1) by 3 but not by 6. That is,

$$2 \equiv 12 \pmod{10} \quad \text{but} \quad 1 \not\equiv 6 \pmod{10}$$

However, by Theorem 11.24, we can divide both sides of (11.1) by 6 if we also divide the modulus by 2 which equals gcd(6, 10). That is,

$$1 \equiv 6 \pmod 5$$

Remark: Suppose p is a prime. Then the integers 1 through $p - 1$ are relatively prime to p. Thus the usual cancellation law does hold when the modulus is a prime p. That is:

If $ab \equiv ac \pmod p$ and $a \not\equiv 0 \pmod p$, then $b \equiv c \pmod p$.

Thus $\mathbf{Z_p}$, the integers modulo a prime p, plays a very special role in number theory.

Reduced Residue Systems, Euler Phi Function

The modified cancellation law, Theorem 11.23, is indicative of the special role played by those integers which are relatively prime (coprime) to the modulus m. We note that a is coprime to m if and only if every element in the residue class $[a]$ is coprime to m. Thus we can speak of a residue class being coprime to m.

The number of residue classes relatively prime to m or, equivalently, the number of integers between 1 and m (inclusive) which are relatively prime to m is denoted by

$$\phi(m)$$

The function $\phi(m)$ is called the *Euler phi function*. The list of numbers between 1 and m which are coprime to m or, more generally, any list of $\phi(m)$ incongruent integers which are coprime to m, is called a *reduced residue system modulo m*.

EXAMPLE 11.14

(a) Consider the modulus $m = 15$. There are eight integers between 1 and 15 which are coprime to 15:

$$1, \quad 2, \quad 4, \quad 7, \quad 8, \quad 11, \quad 13, \quad 14$$

Thus $\phi(15) = 8$ and the above eight integers form a reduced residue system modulo 15.

(b) Consider any prime p. All the numbers $1, 2, \ldots, p-1$ are coprime to p; hence $\phi(p) = p - 1$.

A function f with domain the positive integers $\boldsymbol{N}$ is said to be *multiplicative* if, whenever a and b are relatively prime,

$$f(ab) = f(a)f(b)$$

The following theorem (proved in Problem 11.44) applies.

Theorem 11.25: Euler's phi function is multiplicative. That is, if a and b are relatively prime, then

$$\phi(ab) = \phi(a)\phi(b)$$

11.9 CONGRUENCE EQUATIONS

A *polynomial congruence equation* or, simply, a *congruence equation* (in one unknown x) is an equation of the form

$$a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \equiv 0 \pmod{m} \tag{11.2}$$

Such an equation is said to be of *degree n* if $a \not\equiv 0 \pmod{m}$.

Suppose $s \equiv t \pmod{m}$. Then s is a solution of (11.2) if and only if t is a solution of (11.2). Thus the *number of solutions* of (11.2) is defined to be the number of incongruent solutions or, equivalently, the number of solutions in the set

$$\{0, 1, 2, \ldots, m-1\}$$

Of course, these solutions can always be found by testing, that is, by substituting each of the m numbers into (11.2) to see if it does indeed satisfy the equation.

The *complete set of solutions* of (11.2) is a maximum set of incongruent solutions whereas the *general solution* of (11.2) is the set of all integral solutions of (11.2). The general solution of (11.2) can be found by adding all the multiples of the modulus m to any complete set of solutions.

EXAMPLE 11.15 Consider the equations:

(a) $x^2 + x + 1 \equiv 0 \pmod{4}$, (b) $x^2 + 3 \equiv 0 \pmod{6}$, (c) $x^2 - 1 \equiv 0 \pmod{8}$

Here we find the solutions by testing.

(a) There are no solutions since 0, 1, 2, and 3 do not satisfy the equation.

(b) There is only one solution among $0, 1, \ldots, 5$ which is 3. Thus the general solution consists of the integers $3 + 6k$ where $k \in \mathbf{Z}$.

(c) There are four solutions, 1, 3, 5, and 7. This shows that a congruence equation of degree n can have more than n solutions.

We emphasize that we are not only interested in studying congruence equations in order to find their solutions; this can always be found by testing. We are mainly interested in developing techniques to help us find such solutions, and a theory which tells us conditions under which solutions exist and the number of such solutions. Such a theory holds for linear congruence equations which we investigate below. We will also discuss the Chinese Remainder Theorem, which is essentially a system of linear congruence equations.

Remark 1: The coefficients of a congruence equation can always be reduced modulo m since an *equivalent* equation, that is, an equation with the same solutions, would result. For example, the following are equivalent equations since the coefficients are congruent modulo $m = 6$:

$$15x^2 + 28x + 14 \equiv 0 \pmod 6, \quad 3x^2 + 4x + 2 \equiv 0 \pmod 6, \quad 3x^2 - 2x + 2 \equiv 0 \pmod 6,$$

Usually we choose coefficients between 0 and $m - 1$ or between $-m/2$ and $m/2$

Remark 2: Since we are really looking for solutions of (11.2) among the residue classes modulo m rather than among the integers, we may view (11.2) as an equation over the integers modulo m, rather than an equation over $\mathbf{Z}$, the integers. In this context, the number of solutions of (11.2) is simply the number of solutions in $\mathbf{Z_m}$.

Linear Congruence Equation: $ax \equiv 1 \pmod m$

First we consider the special linear congruence equation

$$ax \equiv 1 \pmod m \tag{11.3}$$

where $a \not\equiv 0 \pmod m$. The complete story of this equation is given in the following theorem (proved in Problem 11.57).

Theorem 11.26: If a and m are relatively prime, then $ax \equiv 1 \pmod m$ has a unique solution; otherwise it has no solution.

EXAMPLE 11.16

(a) Consider the congruence equation $6x \equiv 1 \pmod{33}$. Since $\gcd(6, 33) = 3$, this equation has no solution.

(b) Consider the congruence equation $7x \equiv 1 \pmod 9$. Since $\gcd(7, 9) = 1$, the equation has a unique solution. Testing the numbers 0, 1, …, 8, we find that

$$7(4) = 28 \equiv 1 \pmod 9$$

Thus $x = 4$ is our unique solution. (The general solution is $4 + 9k$ for $k \in \mathbf{Z}$.)

Suppose a solution of (11.3) does exist, that is, suppose $\gcd(a, m) = 1$. Furthermore, suppose the modulus m is large. Then the Euclidean algorithm can be used to find a solution of (11.3). Specifically, we use the Euclidean algorithm to find x_0 and y_0 such that

$$ax_0 + my_0 = 1$$

From this it follows that $ax_0 \equiv 1 \pmod m$; that is, x_0 is a solution to (11.3).

EXAMPLE 11.17 Consider the following congruence equation:

$$81 \equiv 1 \pmod{256}$$

By observation or by applying the Euclidean algorithm to 81 and 256, we find that $\gcd(81, 256) = 1$. Thus the equation has a unique solution. Testing may not be an efficient way to find this solution since the modulus $m = 256$ is relatively large. Hence, we apply the Euclidean algorithm to $a = 81$ and $m = 256$. Specifically, as in Example 11.6, we find $x_0 = -25$ and $y_0 = 7$ such that

$$81x_0 + 256y_0 = 1$$

This means that $x_0 = -25$ is a solution of the given congruence equation. Adding $m = 256$ to -25, we obtain the following unique solution between 0 and 256:

$$x = 231$$

Linear Congruence Equation: $ax \equiv b \pmod{m}$

Now we consider the more general linear congruence equation

$$ax \equiv b \pmod{m} \tag{11.4}$$

where $a \not\equiv 0 \pmod{m}$. We first consider the case (proved in Problem 11.58) where a and m are coprime.

Theorem 11.27: Suppose a and m are relatively prime. Then $ax \equiv b \pmod{m}$ has a unique solution. Moreover, if s is the unique solution to $ax \equiv 1 \pmod{m}$, then the unique solution to $ax \equiv b \pmod{m}$ is $x = bs$.

EXAMPLE 11.18

(a) Consider the congruence equation $3x \equiv 5 \pmod{8}$. Since 3 and 8 are coprime, the equation has a unique solution. Testing the integers $0, 1, \ldots, 7$, we find that

$$3(7) = 21 \equiv 5 \pmod{8}$$

Thus $x = 7$ is the unique solution of the equation.

(b) Consider the linear congruence equation

$$33x \equiv 38 \pmod{280} \tag{11.5}$$

Since $\gcd(33, 280) = 1$, the equation has a unique solution. Testing may not be an efficient way to find this solution since the modulus $m = 280$ is relatively large. We apply the Euclidean algorithm to first find a solution to

$$33x \equiv 1 \pmod{280} \tag{11.6}$$

That is, as in Example 11.6, we find $x_0 = 17$ and $y_0 = 2$ to be a solution of

$$33x_0 + 280y_0 = 1$$

This means that $s = 17$ is a solution of (11.6). Then

$$sb = 17(38) = 646$$

is a solution of (11.5). Dividing 646 by $m = 280$, we obtain the remainder

$$x = 86$$

which is the unique solution 11.5 between 0 and 280. (The general solution is $86 + 280k$ with $k \in \mathbf{Z}$.)

The complete story of the general case of (11.4) is contained in the following theorem (proved in Problem 11.59).

Theorem 11.28: Consider the equation $ax \equiv b \pmod{m}$ where $d = \gcd(a, m)$.

(i) Suppose d does not divide b. Then $ax \equiv b \pmod{m}$ has no solution.

(ii) Suppose d does divide b. Then $ax \equiv b \pmod{m}$ has d solutions which are all congruent modulo M to the unique solution of

$$Ax \equiv B \pmod{M} \quad \text{where} \quad A = a/d,\ B = b/d,\ M = m/d.$$

We emphasize that Theorem 11.27 applies to the equation $Ax \equiv B \pmod{M}$ in Theorem 11.28 since $\gcd(A, M) = 1$.

EXAMPLE 11.19 Solve each congruence equation: (a) $4x \equiv 9 \pmod{14}$; (b) $8x \equiv 12 \pmod{28}$.

(a) Note $\gcd(4, 14) = 2$. However, 2 does not divide 9. Hence the equation does not have a solution.

(b) Note that $d = \gcd(8, 28) = 4$, and $d = 4$ does divide 12. Thus the equation has $d = 4$ solutions. Dividing each term in the equation by $d = 4$ we obtain the congruence equation (11.7) which has a unique solution.

$$2x \equiv 3 \pmod{7} \tag{11.7}$$

Testing the integers $0, 1, \ldots, 6$, we find that 5 is the unique solution of (11.7). We now add $d - 1 = 3$ multiples of 7 to the solution 5 of (11.7) obtaining:

$$5 + 7 = 12, \quad 5 + 2(7) = 19, \quad 5 + 3(7) = 26$$

Accordingly, 5, 12, 19, 26 are the required $d = 4$ solutions of the original equation $8x \equiv 12 \pmod{28}$.

Remark: The solution of equation (11.7) in Example 11.19 was obtained by inspection. However, in case the modulus m is large, we can always use the Euclidean algorithm to find its unique solution as in Example 11.17.

Chinese Remainder Theorem

An old Chinese riddle asks the following question.

> Is there a positive integer x such that when x is divided by 3 it yields a remainder 2, when x is divided by 5 it yields a remainder 4, and when x is divided by 7 it yields a remainder 6?

In other words, we seek a common solution of the following three congruence equations:

$$x \equiv 2 \pmod{3}, \quad x \equiv 4 \pmod{5}, \quad x \equiv 6 \pmod{7}$$

Observe that the moduli 3, 5, and 7 are pairwise relatively prime. (Moduli is the plural of modulus.) Thus the following theorem (proved in Problem 11.60) applies; it tells us that there is a unique solution modulo $M = 3 \cdot 5 \cdot 7 = 105$.

Theorem 11.29 (Chinese Remainder Theorem): Consider the system

$$x \equiv r_1 \pmod{m_1}, \quad x \equiv r_2 \pmod{m_2}, \quad \cdots, \quad x \equiv r_k \pmod{m_k} \tag{11.8}$$

where the m_i are pairwise relatively prime. Then the system has a unique solution modulo $M = m_1 m_2 \cdots m_k$.

One can actually give an explicit formula for the solution of the system (11.8) in Theorem 11.29 which we state as a proposition.

Proposition 11.30: Consider the system (11.8) of congruence equations. Let $M = m_1 m_2 \ldots m_k$, and

$$M_1 = \frac{M}{m_1}, \quad M_2 = \frac{M}{m_2}, \ \ldots, \quad M_k = \frac{M}{m_k}$$

(Then each pair M_i and m_i are co-prime.) Let $s_1, s_2, \ldots, s_k$ be the solutions respectively, of the congruence equations

$$M_1 x \equiv 1 \pmod{m_1}, \ M_2 x \equiv 1 \pmod{m_2}, \ldots, \ M_k x \equiv 1 \pmod{m_k}$$

Then the following is a solution of the system (11.8):

$$x_0 = M_1 s_1 r_1 + M_2 s_2 r_2 + \cdots + M_k s_k r_k \tag{11.9}$$

We now solve the original riddle in two ways.

Method 1: First we apply the Chinese Remainder Theorem (CRT) to the first two equations,

$$\text{(a) } x \equiv 2 \pmod 3 \qquad \text{and} \qquad \text{(b) } x \equiv 4 \pmod 5$$

CRT tells us there is a unique solution modulo $M = 3 \cdot 5 = 15$. Adding multiples of the modulus $m = 5$ to the given solution $x = 4$ of the second equation (b), we obtain the following three solutions of (b) which are less than 15:

$$4, \quad 9, \quad 14$$

Testing each of these solutions in equation (a), we find that 14 is the only solution of both equations. Now we apply the same process to the two equations

$$\text{(c) } x \equiv 14 \pmod{15} \quad \text{and} \quad \text{(d) } x \equiv 6 \pmod 7$$

CRT tells us there is a unique solution modulo $M = 15 \cdot 7 = 105$. Adding multiples of the modulus $m = 15$ to the given solution $x = 14$ of the first equation (c), we obtain the following seven solutions of (b) which are less than 105:

$$14, \quad 29, \quad 44, \quad 59, \quad 74, \quad 89, \quad 104$$

Testing each of these solutions of (c) in the second equation (d) we find that 104 is the only solution of both equations. Thus the smallest positive integer satisfying all three equations is

$$x = 104$$

This is the solution of the riddle.

Method 2: Using the above notation, we obtain

$$M = 3 \cdot 5 \cdot 7 = 105, \quad M_1 = 105/3 = 35, \quad M_2 = 105/5 = 21, \quad M_3 = 105/7 = 15$$

We now seek solutions to the equations

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

Reducing 35 modulo 3, reducing 21 modulo 5, and reducing 15 modulo 7, yields the system

$$2x \equiv 1 \pmod 3, \quad x \equiv 1 \pmod 5, \quad x \equiv 1 \pmod 7$$

The solutions of these three equations are, respectively,

$$s_1 = 2, \quad s_2 = 1, \quad s_3 = 1$$

We now substitute into the formula (11.9) to obtain the following solution of our original system:

$$x_0 = 35 \cdot 2 \cdot 2 + 21 \cdot 1 \cdot 4 + 15 \cdot 1 \cdot 6 = 314$$

Dividing this solution by the modulus $M = 105$, we obtain the remainder

$$x = 104$$

which is the unique solution of the riddle between 0 and 105.

Remark: The above solutions $s_1 = 2$, $s_2 = 1$, $s_3 = 1$ were obtained by inspection. If the moduli are large, we can always use the Euclidean algorithm to find such solutions as in Example 11.17.

Solved Problems

INEQUALITIES, ABSOLUTE VALUE

11.1. Insert the correct symbol, $<$, $>$, or $=$, between each pair of integers:

(*a*) 4 ____ -7; (*b*) -2 _____ -9; (*c*)$(-3)^2$ ____ 9; (*d*) -8 ____ 3,

For each pair of integers, say a and b, determine their relative positions on the number line **R**; or, alternatively, compute $b - a$, and write $a < b$, $a > b$, or $a = b$ according as $b - a$ is positive, negative, or zero. Hence:

(*a*) $4 > -7$; (*b*) $-2 > -9$; (*c*) $(-3)^2 = 9$; (d) $-8 < 3$.

11.2. Evaluate: (*a*) $|2-5|$, $|-2+5|$, $|-2-5|$; (*b*) $|5-8|+|2-4|$, $|4-3|-|3-9|$.
Evaluate inside the absolute value sign first:

(*a*) $|2-5| = |-3| = 3$, $|-2+5| = |3| = 3$, $|-2-5| = |-7| = 7$

(*b*) $|5-8|+|2-4| = |-3|+|-2| = 3+2 = 5$; $|4-3|-|3-9| = |1|-|-6| = 1-6 = -5$

11.3. Find the distance d between each pair of integers:
(*a*) 3 and –7; (*b*) –4 and 2; (*c*) 1 and 9; (*d*) –8 and –3; (*e*) –5 and –8.

The distance d between a and b is given by $d = |a-b| = |b-a|$. Alternatively, as indicated by Fig. 11-5, $d = |a| + |b|$ when a and b have different signs, and $d = |a| - |b|$ when a and b have the same sign and $|a| > |b|$. Thus: (*a*) $d = 3+7 = 10$; (*b*) $d = 4+2 = 6$; (*c*) $d = 9-1 = 8$; (*d*) $d = 8-3 = 5$; (*e*) $d = 8-5 = 3$.

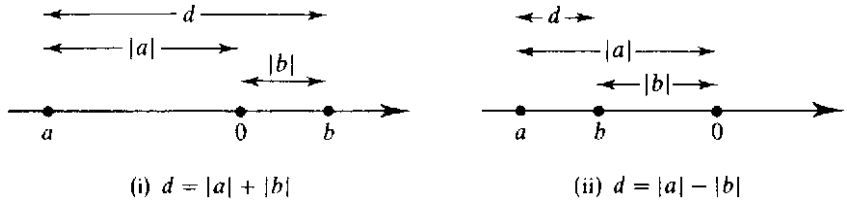

Fig. 11-5

11.4. Find all integers n such that: (*a*) $1 < 2n - 6 < 14$; (*b*) $2 < 8 - 3n < 18$.

(*a*) Add 6 to the "three sides" to get $7 < 2n < 20$. Then divide all sides by 2 (or multiply by 1/2) to get $3.5 < n < 10$. Hence $n = 4, 5, 6, 7, 8, 9$.

(*b*) Add –8 to the three sides to get $-6 < -3n < 10$. Divide by –3 (or multiply by –1/3) and, since –3 is negative, change the direction of the inequality to get

$$2 > n > -3.3 \quad \text{or} \quad -3.3 < n < 2$$

Hence $n = -3, -2, -1, 0, 1$.

11.5. Prove Proposition 11.3: Suppose $a \leq b$, and c is any integer. Then: (i) $a + c \leq b + c$, (ii) $ac = bc$ when $c > 0$; but $ac = bc$ when $c < 0$.

The proposition is certainly true when $a = b$. Hence we need only consider the case when $a < b$, that is, when $b - a$ is positive.

(i) The following difference is positive: $(b + c) - (a + c) = b - a$. Hence $a + c < b + c$.

(ii) Suppose c is positive. By property $[\mathbf{P_1}]$ of the positive integers $\mathbf{N}$, the product $c(b - a)$ is also positive. Thus $ac < bc$.

Now suppose c is negative. Then $-c$ is positive, and the product $(-c)(b-a) = ac-bc$ is also positive. Accordingly, $bc < ac$, whence $ac > bc$.

11.6. Prove Proposition 11.4 (iii): $|ab| = |a||b|$.

The proof consists of analysing the following five cases: (*a*) $a = 0$ or $b = 0$; (*b*) $a > 0$ and $b > 0$; (*c*) $a > 0$ and $b < 0$; (*d*) $ba < 0$ and $b > 0$; (*e*) $ba < 0$ and $b < 0$. We only prove the third case here. (*c*) Since $a > 0$ and $b < 0$, $|a| = a$ and $|b| = -b$. Also $ab < 0$. Hence $|ab| = -(ab) = a(-b) = |a||b|$.

11.7 Prove Proposition 11.4 (iv): $|a \pm b| \leq |a| + |b|$.

Now $ab \leq |ab| = |a||b|$, and so $2ab \leq 2|a||b|$. Hence

$$(a + b)^2 = a^2 + 2ab + b^2 \leq |a|^2 + 2|a||b| + |b|^2 = (|a| + |b|)^2$$

But $\sqrt{(a + b)^2} = |a + b|$. Thus the square root of the above yields $|a + b| \leq |a| + |b|$. Also,

$$|a - b| = |a + (-b)| \leq |a| + |-b| = |a| + |b|$$

MATHEMATICAL INDUCTION, WELL-ORDERING PRINCIPLE

11.8. Prove the proposition that the sum of the first n positive integers is $n(n + 1)/2$; that is:

$$P(n): \quad 1 + 2 + \cdots + n = \frac{1}{2}n(n + 1)$$

$P(1)$ is true since $1 = \frac{1}{2}(1)(1 + 1)$. Assuming $P(k)$ is true, we add $k + 1$ to both sides of $P(k)$ obtaining

$$\begin{aligned} 1 + 2 + 3 + \cdots + k + (k + 1) &= \frac{1}{2}k(k + 1) + (k + 1) = \frac{1}{2}[k(k + 1) + 2(k + 1)] \\ &= \frac{1}{2}[(k + 1)(k + 2)] \end{aligned}$$

This is $P(k + 1)$. Accordingly, $P(k + 1)$ is true whenever $P(k)$ is true. By the principle of mathematical induction, P is true for every $n \in \mathbf{N}$.

11.9. Suppose $a \neq 1$. Show P is true for all $n \geq 1$ where P is defined as follows:

$$P(n): \quad 1 + a + a^2 + \cdots + a^n = \frac{a^{n+1} - 1}{a - 1}$$

$P(1)$ is true since

$$1 + a = \frac{a^2 - 1}{a - 1}$$

Assuming $P(k)$ is true, we add a^{k+1} to both sides of $P(k)$, obtaining

$$\begin{aligned} 1 + a + a^2 + \ldots + a^k + a^{k+1} &= \frac{a^{k+1} - 1}{a - 1} + a^{k+1} = \frac{a^{k+1} - 1 + (a - 1)a^{k+1}}{a - 1} \\ &= \frac{a^{k+2} - 1}{a - 1} \end{aligned}$$

This is $P(k + 1)$. Thus, $P(k + 1)$ is true whenever $P(k)$ is true. By the principle of mathematical induction, P is true for every $n \in \mathbf{N}$.

11.10. Suppose n is a positive integer. Prove $n \geq 1$. (This is not true for the rational numbers $\mathbf{Q}$.) In other words, if $P(n)$ is the statement that $n \geq 1$, then $P(n)$ is true for every $n \in \mathbf{N}$.

$P(n)$ holds for $n = 1$ since $1 \geq 1$. Assuming $P(k)$ is true, that is, $k \geq 1$, add 1 to both sides to obtain

$$k + 1 \geq 1 + 1 = 2 > 1$$

This is $P(k+1)$. Thus $P(k+1)$ is true whenever $P(k)$ is true. By the principle of mathematical induction, P is true for every $n \in \mathbf{N}$.

11.11. Suppose a and b are positive integers. Prove:

(*a*) If $b \neq 1$, then $a < ab$.

(*b*) If $ab = 1$, then $a = 1$ and $b = 1$.

(*c*) If n is composite, then $n = ab$ where $1 < a, b < n$.

(*a*) By Problem 11.10, $b > 1$. Hence $b - 1 > 0$, that is, $b - 1$ is positive. By the property $[\mathbf{P}_1]$ of the positive integers $\mathbf{N}$, the following product is also positive:

$$a(b-1) = ab - a$$

Thus $a < ab$, as required.

(*b*) Suppose $b \neq 1$. By (*a*), $a < ab = 1$. This contradicts Problem 11.10; hence $b = 1$. It then follows that $a = 1$.

(*c*) If n is not prime, then n has a positive divisor a such that $a \neq 1$ and $a \neq n$. Then $n = ab$ where $b \neq 1$ and $b \neq n$. Thus, by Problem 11.10 and by part (a), $1 < a, b < ab = n$.

11.12. Prove Theorem 11.6 (Well-Ordering Principle): Let S be a nonempty set of positive integers. Then S contains a least element.

Suppose S has no least element. Let M consist of those positive integers which are less than every element of S. Then $1 \in M$; otherwise, $1 \in S$ and 1 would be a least element of S. Suppose $k \in M$. Then k is less than every element of S. Therefore $k + 1 \in M$; otherwise $k + 1$ would be a least element of S.

By the Principle of Mathematical Induction, M contains every positive integer. Thus S is empty which contradicts the hypothesis that S is nonempty. Accordingly, the original assumption that S has no least element cannot be true. Thus the theorem is true.

11.13. Prove Theorem 11.5 (Induction: Second Form): Let P be a proposition defined on the integers $n \geq 1$ such that: (i) $P(1)$ is true. (ii) $P(k)$ is true whenever $P(j)$ is true for all $1 \leq j < k$.

Then P is true for all $n \geq 1$.

Let A be the set of integers $n \geq 1$ for which P is not true. Suppose A is not empty. By the Well-Ordering Principle, A contains at least element a_0 By (i), $a_0 \neq 1$.

Since a_0 is the least element of A, P is true for every integer j where $1 \leq j < a_0$. By (ii), P is true for a_0. This contradicts the fact that $a_0 \in A$. Hence A is empty, and so P is true for every integer $n > 1$.

DIVISION ALGORITHM

11.14. For each pair of integers a and b, find integers q and r such that $a = bq + r$ and $0 < r < |b|$:

(*a*) $a = 258$ and $b = 12$; (*b*) $a = 573$ and $b = -16$.

(*a*) Here a and b are positive. Simply divide a by b, that is, 258 by 12, say by long division, to obtain the quotient $q = 21$ and remainder $r = 6$. Alternately, using a calculator, we get

$$258/12 = 21.5, \quad q = INT(a/b) = 21, \quad r = a - bq = 258 - 12(21) = 6$$

(*b*) Here a is positive, but b is negative. Divide a by $|b|$, that is, 573 by 16, say with a calculator to obtain:

$$a/|b| = 573/16 = 35.8125, \quad q' = INT(a/|b|) = 35, \quad r' = 573 - 16(35) = 13$$

Then

$$573 = (16)(35) + 13 \quad \text{and} \quad 573 = (-16)(-35) + 13$$

Thus $q = -35$ and $r = 13$.

11.15. For each pair of integers a and b, find integers q and r such that $a = bq + r$ and $0 < r < |b|$:

(*a*) $a = -381$ and $b = 14$; (*b*) $a = -433$ and $b = -17$.

Here a is negative in each case, hence we have to make some adjustments to be sure that $0 < r < |b|$.

(*a*) Divide $|a| = 381$ by $b = 14$, say with a calculator, to obtain the quotient $q' = 27$ and remainder $r' = 3$. Then

$$381 = (14)(27) + 3 \quad \text{and so} \quad -381 = (14)(-27) - 3$$

But -3 is negative and cannot be the remainder r; hence we add and subtract $b = 14$ as follows:

$$-381 = (14)(-27) - 14 + 14 - 3 = (14)(-28) + 11$$

Thus $q = -28$ and $r = 11$.

(*b*) Divide $|a| = 433$ by $|b| = 17$, say by a calculator, to obtain the quotient $q' = 25$ and remainder $r' = 8$. Then:

$$433 = (17)(25) + 8 \quad \text{and so} \quad -433 = (-17)(25) - 8$$

But –8 is negative and cannot be the remainder r; we correct this by adding and subtracting $|b| = 17$ as follows:

$$-433 = (-17)(25) - 17 + 17 - 8 = (-17)(26) + 9$$

Thus $q = 26$ and $r = 9$.

11.16. Prove $\sqrt{2}$ is not rational, that is, $\sqrt{2} \neq a/b$ where a and b are integers.

Suppose $\sqrt{2}$ is rational and $\sqrt{2} = a/b$ where a and b are integers reduced to lowest terms, i.e., $\gcd(a, b) = 1$. Squaring both sides yields

$$2 = \frac{a^2}{b^2} \quad \text{or} \quad a^2 = 2b^2$$

Then 2 divides a^2. Since 2 is a prime, 2 also divides a. Say $a = 2c$. Then

$$2b^2 = a^2 = 4c^2 \quad \text{or} \quad b^2 = 2c^2$$

Then 2 divides b^2. Since 2 is a prime 2 also divides b. Thus 2 divides both a and b. This contradicts the assumption that $\gcd(a, b) = 1$. Therefore, $\sqrt{2}$ is not rational.

11.17. Prove Theorem 11.8 (Division Algorithm) for the case of positive integers. That is, assuming a and b are positive integers, prove there exist nonnegative integers q and r such that

$$a = bq + r \qquad \text{and} \qquad 0 \leq r < b \tag{11.10}$$

If $a < b$, choose $q = 0$ and $r = a$. If $a = b$, choose $q = 1$ and $r = 0$. In either case, q and r satisfy (11.10).

The proof is now by induction on a. If $a = 1$ then $a < b$ or $a = b$; hence the theorem holds when $a = 1$. Suppose $a > b$. Then $a - b$ is positive and $a - b < a$. By induction, the theorem holds for $a - b$. Thus there exists q' and r' such that

$$a - b = bq' + r' \qquad \text{and} \qquad 0 \leq r' < b$$

Then

$$a = bq' + b + r' = b(q' + 1) + r'$$

Choose $q = q' + 1$ and $r = r'$. Then q and r are nonnegative integers and satisfy (11.10). Thus the theorem is proved.

11.18. Prove Theorem 11.8 (Division Algorithm): Let a and b be integers with $b \neq 0$. Then there exists integers q and r such that $a = bq + r$ and $0 \leq r' < |b|$. Also, the integers q and r are unique.

Let M be the set of nonnegative integers of the form a $-xb$ for some integer x. If $x = -|a|b$ then $a - xb$ is nonnegative; hence M is nonempty. By the Well-Ordering Principle, M has a least element, say r. Since $r \in M$, we have

$$r \geq 0 \qquad \text{and} \qquad r = a - qb$$

for some integer q. We need only show that $r < |b|$. Suppose $r \geq |b|$. Let $r' = r - |b|$.

Then $r' \geq 0$ and also $r' < r$ because $b \neq 0$. Furthermore,

$$r' = r - |b| = a - qb - |b| = \begin{cases} a - (q+1)b, & \text{if } b < 0 \\ a - (q-1)b, & \text{if } b > 0 \end{cases}$$

In either case, r' belongs to M. This contradicts the fact that r is the least element of M Accordingly, $r < |b|$. Thus the existence of q and r is proved.

We now show that q and r are unique. Suppose there exist integers q and r and q' and r' such that

$$a = bq + r \quad \text{and} \quad a = bq' + r' \quad \text{where} \quad 0 < r, r' < |b|$$

Then $bq + r = bq' + r'$; hence

$$b(q - q') = r' - r$$

Thus b divides $r' - r$. But $|r' - r| < |b|$ since $0 < r$, $r' < |b|$. Accordingly, $r' - r = 0$. Since $b \neq 0$ this implies $q - q' = 0$. Consequently, $r' = r$ and $q' = q$; that is, q and r are uniquely determined by a and b.

DIVISIBILITY, PRIMES, GREATEST COMMON DIVISOR

11.19. Find all positive divisors of: (*a*) 18; (*b*) $256 = 2^8$; (*c*) $392 = 2^3 \cdot 7^2$.

(*a*) Since 18 is relatively small, we simply write down all positive integers (≤ 18) which divide 18. These are:

$$1, \quad 2, \quad 3, \quad 6, \quad 9, \quad 18$$

(*b*) Since 2 is a prime, the positive divisors of $256 = 2^8$ are simply the lower powers of 2, i.e.,

$$2^0, \quad 2^1, \quad 2^2, \quad 2^3, \quad 2^4, \quad 2^5, \quad 2^6, \quad 2^7, \quad 2^8$$

In other words, the positive divisors of 256 are:

$$1, \quad 2, \quad 4, \quad 8, \quad 16, \quad 32, \quad 64, \quad 128, \quad 256$$

(*c*) Since 2 and 7 are prime, the positive divisors of $392 = 2^3 \cdot 7^2$ are products of lower powers of 2 times lower powers of 7, i.e.,

$$2^0 \cdot 7^0, \quad 2^1 \cdot 7^0, \quad 2^2 \cdot 7^0, \quad 2^3 \cdot 7^0, \quad 2^0 \cdot 7^1, \quad 2^1 \cdot 7^1, \quad 2^2 \cdot 7^1, \quad 2^3 \cdot 7^1,$$
$$2^0 \cdot 7^2, \quad 2^1 \cdot 7^2, \quad 2^2 \cdot 7^2, \quad 2^3 \cdot 7^2$$

In other words, the positive powers of 392 are:

$$1, \quad 2, \quad 4, \quad 8, \quad 7, \quad 14, \quad 28, \quad 56, \quad 49, \quad 98, \quad 196, \quad 392.$$

(We have used the usual convention that $n^0 = 1$ for any nonzero number n.)

11.20. List all primes between 50 and 100.

Simply list all numbers p between 50 and 100 which cannot be written as a product of two positive integers, excluding 1 and p. This yields:

$$51, \quad 53, \quad 57, \quad 59, \quad 61, \quad 67, \quad 71, \quad 73, \quad 79, \quad 83, \quad 87, \quad 89, \quad 91, \quad 93, \quad 97$$

11.21. Let $a = 8316$ and $b = 10\,920$.

(a) Find $d = \gcd(a, b)$, the greatest common divisor of a and b.

(b) Find integers m and n such that $d = ma + nb$.

(c) Find $\text{lcm}(a, b)$, the least common multiple of a and b.

(a) Apply the Euclidean algorithm to a and b. That is, apply the division algorithm to a and b and then repeatedly apply the division algorithm to each quotient and remainder until obtaining a zero remainder. These steps are pictured in Fig. 11-6(a) using long division and also in Fig. 11-6(b) where the arrows indicate the quotient and remainder in the next step. The last nonzero remainder is 84. Thus $84 = \gcd(8316, 10\,920)$.

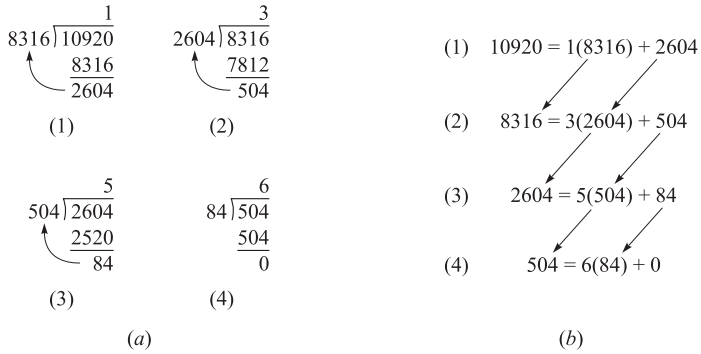

Fig. 11-6

(b) Now find m and n such that $84 = 8316m + 1092n$ by "unraveling" the above steps in the Euclidean algorithm. Specifically, the first three quotients in Fig. 11-6 yields the equations:

$$(1)\ 2604 = 10\,920 - 1(8316); \quad (2)\ 504 = 8316 - 3(2604); \quad (3)\ 84 = 2604 - 5(504).$$

Equation (3) tells us that $d = 84$ is a linear combination of 2604 and 504. Use (2) to replace 5044 in (3) so 84 can be written as a linear combination of 2604 and 8316 as follows:

$$\begin{aligned}(5)\ 84 &= 2604 - 5[8316 - 3(2604)] = 2604 - 5(8316) + 15(2604)\\ &= 16(2604) - 5(8316)\end{aligned}$$

Now use (1) to replace 2604 in (5) so 84 can be written as a linear combination of 8316 and 10 290 as follows:

$$\begin{aligned}(6)\ 84 &= 16[10\,920 - 1(8316)] - 5(8316) = 16(10\,920) - 16(8316) - 5(8316)\\ &= -21(8316) + 16(10\,920)\end{aligned}$$

This is our desired linear combination. In other words, $m = -21$ and $n = 16$.

(c) By Theorem 11.16,

$$\text{lcm}(a, b) = \frac{|ab|}{\gcd(a, b)} = \frac{(8316)(10\,920)}{84} = 1\,081\,080$$

11.22. Find the unique factorization of each number: (a) 135; (b) 1330; (c) 3105; (d) 211.

(a) $135 = 5{\cdot}27 = 5{\cdot}3{\cdot}3{\cdot}3$ or $135 = 3^3{\cdot}5$.

(b) $1330 = 2{\cdot}665 = 2{\cdot}5{\cdot}133 = 2{\cdot}5{\cdot}7{\cdot}19$.

(c) $3105 = 5{\cdot}621 = 5{\cdot}3{\cdot}207 = 5{\cdot}3{\cdot}3{\cdot}69 = 5{\cdot}3{\cdot}3{\cdot}3{\cdot}23$, or $3105 = 3^3{\cdot}5{\cdot}23$.

(d) None of the primes 2, 3, 5, 7, 11, 13 divides 211; hence 211 cannot be factored, that is, 211 is a prime.

(**Remark**: We need only test those primes less than $\sqrt{211}$.)

11.23. Let $a = 2^3 \cdot 3^5 \cdot 5^4 \cdot 11^6 \cdot 17^3$ and $b = 2^5 \cdot 5^3 \cdot 7^2 \cdot 11^4 \cdot 13^2$. Find $\gcd(a, b)$ and $\text{lcm}(a, b)$.

Those primes p_i which appear in both a and b will also appear in $\gcd(a, b)$. Furthermore, the exponent of p_i in $\gcd(a, b)$ will be the smaller of its exponents in a and b. Hence

$$\gcd(a, b) = 2^3 \cdot 5^3 \cdot 11^4$$

Those primes p_i which appear in either a or b will also appear in $\text{lcm}(a, b)$. Also, the exponent of p_i in $\text{lcm}(a, b)$ will be the larger of its exponent in a and b. Hence

$$\text{lcm}(a, b) = 2^5 \cdot 3^5 \cdot 5^4 \cdot 7^2 \cdot 11^6 \cdot 13^2 \cdot 17^3$$

11.24. Prove Theorem 11.9: Suppose a, b, c are integers.

(i) If $a \mid b$ and $b \mid c$, then $a \mid c$.
(ii) If $a \mid b$ then, for any integer x, $a \mid bx$.
(iii) If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$ and $a \mid (b - c)$.
(iv) If $a \mid b$ and $b \neq 0$, then $a = \pm b$ or $|a| < |b|$.
(v) If $a \mid b$ and $b \mid a$, then $|a| = |b|$, that is, $a = \pm b$.
(vi) If $a \mid 1$, then $a = \pm 1$.

(i) If $a \mid b$ and $b \mid c$, then there exist integers x and y such that $ax = b$ and $by = c$. Replacing b by ax, we obtain $axy = c$. Hence $a \mid c$.

(ii) If $a \mid b$, then there exists an integer c such that $ac = b$. Multiplying the equation by x, we obtain $acx = bx$. Hence $a \mid bx$.

(iii) If $a \mid b$ and $a \mid c$, then there exist integers x and y such that $ax = b$ and $ay = c$. Adding the equalities, we obtain

$$ax + ay = b + c \qquad \text{and so} \qquad a(x + y) = b + c$$

Hence $a \mid (b + c)$. Subtracting the equalities $ay = b$ and $by = c$, we obtain

$$ax - ay = b - c \quad \text{and so} \quad a(x - y) = b - c.$$

Thus $a \mid (b - c)$.

(iv) If $a \mid b$, then there exists c such that $ac = b$. Then

$$|b| = |ac| = |a||c|$$

Hence either $|c| = 1$ or $|a| < |a||c| = |b|$. If $|c| = 1$, then $c = \pm 1$; where $a = \pm b$, as required.

(v) If $a \mid b$, then $a = \pm b$ or $|a| < |b|$. If $|a| < |b|$ then $b \mid a$. Hence $a = \pm b$.

(vi) If $a \mid 1$, then $a = \pm 1$ or $|a| < |1| = 1$. By Problem 11.11, $|a| \geq 1$. Therefore, $a = \pm 1$.

11.25. A nonempty subset J of $\mathbf{Z}$ is called an *ideal* if J has the following two properties:

(1) If $a, b \in J$, then $a + b \in J$. (2) If $a \in J$ and $n \in \mathbf{Z}$, then $na \in J$.

Let d be the least positive integer in an ideal $J \neq \{0\}$. Prove that d divides every element of J.

Since $J \neq \{0\}$, there exists $a \in J$ with $a \neq 0$. Then $-a = (-1)a \in J$. Thus J contains positive elements. By the Well-Ordering Principle, J contains a least positive integer, so d exists. Now let $b \in J$. Dividing b by d, the division algorithm tells us there exist q and r such that

$$b = qd + r \quad \text{and} \quad 0 \leq r < d$$

Now $b, d \in J$ and J is an ideal; hence $b + (-q)d = r$ also belongs to J. By the minimal property of d, we must have $r = 0$. Hence $d \mid b$, as required.

11.26. Prove Theorem 11.13: Let d be the smallest positive integer of the form $ax + by$. Then $d = \gcd(a, b)$.

Consider the set $J = \{ax + yb \mid x, y \in \mathbf{Z}\}$. Then

$$a = 1(a) + 0(b) \in J \quad \text{and} \quad b = 0(a) + 1(b) \in J$$

Also, suppose $s, t \in J$, say, $s = x_1a + y_1b$ and $t = x_2a + y_2b$. Then, for any $n \in \mathbf{Z}$, the following belong to J:

$$s + t = (x_1 + x_2)a + (y_1 + y_2)b \quad \text{and} \quad ns = (nx_1)a + (ny_1)b$$

Thus J is an ideal. Let d be the least positive element in J. We claim $d = \gcd(a, b)$.

By the preceding Problem 11.25, d divides every element of J. Thus, in particular, d divides a and b. Now suppose h divides both a and b. Then h divides $xa + yb$ for any x and y; that is, h divides every element of J. Thus h divides d, and so $h \leq d$. Accordingly, $d = \gcd(a, b)$.

11.27. Prove Theorem 11.17: Suppose $\gcd(a, b) = 1$, and a and b divide c. Then ab divides c.

Since $\gcd(a, b) = 1$, there exist x and y such that $ax + by = 1$. Since $a \mid c$ and $b \mid c$, there exist m and n such that $c = ma$ and $c = nb$. Multiplying $ax + by = 1$ by c yields

$$acx + bcy = c \quad \text{or} \quad a(nb)x + b(ma)y = c \quad \text{or} \quad ab(nx + my) = c$$

Thus ab divides c.

11.28. Prove Corollary 11.19: Suppose a prime p divides a product ab. Then $p \mid a$ or $p \mid b$.

Suppose p does not divide a. Then $\gcd(p, a) = 1$ since the only divisors of p are ± 1 and $\pm p$. Thus there exist integers m and n such that $1 = mp + nq$. Multiplying by b yields $b = mpb + nab$. By hypothesis, $p|ab$, say, $ab = cp$. Then:

$$b = mpb + nab = mpb + ncp = p(mb + nc).$$

Hence $p \mid b$, as required.

11.29. Prove: (*a*) Suppose $p \mid q$ where p and q are primes. Then $p = q$.
(*b*) Suppose $p \mid q_1q_2 \cdots q_r$ where p and the q's are primes. Then p is equal to one of the q's.

(*a*) The only divisors of q are ± 1 and $\pm q$. Since $p > 1$, $p = q$.

(*b*) If $r = 1$, then $p = q_1$ by (a). Suppose $r > 1$. By Problem 11.28 (Corollary 11.19) $p \mid q_1$ or $p \mid (q_2 \cdots q_r)$. If $p \mid q_1$, then $p = q_1$ by (a). If not, then $p \mid (q_2 \cdots q_r)$. We repeat the argument. That is, we get $p = p_2$ or $p \mid (q_3 \cdots q_r)$. Finally (or by induction) p must equal one of the q's.

11.30. Prove the Fundamental Theorem of Arithmetic (Theorem 11.20): Every integer $n > 1$ can be expressed uniquely (except for order) as a product of primes.

We already proved Theorem 11.11 that such a product of primes exists. Hence we need only show that such a product is unique (except for order). Suppose

$$n = p_1p_2 \cdots p_k = q_1q_2 \cdots q_r$$

where the p's and q's are primes. Note that $p_1 \mid (q_1q_2 \cdots q_r)$. By the preceding Problem 11.29, p_1 equals one of the q's. We rearrange the q's so that $p_1 = q_1$. Then

$$p_1p_2 \cdots p_k = p_1q_2 \cdots q_r \quad \text{and so} \quad p_2 \cdots p_k = q_2 \cdots q_r$$

By the same argument, we can rearrange the remaining q's so that $p_2 = q_2$. And so on. Thus n can be expressed uniquely as a product of primes (except for order).

CONGRUENCES

11.31. Which of the following are true?

(*a*) $446 \equiv 278 \pmod 7$, (*c*) $269 \equiv 413 \pmod{12}$, (*e*) $445 \equiv 536 \pmod{18}$
(*b*) $793 \equiv 682 \pmod 9$, (*d*) $473 \equiv 369 \pmod{26}$, (*f*) $383 \equiv 126 \pmod{15}$

Recall $a \equiv b \pmod m$ if and only if m divides $a - b$.

(*a*) Find the difference $446 - 278 = 168$. Divide the difference 168 by the modulus $m = 7$. The remainder is 0; hence the statement is true,

(*b*) Divide the difference $793 - 682 = 111$ by the modulus $m = 9$. The remainder is not 0; hence the statement is false.

(*c*) True; since 12 divides $269 - 413 = -144$.

(*d*) True; since 26 divides $472 - 359 = 104$.

(*e*) False; since 18 does not divide $445 - 536 = -91$.

(*f*) False; since 15 does not divide $383 - 126 = 157$.

11.32. Find the smallest integer in absolute value which is congruent modulo $m = 7$ to each of the following numbers: (*a*) 386; (*b*) 257; (*c*) -192; (*d*) -466.

The integer should be in the set $\{-3, -2, -1, 0, 1, 2, 3\}$.

(*a*) Dividing 386 by $m = 7$ yields a remainder 1; hence $386 \equiv 1 \pmod 7$.

(*b*) Dividing 257 by $m = 7$ yields a remainder 5; hence $257 \equiv 5 \equiv -2 \pmod 7$. (We obtain -2 by subtracting the modulus $m = 7$ from 5.)

(*c*) Dividing 192 by $m = 7$ yields a remainder 3; hence $-192 \equiv -3 \pmod 7$.

(*d*) Dividing 466 by $m = 7$ yields a remainder 4; hence $-466 \equiv -4 \equiv 3 \pmod 7$. (We obtain 3 by adding the modulus $m = 7$ to -4.)

11.33. Find all numbers between -50 and 50 which are congruent to 21 modulo $m = 12$, that is, find all x such that $-50 \le x \le 50$ and $x \equiv 21 \pmod{12}$.

Add and subtract multiples of the modulus $m = 12$ to the given number 21 to obtain:

$$21 + 0 = 21, \quad 21 + 12 = 33, \quad 33 + 12 = 46, \quad 21 - 12 = 9$$
$$9 - 12 = -3, \quad -3 - 12 = -15, \quad -15 - 12 = -27, \quad -27 - 12 = -39$$

That is: $-39, -27, -15, -3, 9, 21, 33, 46$

11.34. Prove Theorem 11.21: Let m be a positive integer. Then:

(i) For any integer a, we have $a \equiv a \pmod m$.

(ii) If $a \equiv b \pmod m$, then $b \equiv a \pmod m$.

(iii) If $a \equiv b \pmod m$ and $b \equiv c \pmod m$, then $a \equiv c \pmod m$.

(i) The difference $a - a = 0$ is divisible by m; hence $a \equiv a \pmod m$.

(ii) If $a \equiv b \pmod m$, then $m \mid (a - b)$. Hence m divides $-(a - b) = b - a$. Therefore, $b \equiv a \pmod m$.

(iii) We are given $m \mid (a - b)$ and $m \mid (b - c)$. Hence m divides the sum $(a - b) + (b - c) = a - c$. Therefore, $a \equiv c \pmod m$.

11.35. Prove Theorem 11.22: Suppose $a \equiv c \pmod m$ and $b \equiv d \pmod m$. Then:

(i) $a + b \equiv c + d \pmod m$. (ii) $a \cdot b \equiv c \cdot d \pmod m$.

We are given that $m|(a - c)$ and $m|(b - d)$.

(i) Then m divides the sum $(a - c) + (b - d) = (a + b) - (c + d)$. Hence $a + b \equiv c + d \pmod m$.

(ii) Then m divides $b(a - c) = ab - bc$ and m divides $c(b - d) = bc - cd$. Thus m divides the sum $(ab - bc) + (bc - cd) = ab - cd$. Thus $ab \equiv cd \pmod m$.

11.36. Let $d = \gcd(a, b)$. Show that a/d and b/d are relatively prime.

There exists x and y such that $d = xa + yb$. Dividing the equation by d, we get $1 = x(a/d) + y(b/d)$. Hence a/d and b/d are relatively prime.

11.37. Prove Theorem 11.24: Suppose $ab \equiv ac \pmod m$ and $d = \gcd(a, m)$. Then $b \equiv c \pmod{m/d}$.

By hypothesis, m divides $ab - ac = a(b - c)$. Hence, there is an integer x such that $a(b - c) = mx$. Dividing by d yields $(a/d)(b - c) = (m/d)x$. Thus m/d divides $(a/d)(b - c)$. Since m/d and a/d are relatively prime, m/d divides $b - c$. That is, $b \equiv c \pmod{m/d}$, as required.

RESIDUE SYSTEMS, EULER PHI FUNCTION ϕ

11.38. For each modulo m, exhibit two complete residue systems, one consisting of the smallest nonnegative integers, and the other consisting of the integers with the smallest absolute values: $(a)\ m = 9$; $(b)\ m = 12$.

In the first case choose $\{0, 1, 2, \ldots, m-1\}$, and in the second case choose

$$\{-(m-1)/2, \ldots, -1, 0, 1, \ldots, (m-1)/2\} \quad \text{or} \quad \{-(m-2)/2, \ldots, -1, 0, 1, \ldots, m/2\}$$

according as m is even or odd:

(a) $\{0, 1, 2, 3, 4, 5, 6, 7, 8\}$ and $\{-4, -3, -2, -1, 0, 1, 2, 3, 4\}$

(b) $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$ and $\{-5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6\}$.

11.39. Find a reduced residue system modulo m and $\phi(m)$ where: $(a)\ m = 9$; $(b)\ m = 16$; $(c)\ m = 7$.

Choose those positive numbers less than m and relatively prime to m. The number of such numbers is $\phi\ (m)$.

(a) $\{1, 2, 4, 5, 7, 8\}$; hence $\phi\ (9) = 6$.

(b) $\{1, 3, 5, 7, 9, 11, 13, 15\}$; hence $\phi\ (16) = 8$.

(c) $\{1, 2, 3, 4, 5, 6\}$; hence $\phi\ (7) = 6$. (This is expected since $\phi(p) = p - 1$ for any prime p.)

11.40. Recall $S_m = 0,\ 1,\ 2, \ldots, m-1$ is a complete residue system modulo m. Prove:

(a) Any m consecutive integers is a complete residue system modulo m.

(b) If $\gcd(a, m) = 1$, then $aS_m = \{0, a, 2a, 3a, \ldots, (m-1)a\}$ is a complete residue system modulo m.

(a) Consider any other sequence of m integers, say $\{a, a+1, a+2, \ldots, a+(m-1)\}$. The absolute value of the difference s of any two of the integers is less than m. Thus m does not divide s, and so the numbers are incongruent modulo m.

(b) Suppose $ax \equiv ay \pmod m$ where $x, y \in S_m$. Since $\gcd(a, m) = 1$, the modified cancellation law Theorem 11.24 tells us $x \equiv y \pmod m$. Since $x, y \in S_m$, we must have $x = y$. That is, aS_m is a complete residue system modulo m.

11.41. Exhibit a complete residue system modulo $m = 8$ consisting entirely of multiples of 3.

By Problem 11.40(b), $3S_8 = \{0,\ 3,\ 6,\ 9,\ 12,\ 15,\ 18,\ 21\}$ is a complete residue system modulo $m = 8$.

11.42. Show that if p is a prime, then $\phi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1)$.

Clearly, $\gcd(a,\ p^n) \neq 1$ if and only if p divides a. Thus the only numbers between 1 and p^n which are not relatively prime to p^n are the multiples of p, that is, $p, 2p,\ 3p, \ldots, p^{n-1}(p)$. There are p^{n-1} such multiples of p. All the other numbers between 1 and p^n are relatively prime to p^n. Thus, as claimed:

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

11.43. Find: $(a)\ \phi\ (81),\ \phi(7^6)$; $(b)\ \phi\ (72),\ \phi\ (3000)$.

(a) By Problem 11.42,

$$\phi(81) = \phi(3^4) = 3^3(3-1) = 27(2) = 54 \quad \text{and} \quad \phi(7^6) = 7^5(7-1) = 6(7^5)$$

(b) Use Theorem 11.24 that ϕ is multiplicative:

$$\phi(72) = \phi(3^2 \cdot 2^3) = \phi(3^2)\phi(2^3) = 3(3-1) \cdot 2^2(2-1) = 24$$
$$\phi(3000) = \phi(3 \cdot 2^2 \cdot 5^3) = \phi(3)\phi(2^2)\phi(5^3) = 2 \cdot 2 \cdot 5^2(5-1) = 400$$

11.44. Prove Theorem 11.25: If a and b are relatively prime, then $\phi(ab) = \phi(a)\phi(b)$.

Let a and b be coprime (relatively prime) positive integers, and let S be the set of numbers from 1 to ab arranged in an array as in Fig. 11-7. That is, the first row of S is the list of numbers from 1 to a, the second row is the list of numbers from $a + 1$ to $2a$, and so on. Since a and b are coprime, any integer x is coprime to ab if and only if it is coprime to both a and b. We find the number of such integers x in the array S.

Since $na + k \equiv k \pmod{a}$, each column in S belongs to the same residue class modulo a. Therefore, any integer x in S is coprime to a if and only if x belongs to a column headed by some integer k which is coprime to a. On the other hand, there are $\phi(a)$ such columns since the first row is a residue system modulo a.

1	2	3	...	k	...	a
$a+1$	$a+2$	$a+3$	...	$a+k$	...	$2a$
$2a+1$	$2a+2$	$2a+3$	...	$2a+k$	...	$3a$
.....						
$(b-1)a+1$	.....			$(b-1)a+k$	...	ba

Fig. 11-7

Now let us consider an arbitrary column in the array S which consists of the numbers:

$$k, \quad a+k, \quad 2a+k, \quad 3a+k, \ldots, (b-1)a+k \tag{11.11}$$

By Problem 11.10, these b integers form a residue system modulo b, that is, no two of the integers are congruent modulo b. Therefore, (11.11) contains exactly $\phi(b)$ integers which are coprime to b. We have shown that the array S contains $\phi(a)$ columns consisting of those integers which are coprime to a, and each such column contains $\phi(b)$ integers which are coprime to b. Thus there are $\phi(a)\,\phi(b)$ integers in the array S which are coprime to both a and b and hence are coprime to ab. Accordingly, as required

$$\phi(ab) = \phi(a)\phi(b)$$

ARITHMETIC MODULO m, $\mathbf{Z}_m$

11.45. Exhibit the addition and multiplication tables for: (*a*) $\mathbf{Z}_4$; (*b*) $\mathbf{Z}_7$

(*a*) See Fig. 11-8. (*b*) See Fig. 11-9.

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

×	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Fig. 11-8

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

×	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Fig. 11-9

11.46. In $\mathbf{Z}_{11}$, find: (*a*) $-2, -5, -9, -10$; (*b*) 2/7, 3/7, 5/7, 8/7, 10/7, 1/7.

(*a*) Note $-a = m - a$ since $(m - a) + a = 0$. Therefore:

$$-2 = 11 - 2 = 9, \quad -5 = 11 - 5 = 6, \quad -9 = 11 - 9 = 2, \quad -10 = 11 - 10 = 1$$

(*b*) By definition a/b is the integer c such that $bc = a$. Since we are dividing by 7, first compute the multiplication table for 7 in $\mathbf{Z}_{11}$ as in Fig. 11-10. Now find the number inside the table, and the answer will be above this number. Thus:

×	0	1	2	3	4	5	6	7	8	9	10
7	0	7	3	10	6	2	9	5	1	8	4

Fig. 11-10

$$2/7 = 5, \quad 3/7 = 2, \quad 5/7 = 7, \quad 8/7 = 9, \quad 10/7 = 3, \quad 1/7 = 8$$

Note that $7^{-1} = 8$ since $7(8) = 8(7) = 1$.

11.47. Consider $\mathbf{Z_p}$ where p is a prime. Prove:

(*a*) If $ab = ac$ and $a \neq 0$, then $b = c$;

(*b*) If $ab = 0$, then $a = 0$ or $b = 0$.

(*a*) If $ab = ac$ in $\mathbf{Z}_p$, then $ab \equiv ac \pmod{p}$. Since $a \neq 0$, $\gcd(a, p) = 1$. By Theorem 11.23 we can cancel the a's to obtain $b \equiv c \pmod{p}$. Therefore $b = c$ in $\mathbf{Z_p}$.

(*b*) If $ab = 0$ in $\mathbf{Z_p}$, then $ab = 0$ (mod p). Therefore, p divides the product ab. Since p is a prime, $p \mid a$ or $p \mid b$; that is, $a \equiv 0 \pmod{p}$ or $b \equiv 0 \pmod{p}$. Thus $a = 0$ or $b = 0$ in $\mathbf{Z_p}$.

11.48. Consider $a \neq 0$ in $\mathbf{Z}_m$ where $\gcd(a, m) = 1$. Show that a has a multiplicative inverse in $\mathbf{Z}_m$.

Since $a \neq 0$ and $\gcd(a, m) = 1$, there exists integers x and y such that $ax + my = 1$ or $ax - 1 = my$. Thus m divides $ax - 1$ and hence $ax = 1 \pmod{m}$. Reduce x modulo m to an element x' in $\mathbf{Z}_m$. Then $ax' = 1$ in $\mathbf{Z}_m$.

11.49. Find a^{-1} in $\mathbf{Z}_m$ where: (*a*) $a = 37$ and $m = 249$; (*b*) $a = 15$ and $m = 234$.

(*a*) First find $d = \gcd(37,249)$ obtaining $d = 1$. Then, as in Example 11.6, find x and y such that $ax + my = 1$. This yields $x = -74$ and $y = 14$. That is,

$$-74(37) + 11(249) = 1 \quad \text{so} \quad -74(37) \equiv 1 (\text{mod } 249)$$

Add $m = 249$ to -74 to obtain $-74 + 249 = 175$. Thus $(175)(37) \equiv 1 \pmod{249}$.
Accordingly, $a^{-1} = 175$ in $\mathbf{Z}_{249}$.

(*b*) First find $d = \gcd(15, 234)$ obtaining $d = 3$. Thus $d \neq 1$, and hence 15 has no multiplicative inverse in $\mathbf{Z}_{234}$.

11.50. For the following polynomials over $\mathbf{Z}_7$ find: (*a*) $f(x) + g(x)$ and (*b*) $f(x)h(x)$.

$$f(x) = 6x^3 - 5x^2 + 2x - 4, \quad g(x) = 5x^3 + 2x^2 + 6x - 1, \quad h(x) = 3x^2 - 2x - 5$$

Perform the operations as if the polynomials were over the integers $\mathbf{Z}$, and then reduce the coefficients modulo 7.

(*a*) We get: $f(x) + g(x) = 11x^3 - 3x^2 + 8x - 5 = 4x^3 - 3x^2 + x - 5 = 4x^3 + 4x^2 + x + 2$

(*b*) First find the product $f(x)h(x)$ as in Fig. 11-11. Then, reducing modulo 7, we obtain: (*g*)

$$f(x)h(x) = 4x^5 - 6x^4 + 2x^2 - 2x + 6 = 4x^5 + x^4 + 2x^2 + 5x + 6$$

$$
\begin{array}{r}
6x^3 - 5x^2 + 2x - 4 \\
3x^2 - 2x - 5 \\
\hline
18x^5 - 15x^4 + 6x^3 - 12x^2 \\
-12x^4 + 10x^3 - 4x^2 + 8x \\
-30x^2 + 25x^2 - 10x + 20 \\
\hline
18x^5 - 27x^4 + 14x^3 + 9x^2 - 2x + 20
\end{array}
$$

Fig. 11-11

CONGRUENCE EQUATIONS

11.51. Solve the congruence equation $f(x) = 4x^4 - 3x^3 + 2x^2 + 5x - 4 \equiv 0 \pmod 6$.

Since the equation is not linear, we solve the equation by testing the numbers in a complete residue system modulo 6, say, $\{0, 1, 2, 3, 4, 5\}$. We have:

$$
\begin{array}{lll}
f(0) = 4 \not\equiv 0 (\text{mod } 6), & f(2) = 54 \equiv 0 \pmod 6, & f(4) = 880 \equiv 4 \not\equiv 0 \pmod 6 \\
f(1) = 4 \not\equiv 0 (\text{mod } 6), & f(3) = 272 \equiv 2 \not\equiv 0 \pmod 6, & f(5) = 2196 \equiv 0 \pmod 6
\end{array}
$$

Thus only 2 and 5 are roots of $f(x)$ modulo 6. That is, $\{2, 5\}$ is a complete set of solutions.

11.52. Solve the congruence equation $f(x) = 26x^4 - 31x^3 + 46x^2 - 76x + 57 \equiv 0 \pmod 8$.

First we reduce the coefficients of $f(x)$ modulo 8 to obtain the equivalent congruence equation

$$g(x) = 2x^4 - 7x^3 + 6x^2 - 4x + 1 \equiv 0 \pmod 8$$

Since $7 \equiv -1 \pmod 8$ and $6 = -2 \pmod 8$, we can further simplify our original equation to obtain the equivalent congruence equation

$$h(x) = 2x^4 + x^3 - 2x^2 - 4x + 1 \equiv 0 \pmod 8$$

We test the numbers in a complete residue system modulo 8 and, in order to keep our arithmetic as simple as possible, we choose $\{-3, -2, -1, 0, 1, 2, 3, 4\}$. (That is, we chose those numbers whose absolute value is minimal.) Substituting these numbers in $h(x)$ we obtain:

$$
\begin{array}{lll}
h(-3) = 130 \equiv 2 \pmod 8, & h(0) = 1 \equiv 1 \pmod 8, & h(3) = 160 \equiv 0 \pmod 8 \\
h(-2) = 9 \equiv 1 \pmod 8, & h(1) = -2 \equiv 6 \pmod 8, & h(4) = 529 \equiv 1 \pmod 8 \\
h(-1) = 4 \equiv 4 \pmod 8, & h(2) = 25 \equiv 1 \pmod 8, &
\end{array}
$$

Thus 3 is the only solution of $f(x) \pmod 8$.

11.53. Solve each linear congruence equation:

(*a*) $3x \equiv 2 \pmod 8$; (*b*) $6x \equiv 5 \pmod 9$; (*c*) $4x \equiv 6 \pmod{10}$

Since the moduli are relatively small, we find all the solutions by testing. Recall $ax \equiv b \pmod m$ has exactly $d = \gcd(a, m)$ solution providing d divides b.

(*a*) Here $\gcd(3, 8) = 1$, hence the equation has a unique solution. Testing $0, 1, 2, \ldots, 7$, we find that $3(6) = 18 \equiv 2 \pmod 8$. Thus 6 is the unique solution.

(*b*) Here $\gcd(6, 9) = 3$, but 3 does not divide 5. Hence the system has no solution.

(*c*) Here $\gcd(4, 10) = 2$ and 2 divides 6; hence the system has two solutions. Testing $0, 1, 2, 3, \ldots, 9$, we see that

$$4(4) = 16 \equiv 6 \pmod{10} \quad \text{and} \quad 4(9) = 36 \equiv 6 \pmod{10}$$

Hence 4 and 9 are our two solutions.

11.54. Solve the congruence equation $1092x \equiv 213 \pmod{2295}$.

Testing is not an efficient way to solve this equation since the modulus $m = 2295$ is large. First use the Euclidean algorithm to find $d = \gcd(1092, 2295) = 3$. Dividing 213 by $d = 3$ yields 0 as a remainder; that is, 3 does divide 213. Thus the equation will have three (incongruent) solutions.

Divide the equation and the modulus $m = 2295$ by $d = 3$ to obtain the congruence equation

$$364x \equiv 71 \pmod{765} \tag{11.12}$$

We know that 364 and 796 are relatively prime since we divided by $d = \gcd(1092, 2295) = 3$; hence the equation (11.12) has unique solution modulo 765. We solve (11.12) by first finding the solution of the equation

$$364x \equiv 1 \pmod{765} \tag{11.13}$$

This solution is obtained by finding s and t such that

$$364s + 765t = 1$$

Using the Euclidean algorithm and "unraveling" as in Example 11.6 and Problem 11.21, we obtain $s = 124$ and $t = -59$.

Accordingly, $s = 124$ is the unique solution of (11.13). Multiplying this solution $s = 124$ by 71 and reducing modulo 765 we obtain

$$124(71) = 8804 \equiv 389 \pmod{765}$$

This is the unique solution of(11.12).

Lastly, we add the new modulus $m = 765$ to the solution $x_1 = 389$ two times to obtain the other two solutions of the given equation:

$$x_2 = 389 + 765 = 1154, \quad x_3 = 1154 + 765 = 1919$$

In other words, $x_1 = 389, x_2 = 1154, x_3 = 1919$ form a complete set of solutions of the given congruence equation $1092x \equiv 213 \pmod{2295}$.

11.55. Solve the congruence equation $455x \equiv 204 \pmod{469}$.

First use the Euclidean algorithm to find $d = \gcd(455, 469) = 7$. Dividing 204 by $d = 7$ yields 1 as a remainder; that is, 7 does not divide 204. Thus the equation has no solution.

11.56. Find the smallest positive integer x such that when x is divided by 3 it yields a remainder 2, when x is divided by 7 it yields a remainder 4, and when x is divided by 10 it yields a remainder 6.

We seek the smallest positive common solution of the following three congruence equations:

$$(a)\ x \equiv 2 \pmod{3}; \quad (b)\ x \equiv 4 \pmod{7}; \quad (c)\ x \equiv 6 \pmod{10}$$

Observe that the moduli 3, 7, and 10 are pairwise relatively prime. (Moduli is the plural of modulus.) The Chinese Remainder Theorem (CRT), Theorem 11.29, tells us that there is a unique solution modulo the product $m = 3(7)(10) = 210$. We solve the problems in two ways.

Method 1: First we apply CRT to the first two equations,

$$(a)\ x \equiv 2 \pmod{3} \quad \text{and} \quad (b)\ x \equiv 4 \pmod{7}$$

We know there is a unique solution modulo $M = 3 \cdot 7 = 21$. Adding multiples of the modulus $m = 7$ to the given solution $x = 4$ of the second equation (b), we obtain the following three solutions of (b) which are less than 21:

$$4, \quad 11, \quad 18$$

Testing each of these solutions of (b) in the first equation (a), we find that 11 is the only solution of both equations.

Now we apply the same process to the two equations

$$(c)\ x \equiv 6 \pmod{10} \quad \text{and} \quad (d)\ x \equiv 11 \pmod{21}$$

CRT tells us there is a unique solution modulo $M = 21 \cdot 10 = 210$. Adding multiples of the modulus $m = 21$ to the given solution $x = 11$ of the equation (d), we obtain the following 10 solutions of (d) which are less than 210:

$$11,\ 32,\ 53,\ 74,\ 95,\ 116,\ 137,\ 158,\ 179,\ 210$$

Testing each of these solutions of (d) in the equation (c), we find that $x = 116$ is the only solution of equation (c). Accordingly, $x = 116$ is the smallest positive integer satisfying all of the three given equations (a), (b), and (c).

Method 2: Using the notation of Proposition 11.30, we obtain

$$M = 3 \cdot 7 \cdot 10 = 210, \quad M_1 = 210/3 = 70, \quad M_2 = 210/7 = 30, \quad M_3 = 210/10 = 21$$

We now seek solutions to the equations

$$70x \equiv 1 \pmod{3}, \quad 30x \equiv 1 \pmod{7}, \quad 21x \equiv 1 \pmod{10}$$

Reducing 70 modulo 3, reducing 30 modulo 7, and reducing 21 modulo 10, we obtain the equivalent system

$$x \equiv 1 \pmod{3}, \quad 2x \equiv 1 \pmod{7}, \quad x \equiv 1 \pmod{10}$$

The solutions of these three equations are, respectively,

$$s_1 = 1, \quad s_2 = 4, \quad s_3 = 1$$

Substituting into the formula

$$x_0 = M_1 s_1 r_1 + M_2 s_2 r_2 + \cdots + M_k s_k r_k$$

we obtain the following solution of our original system:

$$x_0 = 70 \cdot 1 \cdot 2 + 30 \cdot 4 \cdot 4 + 21 \cdot 1 \cdot 6 = 746$$

Dividing this solution by the modulus $M = 210$, we obtain the remainder $x = 116$ which is the unique solution of the original system between 0 and 210.

11.57. Prove Theorem 11.26: If a and m are relatively prime, then $ax \equiv 1 \pmod{m}$ has a unique solution; otherwise it has no solution.

Suppose x_0 is a solution. Then m divides $ax_0 - 1$, and hence there exists y_0 such that $my_0 = ax_0 - 1$. Therefore

$$ax_0 + my_0 = 1 \tag{11.14}$$

and a and m are coprime (relatively prime). Conversely, if a and m are coprime, then there exist x_0 and y_0 satisfying (11.14), in which case x_0 is a solution of $ax \equiv 1 \pmod{m}$.

It remains to prove that x_0 is a unique solution modulo m. Suppose x_1 is another solution. Then

$$ax_0 \equiv 1 \equiv ax_1 \pmod{m}$$

Since a and m are coprime, the Modified Cancellation Law holds here, so

$$x_0 \equiv x_1 \pmod{m}$$

Thus the theorem is proved.

11.58. Prove Theorem 11.27: Suppose a and m are relatively prime. Then $ax \equiv b \pmod{m}$ has a unique solution. Moreover, if s is the unique solution of $ax \equiv 1 \pmod{m}$, then $x = bs$ is the unique solution to $ax \equiv b \pmod{m}$.

By Theorem 11.26 (proved in Problem 11.57), a unique solution s of $ax \equiv 1 \pmod{m}$ exists. Hence $as \equiv 1 \pmod{m}$ and so

$$a(bs) = (as)b \equiv 1 \cdot b = b \pmod{m}$$

That is, $x = bs$ is a solution of $ax \equiv b \pmod{m}$. Suppose x_0 and x_1 are two such solutions. Then

$$ax_0 \equiv b \equiv ax_1 \pmod{m}$$

Since a and m are coprime, the Modified Cancellation Law tells us that $x_0 \equiv x_1 \pmod{m}$. That is, $ax \equiv b \pmod{m}$ has a unique solution modulo m.

11.59. Prove Theorem 11.28: Consider the following equation where $d = \gcd(a, m)$:

$$ax \equiv b \pmod{m} \tag{11.15}$$

(i) Suppose d does not divide b. Then (11.15) has no solution.

(ii) Suppose d does divide b. Then (11.15) has d solutions which are all congruent modulo M to the unique solution of the following equation where $A = a/d$, $B = b/d$, $M = m/d$:

$$Ax \equiv B \pmod{M} \tag{11.16}$$

(i) Suppose x_0 is a solution of (11.15). Then $ax_0 \equiv b \pmod{m}$, and so m divides $ax_0 - b$. Thus there exists an integer y_0 such that $my_0 = ax_0 - b$ or $my_0 + ax_0 = b$. But $d = \gcd(a, m)$, and so d divides $my_0 + ax_0$. That is, d divides b. Accordingly, if d does not divide b, then no solution exists.

(ii) Suppose x_0 is a solution of (11.15). Then, as above,

$$my_0 + ax_0 = b$$

Dividing through by d we get (11.16). Hence M divides $Ax_0 - B$ and so x_0 is a solution of (11.16). Conversely, suppose x_1 is a solution of (11.16). Then, as above, there exists an integer y_1 such that

$$My_1 + Ax_1 = B$$

Multiplying through by d yields

$$dMy_1 + dAx_1 = dB \quad \text{or} \quad my_1 + ax_1 = b$$

Therefore m divides $ax_1 - b$ whence x_1 is a solution of (11.15). Thus (11.16) has the same integer solution. Let x_0 be the unique smallest positive solutions of (11.16). Since $m = dM$,

$$x_0, \quad x_0 + M, \quad x_0 + 2M, \quad x_0 + 3M, \quad \ldots, \quad x_0 + (d-1)M$$

are precisely the solution of (11.16) and (11.15) between 0 and m. Thus (11.15) has d solutions modulo m, and all are congruent to x_0 modulo M.

11.60. Prove the Chinese Remainder Theorem (Theorem 11.29:) Given the system:

$$x \equiv r_1 \pmod{m_1}, \quad x \equiv r_2 \pmod{m_2}, \quad \ldots, \quad x \equiv r_k \pmod{m_k} \tag{11.17}$$

where the m_i are pairwise relatively prime. Then the system has a unique solution modulo $M = m_1 m_2 \cdots m_k$.

Consider the integer

$$x_0 = M_1 s_1 r_1 + M_2 s_2 r_2 + \cdots + M_k s_k r_k$$

where $M_i = M/m_i$ and s_i is the unique solution of $M_i x \equiv 1 \pmod{m_i}$. Let j be given.

For $i \neq j$, we have $m_j | M_i$ and hence

$$M_i s_i r_i \equiv 0 \pmod{m_j}$$

On the other hand, $M_j S_j \equiv 1 \pmod{m_j}$; and hence

$$M_j s_j r_j \equiv r_j \pmod{m_j}$$

Accordingly,

$$x_0 \equiv 0 + \cdots + 0 + r_j + 0 + \cdots + 0 \equiv r_j \pmod{m_j}$$

In other words, x_0 is a solution of each of the equations in (11.17).

It remains to show that x_0 is the unique solution of the system (11.17) modulo M.

Suppose x_1 is another solution of all the equations in (11.17). Then:

$$x_0 \equiv x_1 \pmod{m_1}, \quad x_0 \equiv x_1 \pmod{m_2}, \quad \cdots, \quad x_0 \equiv x_1 \pmod{m_k}$$

Hence $m_i \mid (x_0 - x_1)$, for each i. Since the m_i are relatively prime, $M = \text{lcm}(m_1, m_2, \ldots, m_k)$ and so $M \mid (x_0 - x_1)$. That is, $x_0 = x_1 \pmod{M}$. Thus the theorem is proved.

Supplementary Problems

ORDER AND INEQUALITIES, ABSOLUTE VALUE

11.61. Insert the correct symbol, $<$, $>$, or $=$, between each pair of integers:

(a) $2 \_\_\_ -6$; (c) $-7 \_\_\_ 3$; (e) $2^3 \_\_\_ 11$; (g) $-2 \_\_\_ -7$;
(b) $-3 \_\_\_ -5$; (d) $-8 \_\_\_ -1$; (f) $2^3 \_\_\_ -9$; (h) $4 \_\_\_ -9$.

11.62. Evaluate: (a) $|3-7|, |-3+7|, |-3-7|$; (b) $|2-5|+|3+7|, |1-4|-|2-9|$;
(c) $|5-9|+|2-3|, |-6-2|-|2-6|$.

11.63. Find the distance d between each pair of integers: (a) 2 and -5; (b) -6 and 3; (c) 2 and 8; (d) -7 and -1; (e) 3 and -3; (f) -7 and -9.

11.64. Find all integers n such that: (a) $3 < 2n-4 < 10$; (b) $1 < 6-3n < 13$.

11.65. Prove Proposition 11.1: (i) $a \le a$, for any integer a; (ii) If $a \le b$ and $b \le a$, then $a = b$.

11.66. Prove Proposition 11.2: For any integers a and b, exactly one of the following holds: $a < b, a = b,$ or $a > b$.

11.67. Prove: (a) $2ab \le a^2 + b^2$; (b) $ab + ac + bc \le a^2 + b^2 + c^2$.

11.68. Proposition 11.4: (i) $|a| \ge 0$, and $|a| = 0$ iff $a = 0$; (ii) $-|a| \le a \le |a|$; (iii) $||a| - |b|| \le |a \pm b|$.

11.69. Show that $a - xb \ge 0$ if $b \ne 0$, and $x = -|a|b$.

MATHEMATICAL INDUCTION, WELL-ORDERING PRINCIPLE

11.70. Prove the proposition that the sum of the first n even positive integers is $n(n+1)$; that is,

$$P(n): 2 + 4 + 6 + \cdots + 2n - = n(n+1)$$

11.71. Prove that the sum of the first n cubes is equal to the square of the sum of the first n positive integers:

$$P(n): 1^3 + 2^3 + 3^3 + \cdots + n^3 = (1 + 2 + \cdots + n)^2$$

11.72. Prove: $1 + 4 + 7 + \cdots + (3n-2) = n(3n-1)/2$

11.73. Prove: (a) $a^n\, a^m = a^{n+m}$; (b) $(a^n)^m = a^{nm}$; (c) $(ab)^n = a^n b^n$

11.74. Prove: $\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \frac{1}{3\cdot 4} + \cdots + \frac{1}{n(n+1)} = \frac{n}{n+1}$

11.75. Prove: $\frac{1}{1\cdot 3} + \frac{1}{3\cdot 5} + \frac{1}{5\cdot 7} + \cdots + \frac{1}{(2n-1)(2n+1)} = \frac{n}{2n+1}$

11.76. Prove: $\frac{1^2}{1\cdot 3} + \frac{2^2}{3\cdot 5} + \frac{3^2}{5\cdot 7} + \cdots + \frac{n^2}{(2n-1)(2n+1)} = \frac{n(n+1)}{2(2n+1)}$

11.77. Prove: $x^{n+1} - y^{n+1} = (x-y)(x^n + x^{n-1}y + x^{n-2}y^2 + \cdots + y^n)$

11.78. Prove: $|P(A)| = 2^n$ where $|A| = n$. (Here $P(A)$ is the power set of the set A with n elements.)

DIVISION ALGORITHM

11.79. For each pair of integers a and b, find integers q and r such that $a = bq + r$ and $0 \le r < |b|$:
(a) $a = 608$ and $b = -17$; (b) $a = -278$ and $b = 12$; (c) $a = -417$ and $b = -8$.

11.80. Prove each of the following statements:

(a) Any integer a is of the form $5k$, $5k+1$, $5k+2$, $5k+3$, or $5k+4$.

(b) One of five consecutive integers is a multiple of 5.

11.81. Prove each of the following statements:

(a) The product of any three consecutive integers is divisible by 6.

(b) The product of any four consecutive integers is divisible by 24.

11.82. Show that each of the following numbers is not rational: (a) $\sqrt{3}$; (b) $\sqrt[3]{2}$.

11.83. Show that $\sqrt{p}$ is not rational, where p is any prime number.

DIVISIBILITY, GREATEST COMMON DIVISORS, PRIMES

11.84. Find all possible divisors of: (a) 24; (b) $19683 = 3^9$; (c) $432 = 2^4 \cdot 3^3$.

11.85. List all prime numbers between 100 and 150.

11.86. Express as a product of prime numbers: (a) 2940; (b) 1485; (c) 8712; (d) 319 410.

11.87. For each pair of integers a and b, find $d = \gcd(a, b)$ and find m and n such that $d = ma + nb$:

(a) $a = 356$, $b = 48$; (b) $a = 1287$, $b = 165$; (c) $a = 2310$, $b = 168$; (d) $a = 195, b = 968$; (e) $a = 249, b = 37$.

11.88. Find: (a) lcm(5, 7); (b) lcm(3, 33); (c) 1cm (12, 28).

11.89. Suppose $a = 5880$ and $b = 8316$. (a) Express a and b as products of primes.
(b) Find $\gcd(a, b)$ and $\text{lcm}(a, b)$. (c) Verify that $\text{lcm}(a, b) = |ab|/\gcd(a, b)$.

11.90. Prove: (a) If $a|b$, then (i) $a| - b$, (ii) $-a|b$, (iii) $-a| - b$; (b) If $ac|bc$, then $b|c$.

11.91. Prove: (a) If $n > 1$ is composite, then n has a positive divisor d such that $d \leq \sqrt{n}$. (b) If $n > 1$ is not divisible by a prime $p \leq \sqrt{n}$, then n is a prime.

11.92. Prove: (a) If $am + bn = 1$, then $\gcd(a, b) = 1$; (b) If $a = bq + r$, then $\gcd(a, b) = \gcd(b, r)$.

11.93. Prove: (a) $\gcd(a, a + k)$ divides k; (b) $\gcd(a, a + 2)$ equals 1 or 2.

11.94. Prove: (a) If $a > 2$ and $k > 1$, then $a^k - 1$ is composite. (b) If $n > 0$ and $2^n - 1$ is prime, then n is prime.

11.95. Let n be a positive integer. Prove:

(a) 3 divides n if and only if 3 divides the sum of the digits of n.

(b) 9 divides n if and only if 9 divides the sum of the digits of n.

(c) 8 divides n if and only if 8 divides the integer formed by the last three digits of n.

11.96. Extend the definition of gcd and lcm to any finite set of integers, that is, for integers $a_1, a_2, \ldots, a_k$, define: (a) $\gcd(a_1, a_2, \ldots, a_k)$; (b) $\text{lcm}(a_1, a_2, \ldots, a_k)$.

11.97. Prove: If $a_1|n, a_2|n, \ldots, a_k|n$, then $m|n$ where $m = \text{lcm}(a_1, a_2, \ldots, a_k)$.

11.98. Prove: There are arbitrarily large gaps between prime numbers, that is, for any positive integer k, there exist k consecutive composite (nonprime) integers.

CONGRUENCES

11.99. Which of the following are true?
(a) $224 \equiv 762 \pmod 8$; (b) $582 \equiv 263 \pmod{11}$; (c) $156 \equiv 369 \pmod 7$; (d) $-238 \equiv 483 \pmod{13}$.

11.100. Find the smallest nonnegative integer which is congruent modulo $m = 9$ to each of the following numbers: (a) 457; (b) 1578; (c) -366; (d) -3288. (The integer should be in the set $\{0, 1, 2, \ldots, 7, 8\}$).

11.101. Find the smallest integer in absolute value which is congruent modulo $m = 9$ to each of the following numbers: (a) 511; (b) 1329; (c) -625; (d) -2717. (The integer should be in the set $\{-4, -3, -2, -1, 0, 1, 2, 3, 4\}$).

11.102. Find all numbers between 1 and 100 which are congruent to 4 modulo $m = 11$.

11.103. Find all numbers between -50 and 50 which are congruent to 12 modulo $m = 9$.

RESIDUE SYSTEMS, EULER PHI FUNCTION ϕ

11.104. For each modulo m, exhibit two complete residue systems, one consisting of the smallest nonnegative integers, and the other consisting of the integers with the smallest absolute values: (a) $m = 11$; (b) $m = 14$.

11.105. Exhibit a reduced residue system modulo m and find $\phi(m)$ where: (a) $m = 4$; (b) $m = 11$; (c) $m = 14$; (d) $m = 15$.

11.106. Exhibit a complete residue system modulo $m = 8$ consisting entirely of: (a) multiples of 5; (b) powers of 3.

11.107. Show that $\{1^2, 2^2, 3^2, \ldots, m^2\}$ is not a complete residue system modulo m for $m > 2$.

11.108. Find: (a) $\phi(10)$; (b) $\phi(12)$; (c) $\phi(15)$; (d) $\phi(3^7)$; (e) $\phi(5^6)$; (f) $\phi(2^4 \cdot 7^6 \cdot 13^3)$.

11.109. Find the number s of positive integers less than 3200 which are coprime to 8000.

11.110. Consider an arbitrary column in the array S in Fig. 11-7 which consists of the numbers:

$$k, a+k, 2a+k, 3a+k, \ldots, (b-1)a+k$$

Show that these b integers form a residue system modulo b.

ARITHMETIC MODULO m, $\mathbf{Z_m}$

11.111. Exhibit the addition and multiplication tables for: (a) $\mathbf{Z}_2$; (b) $\mathbf{Z}_8$.

11.112. In. $\mathbf{Z}_{13}$, find: (a) $-2, -3, -5, -9, -10, -11$; (b) 2/9, 4/9, 5/9, 7/9, 8/9.

11.113. In $\mathbf{Z}_{17}$, find: (a) $-3, -5, -6, -8, -13, -15, -16$; (b) 3/8, 5/8, 7/8, 13/8, 15/8.

11.114. Find a^{-1} in $\mathbf{Z}_m$ Where: (a) $a = 15, m = 127$; (b) $a = 61, m = 124$; (c) $a = 12, m = 111$.

11.115. Find the product $f(x)g(x)$ for the following polynomials over $\mathbf{Z}_5$:

$$f(x) = 4x^3 - 2x^2 + 3x - 1, g(x) = 3x^2 - x - 4$$

CONGRUENCE EQUATIONS

11.116. Solve each congruence equation:

(a) $f(x) = 2x^3 - x^2 + 3x + 1 \equiv 0 \pmod 5$

(b) $g(x) = 3x^4 - 2x^3 + 5x^2 + x + 2 \equiv 0 \pmod 7$

(c) $h(x) = 45x^3 - 37x^2 + 26x + 312 \equiv 0 \pmod 6$

11.117. Solve each linear congruence equation:

(a) $7x \equiv 3 \pmod 9$; (b) $4x \equiv 6 \pmod{14}$; (c) $6x \equiv 4 \pmod 9$.

11.118. Solve each linear congruence equation:

(a) $5x \equiv 3 \pmod 8$; (b) $6x \equiv 9 \pmod{16}$; (c) $9x \equiv 12 \pmod{21}$.

11.119. Solve each linear congruence equation: (a) $37x \equiv 1 \pmod{249}$; (b) $195x \equiv 23 \pmod{968}$.

11.120. Solve each linear congruence equation: (a) $132x \equiv 169 \pmod{735}$; (b) $48x \equiv 284 \pmod{356}$

11.121. A puppet theater has only 60 seats. The admission to the theater is \$2.25 per adult and \$1.00 per child. Suppose \$117.25 was collected. Find the number of adults and children attending the performance.

11.122. A boy sells apples for 12 cents each and pears for 7 cents each. Suppose the boy collected \$3.21. Find the number of apples and pears that he sold.

11.123. Find the smallest positive solution of each system of congruence equations:

(a) $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$, $x \equiv 4 \pmod{11}$
(b) $x \equiv 3 \pmod 5$, $x \equiv 4 \pmod 7$, $x \equiv 6 \pmod 9$
(c) $x \equiv 5 \pmod{45}$, $x \equiv 6 \pmod{49}$, $x \equiv 7 \pmod{52}$

Answers to Supplementary Problems

11.61. (a) $2 > -6$; (b) $-3 > -5$; (c) $-7 < 3$; (d) $-8 < -1$; (e) $2^3 < 11$; (f) $2^3 > -9$; (g) $-2 > -7$; (h) $4 > -9$

11.62. (a) 4, 4, 10; (b) $3 + 10 = 13$, $3 - 7 = -4$; (c) $4 + 1 = 5$, $8 - 4 = 4$.

11.63. (a) 7; (b) 9; (c) 6; (d) 6; (e) 6; (f) 2.

11.64. (a) 4, 5, 6; (b) $-2, -1, 0, 1$.

11.79. (a) $q = -15$, $r = 13$; (b) $q = -24$, $r = 10$. (c) $q = 53$, $r = 7$

11.81. (a) One is divisible by 2 and one is divisible by 3. (b) One is divisible by 4, another is divisible by 2, and one is divisible by 3.

11.84. (a) 1, 2, 3, 4, 6, 8, 12, 24; (b) 3^n for $n = 0$ to 9; (c) $2^r 3^s$ for $r = 0$ to 4 and $s = 0$ to 3.

11.85. 101, 103, 107, 109, 113, 127, 131, 137, 139, 149.

11.86. (a) $2940 = 2^2 \cdot 3 \cdot 5 \cdot 7^2$; (b) $1485 = 3^3 \cdot 5 \cdot 11$; (c) $8712 = 2^3 \cdot 3^2 \cdot 11^2$; (d) $319\,410 = 2 \cdot 3^3 \cdot 5 \cdot 7 \cdot 13^2$.

11.87. (a) $d = 4 = 5(356) - 37(48)$; (b) $d = 33 = 8(165) - 1(1287)$; (c) $d = 42 = 14(168) - 1(2310)$; (d) $d = 1 = 139(195) - 28(968)$; (e) $11(249) - 74(37)$.

11.88. (a) 35; (b) 33; (c) 84.

11.89. (a) $a = 2^3 \cdot 3 \cdot 5 \cdot 7^2$, $b = 2^2 \cdot 3^3 \cdot 7 \cdot 11$; (b) $\gcd(a, b) = 2^2 \cdot 3 \cdot 7$, $\text{lcm}(a, b) = 2^3 \cdot 3^3 \cdot 5 \cdot 7^2 \cdot 11 = 1, 164, 240$.

11.94. (a) Hint: $a^k - 1 = (a-1)(1 + a + a^2 + \cdots + a^{k-1})$; (b) Hint: If $n = ab$, then $2^n - 1 = (2^a)^b - 1$.

11.98. $(k + 1)! + 2$, $(k + 1)! + 3$, $(k + 1)! + 4, \ldots,$ $(k + 1)! + (k + 1)$ are divisible by $2, 3, 4, \ldots, k + 1$, respectively.

11.99. (a) False; (b) true; (c) false; (d) false.

11.100. (a) 7; (b) 3; (c) 3; (d) 6.

11.101. (a) -2; (b) -3; (c) -4; (d) 1.

11.102. 4, 15, 26, 37, 48, 59, 70, 81, 92.

11.103. $-42, -33, -24, -15, -6, 3, 12, 21, 30, 39, 48$.

11.104. (a) $\{0, 1, \ldots, 10\}$ and $\{-5, -4, \ldots, -1, 0, 1, \ldots, 4, 5)$.
(b) $\{0, 1, \ldots, 13\}$ and $\{-6, -5, \ldots, -1, 0, 1, \ldots, 6, 7\}$.

11.105. (a) $\{1, 3\}$; (b) $\{1, 2, \ldots, 10\}$; (c) $\{1, 3, 5, 9, 11, 13\}$; (d) $\{1, 2, 4, 7, 8, 11, 13, 14\}$.

11.106. (a) $\{5, 10, 15, 20, 25, 30, 35, 40\}$; (b) $\{3, 9, 27, 81, 243, 729, 2187, 6561\}$.

11.107. $m - 1 \equiv -1 \pmod{m}$ and so $(m - 1)^2 \equiv 1 \pmod{m}$.

11.108. (a) 4; (b) 4; (c) = 8; (d) $2(3^6)$; (e) $4(5^5)$; (f) $(2^3)(6 \cdot 7^5)(12 \cdot 13^2)$

11.109. $\phi(8000) = \phi(2^5 \cdot 5^2) = 2^4 \cdot 4 \cdot 5 = 320$. Hence $s = 4(320) = 1280$.

11.112. (a) 11, 10, 8, 4, 3, 2; (b) 6, 12, 2, 8, 11.

11.113. (a) 14, 12, 11, 9, 4, 2; (b) 11, 7, 3, 8, 4.

11.114. (a) 17; (b) 61; (c) a^{-1} does not exist.

11.115. $2x^5 + 2x^2 - x + 4$

11.116. (a) 1, 3, 4; (b) 2, -2; (c) 0, 2, 3, -1.

11.117. (a) 3; (b) 5, 12; (c) no solution.

11.118. (a) 7; (b) no solution; (c) 6, 13, 20.

11.119. (a) 175; (b) 293.

11.120. (a) No solution; (b) 43, 132, 221, 310.

11.121. 49 adults, 7 children.

11.122. 25 apples, 3 pears; 18 apples, 15 pears; 11 apples, 27 pears; or 4 apples, 39 pears.

11.123. (a) 158; (b) 1(123); (c) 31 415.