Example 2.30. For each of the following values of n and d, find integers q and r such that $n = dq + r$ and $0 \leq r < d$

a $n = 54, d = 4$

b $n = -54, d = 4$

c $n = 54, d = 70$

Example 2.31. What are the quotient and remainder when 101 is divided by 11?

Solution. Exercise ■

2.3 Modular Arithmetic

Definition 23

Given an integer n and a positive integer d, if n and d are integers and $d > 0$, then

$$n \text{ div } d = q \text{ and } n \text{ mod } d = r \leftrightarrow n = dq + r,$$

where q and r are integers and $0 \leq r < d$.

Example 2.32. Compute 32 div 9 and 32 mod 9 by hand or with a four-function calculator.

Because we are often interested only in remainders, we have special notations for them. We have already introduced the notation a **mod** m to represent the remainder when an integer a is divided by the positive integer m. We now introduce a different, but related, notation that indicates that two integers have the same remainder when they are divided by the positive integer m.

Definition 24

If a and b are integers and m is a positive integer, then a is congruent to b modulo m if m divides $a - b$. We use the notation $a \equiv b(\text{ mod } m)$ to indicate that a is congruent to b modulo m. We say that $a \equiv b(\text{mod}m)$ is a **congruence** and that m is its **modulus** (plural **moduli**). If a and b are not congruent modulo m, we write $a \not\equiv b(\text{mod}m)$.

Although both notations $a \equiv b(\text{mod}m)$ and a **mod** $m = b$ include "mod," they represent fundamentally different concepts. The first represents a relation on the set of integers, whereas the second represents a function.

Theorem 2.8. *Let a and b be integers, and let m be a positive integer.*

*Then $a \equiv b(\text{ mod } m)$ if and only if a **mod** $m = b$ **mod** m.*

Recall that a **mod** m and b **mod** m are the remainders when a and b are divided by m, respectively. Consequently, ***Theorem 2.8*** also says that $a \equiv b(\text{ mod } m)$ if and only if a and b have the same remainder when divided by m.

Example 2.33. Determine whether 17 is congruent to 5 modulo 6 and whether 24 and 14 are congruent modulo 6.

Solution. Because 6 divides $17 - 5 = 12$, we see that $17 \equiv 5(\text{ mod } 6)$. However, because $24 - 14 = 10$ is not divisible by 6, we see that $24 \not\equiv 14(textmod6)$. ■

Theorem 2.9. *Let m be a positive integer. The integers a and b are congruent modulo m if and only if there is an integer k such that $a = b + km$.*

Proof: Suppose $a \equiv b(\bmod m)$, then by the definition of congruence

$$m|(a-b)$$

$$\Longrightarrow a-b=km \text{ for some integer } k$$

$$\text{so that } a=b+km$$

Conversely, suppose there is an integer k such that

$$a=b+km$$

$$\text{then } km=a-b$$

Hence, m divides $a-b$, so that $a \equiv b(\bmod m)$.

Theorem 2.10. *Let m be a positive integer. If $a \equiv b(\bmod m)$ and $c \equiv d(\bmod m)$, then*

$$a+c \equiv b+d(\bmod m) \text{ and } ac \equiv bd(\bmod m).$$

Proof: We use a direct proof. Because $a \equiv b(\bmod m)$ and $c \equiv d(\bmod m)$,

$$b=a+sm \text{ and } d=c+tm \text{ for integers } s \text{ and } t$$

and

$$b+d=(a+sm)+(c+tm)=(a+c)+m(s+t)$$

Hence,

$$bd=(a+sm)(c+tm)=ac+m(at+cs+stm)$$

$$a+c \equiv b+d(\bmod m) \text{ and } ac \equiv bd(\bmod m)$$

Example 2.34. Because $7 \equiv 2(\bmod 5)$ and $11 \equiv 1(\bmod 5)$, it follows from ***Theorem 2.10*** that

$$18=7+11 \equiv 2+1=3(\bmod 5)$$

and that

$$77=7.11 \equiv 2.1=2(\bmod 5).$$

Corollary 2.11. *Let m be a positive integer and let a and b be integers. Then*

$$(a+b) \bmod m=((a \bmod m)+(b \bmod m)) \bmod m$$

and

$$ab \bmod m=((a \bmod m)(b \bmod m)) \bmod m.$$

Example 2.35. Find the value of $(19^3 \bmod 31)^4 \bmod 23$.

Solution. To compute $(19^3 \bmod 31)^4 \bmod 23$, we will first evaluate $19^3 \bmod 31$.

$$19^3 \bmod 31=6859 \bmod 31=8$$

Therefore,

$$(19^3 \bmod 31)^4 \bmod 23=8^4 \bmod 23$$

Next, note that $8^4=4096$. Because $4096=178 \times 23+2$, we have $4096 \bmod 23=2$
Hence,

$$(19^3 \bmod 31)^4 \bmod 23=8^4 \bmod 23=4096 \bmod 23=2$$

2.4 Greatest Common Divisors and Least Common Multiples

The largest integer that divides both of two integers is called the **greatest common divisor** of these integers.

Definition 25: Greatest Common Divisor (GCD)

Let a and b be integers, not both zero. The largest integer d such that $d|a$ and $d|b$ is called the greatest common divisor of a and b. The greatest common divisor of a and b is denoted by $gcd(a, b)$.

Example 2.36. Find the greatest common divisor of each of the pairs of integers

1. 27 and 72 2. 72 and 63 3. 5 and 9 4. 7 and 21 5. 48 and 54 6. 24 and 36

Definition 26

1. The integers a and b are relatively prime if their greatest common divisor is 1.
2. The integers $a_1, a_2, ..., a_n$ are pairwise relatively prime if $gcd(a_i, a_j) = 1$ whenever $1 \leq i < j \leq n$.

Example 2.37. Determine whether the integers 10, 17, and 21 are pairwise relatively prime and whether the integers 10, 19, and 24 are pairwise relatively prime.

Another way to find the greatest common divisor of two positive integers is to use the prime factorizations of these integers. Suppose that the prime factorizations of the positive integers a and b are

$$a = p_1^{a_1}, p_2^{a_2}, ..., p_n^{a_n}, \text{ and } b = p_1^{b_1}, p_2^{b_2}, ..., p_n^{b_n}$$

where each exponent is a nonnegative integer, and where all primes occurring in the prime factorization of either a or b are included in both factorizations, with zero exponents if necessary. Then $gcd(a, b)$ is given by

$$gcd(a, b) = p_1^{min(a_1,b_1)}, p_2^{min(a_2,b_2)}, ..., p_n^{min(a_n,b_n)}$$

where $min(x, y)$ represents the minimum of the two numbers x and y.

Example 2.38. Find $gcd(120, 500)$

Prime factorizations can also be used to find the least common multiple of two integers.

Definition 27: Least Common Multiple (LCM)

The least common multiple of the positive integers a and b is the smallest positive integer that is divisible by both a and b. The least common multiple of a and b is denoted by $lcm(a, b)$.

The least common multiple exists because the set of integers divisible by both a and b is nonempty (because ab belongs to this set, for instance), and every nonempty set of positive integers has a least element (by the well-ordering property). Then the least common multiple of a and b is given by

$$lcm(a, b) = p_1^{max(a_1,b_1)}, p_2^{max(a_2,b_2)}, ..., p_n^{max(a_n,b_n)}$$

where $max(x, y)$ denotes the maximum of the two numbers x and y.

Example 2.39. What is the least common multiple of $2^3 3^5 7^2$ and $2^4 3^3$?

Theorem 2.12. *Let a and b be positive integers. Then*

$$ab = gcd(a, b) \cdot lcm(a, b).$$

2.5 The Euclidean Algorithm

Computing the greatest common divisor of two integers directly from the prime factorizations of these integers is inefficient. The reason is that it is time-consuming to find prime factorizations. We will give a more efficient method of finding the greatest common divisor, called the **Euclidean algorithm**.

Lemma 2.13. *Let $a = bq + r$, where a, b, q, and r are integers. Then $gcd(a,b) = gcd(b,r)$.*

Proof: Exercise! □

Suppose that a and b are positive integers with $a \geq b$. Let $r_0 = a$ and $r_1 = b$. When we successively apply the division algorithm, we obtain

$$\begin{aligned}
r_0 &= r_1 q_1 + r_2 && 0 \leq r_2 < r_1,\\
r_1 &= r_2 q_2 + r_3 && 0 \leq r_3 < r_2,\\
r_2 &= r_3 q_3 + r_4 && 0 \leq r_4 < r_3,\\
&\vdots\\
r_{n-2} &= r_{n-1} q_{n-1} + r_n && 0 \leq r_n < r_{n-1},\\
r_{n-1} &= r_n q_n
\end{aligned}$$

Eventually a remainder of zero occurs in this sequence of successive divisions, because the sequence of remainders $a = r_0 > r_1 > r_2 > ... \leq 0$ cannot contain more than a terms. It follows from Lemma 2.13 that

$$gcd(a,b) = gcd(r_0,r_1) = gcd(r_1,r_2) = ... = gcd(r_{n-2},r_{n-1}) = gcd(r_{n-1},r_n) = gcd(r_n,0),$$

Hence, the greatest common divisor is the last nonzero remainder in the sequence of divisions.

Example 2.40. Find the greatest common divisor of 414 and 662 using the Euclidean algorithm.

Solution. Successive uses of the division algorithm give:

$$\begin{aligned}
662 &= 414 \cdot 1 + 248\\
414 &= 248 \cdot 1 + 166\\
248 &= 166 \cdot 1 + 82\\
166 &= 82 \cdot 2 + 2\\
82 &= 2 \cdot 41
\end{aligned}$$

Hence, $gcd(414,662) = 2$, because 2 is the last nonzero remainder. ■

GCD as Linear Combination

Theorem 2.14. *BEZOUT'S THEOREM If a and b are positive integers, then there exist integers s and t such that $gcd(a,b) = sa + tb$.*

Definition 28: 1

a and b are positive integers, then integers s and t such that $gcd(a,b) = sa + tb$ are called **Bezout coefficients** of a and b. Also, the equation $gcd(a,b) = sa + tb$ is called **Bezout's identity**.

Example 2.41. Express $gcd(6,14)$ as a linear combination of 6 and 14

Example 2.42. Express $gcd(252, 198) = 18$ as a linear combination of 252 and 198 by working backwards through the steps of the Euclidean algorithm.

Example 2.43. Express $gcd(330, 156) = 6$ as a linear combination of 330 and 156 by working backwards through the steps of the Euclidean algorithm.

Finding an Inverse Modulo n

Recall that the identity element of multiplication is 1. Hence, x is a multiplicative inverse of a modulo m if $a * x$ and 1 are congruent modulo m:

The multiplicative modular inverse does not always exist! If it does exists, however, all numbers of the form $x + k * m$ satisfy the required congruency. In particular, in such cases you can always find the solution (exactly one!) in the range $\{1, ..., m - 1\}$.

Corollary 2.15. *For all integers a and n, if $gcd(a, n) = 1$, then there exists an integer x such that $ax \equiv 1(modn)$, and so x is an inverse for a modulo n.*

Example 2.44. Find an inverse of 3 modulo 7

Example 2.45. Find an inverse for 43 modulo 660.

Example 2.46. Find a positive inverse for 3 modulo 40

Example 2.47. Find an inverse of 101 modulo 4620

Once we have an inverse a^{-1} of a modulo m, we can solve the congruence $ax \equiv b(modm)$ by multiplying both sides of the linear congruence by a^{-1},

Example 2.48. What are the solutions of the linear congruence $3x \equiv 4(mod\ 7)$?

Example 2.49. Use inverse to solve linear congruence $57x \equiv 13(mod\ 67)$

The Chinese Remainder Theorem

Theorem 2.16. *Let $m_1, m_2, ..., m_n$ be pairwise relatively prime positive integers greater than one and $a_1, a_2, ..., a_n$ arbitrary integers. Then the system*

$$\begin{aligned} x &\equiv a_1(mod\ m_1), \\ x &\equiv a_2(mod\ m_2), \\ &\cdot \\ &\cdot \\ &\cdot \\ x &\equiv a_n(mod\ m_n), \end{aligned}$$

has a unique solution modulo $m = m_1 m_2 ... m_n$. (That is, there is a solution x with $0 \leq x < m$, and all other solutions are congruent modulo m to this solution.)

1. Find all integers x, $0 \leq x < 15$ such that:

$$\begin{aligned} x &\equiv 1(mod\ 3), \\ x &\equiv 2(mod\ 5), \end{aligned}$$

2. Find all integers x, $0 \leq x < 15$ such that:

$$\begin{aligned} x &\equiv 3(mod\ 7), \\ x &\equiv 6(mod\ 13) \end{aligned}$$

$x \equiv 3 \bmod 7$

$x \equiv 6 \bmod 13$