Divisibility and Factorization

Elementary number theory is the study of the divisibility properties of the integers. Inasmuch as these divisibility properties form the basis for the study of more advanced topics in number theory, they can be thought of as forming the foundation for the entire area of number theory. It is both beautiful and appropriate that such a pure area of mathematics is derived from such a simple source. In addition, the main topics of this chapter are quite old, dating back to the Alexandrian Greek period of mathematics, which began approximately 300 B.C. In fact, most of the ideas discussed here appear in Euclid’s Elements.

In this chapter, we develop the concept of divisibility and the related concept of factorization, which culminate in an extremely important property of the integers appropriately named the Fundamental Theorem of Arithmetic. In addition, we will encounter and highlight certain proof strategies that are used again and again in elementary number theory. These strategies form some of the important “tools of the trade” of the number theorist.

## 1.1 Divisibility

The fundamental relation connecting one integer to another is the notion of divisibility. In terms of long division, the divisibility relation means “divides evenly with zero remainder.” Hence, the integer 3 divides the integer 6 since 3 divides evenly into 6 (two times) with zero remainder. Similarly, the integer 3 does not divide the integer 5, since 3 does not divide evenly into 5; 3 divides into 5 with a quotient of 1 and a remainder of 2. We now make the divisibility relation more mathematically precise.
Proposition I.2: Let \( a, b \in \mathbb{Z} \) and \( c \neq 0 \). Then
\[
(a + b)c = ac + bc.
\]

Proof: Since \( a, b \in \mathbb{Z} \), there exists an integer \( n \) such that \( a = nc \) and an integer \( m \) such that \( b = mc \). Then
\[
algebraic expression
\]
\( (a + b)c = ac + bc \).

Proposition I.2: Let \( a, b \in \mathbb{Z} \) and \( c \neq 0 \). Then
\[
(a + b)c = ac + bc.
\]

Proof: Since \( a, b \in \mathbb{Z} \), there exists an integer \( n \) such that \( a = nc \) and an integer \( m \) such that \( b = mc \). Then
\[
algebraic expression
\]
\( (a + b)c = ac + bc \).

Example 1:

Definition I.1: Let \( a, b \in \mathbb{Z} \). Then \( a \), \( b \) is a divisor of \( c \) if \( c \) is a multiple of \( a \) and \( b \).
We must show that \( q = u + vq = v - v = 0 \)

We have \( r = q \) and \( r = 0 \).

and 

\( q > u \geq 0 \) and \( q > v \geq 0 \). Assume the

last two properties. It remains to show the uniqueness of \( u \) and \( v \) as defined above. Having the

which is precisely what \( q \) is.

Reversing the inequality and adding 0 to all terms

\[ \frac{q}{v} < v < q \]

Multiplying all terms of this inequality by \( q \) we obtain

\[ \frac{q}{v} > 1 - \frac{q}{v} \]

It remains to show that \( u \geq 0 \). By Lemma 1.2 we have that

\[ \frac{q}{v} > 1 - \frac{q}{v} \]

where each number \( q \) is a natural

Theorem 1.2 (The Division Algorithm)

Let \( a \in \mathbb{N} \) and \( b \in \mathbb{N} \). Then

\[ a \equiv b \pmod{a} \]

Furthermore, this number is a unique integer (the divisor)

\[ \frac{a}{b} = \frac{q}{v} \]

more commonly via the equation

The long division on \( \frac{a}{b} \) can be expressed

the long division on \( \frac{a}{b} \) is

\[ \frac{a}{b} = q \]

When one integer (the divisor) is divided into another integer (the dividend)

\[ \frac{a}{b} = q \]

since \( [x] \geq 1 \) is an integer, this contradicts the fact that \([x] = \frac{a}{b} \]

---

Figure 1.1

Remainder

\[ \frac{a}{b} = q \]

Divisor \[ \frac{a}{b} = q \]

Quotient

\[ \frac{a}{b} = q \]

Definition 3: The Euclidean integer function of \( x \) denoted \([x]\) is

The Euclidean integer function of \( x \) denoted \([x]\) is

\[ \frac{a}{b} = q \]

Definition: \([x]\) is the greatest integer function of \( x \).

are integer combinations of \( x \). This fact is extremely

a special case of Proposition 1.2 is important enough to be highlighted

Proposition 1.2: The expression \( a + b \) in Proposition 1.2 is said to be an

Proof: Since the greatest integer function of \( \frac{a}{b} \), \( a \to b \) is the
odd)

Prove that the sum of two odd integers is even (q)
Prove that the product of two even integers are even.
Z ∈ Z, w ∈ Z.
Let w ∈ Z. Prove that w is an odd integer if and only if w = 2n + 1 for some integer n.

Definition 4: Let n ∈ Z. Then n is said to be even if 2n + 1 is and n is said to

be odd if 2n + 1 is even. Note that every integer is either even or odd.

Example 4: Let n ∈ Z. Then n is said to be even if 2n + 1 is and n is said to

be odd if 2n + 1 is even. Note that every integer is either even or odd.

We conclude this section with a definition and an example of concepts with

odd and even numbers.

2.7 The Division Algorithm

We refer to the number a as the dividend, the number b as the divisor, the number q as the

quotient, and the number r as the remainder. We write the division algorithm as:

\[ a = bq + r \]

where \( 0 \leq r < |b| \) and \( b \neq 0 \). This is known as the division algorithm.

The division algorithm is useful in proving various properties of integers and in solving

problems involving divisibility.

Example 5: Consider the integers 12 and 5. We divide 12 by 5 and obtain:

\[ 12 = 5 \times 2 + 2 \]

Thus, 2 is the remainder when 12 is divided by 5.

Exercise 1.1: For each of the following pairs of integers, determine the quotient and

remainder:

1. (15, 3)
2. (22, 7)
3. (101, 9)
4. (123, 11)
5. (89, 4)
6. (78, 6)
7. (67, 2)
8. (56, 5)
9. (45, 3)
10. (34, 2)

Note that in the division algorithm, the quotient and remainder are unique.

Since \( a = bq + r \) and \( 0 \leq r < |b| \), we have that \( r = a - bq \) is a solution.

Note that \( b - 1 \) is the remainder when \( b - 1 \) is divided by 2.

where implies that
\[ u = \sqrt[n]{a} \leq q \Rightarrow q = u \]

We have

**Proposition 1.1: Let \( \sqrt[n]{a} \leq q \geq 1 \). Then \( \sqrt[n]{a} \) is a composite number.**

There exists \( a \neq 1 \) such that \( \sqrt[n]{a} \).

**Proof:**

Since \( n \) is a composite number, let \( n = pq \) where \( p \) is a prime number. Then \( n \) is a prime number.

**Theorem 1.6: (Euclid's Theorem)**

There are infinitely many prime numbers.

**Proof:**

Assume the contrary. Then there are only finitely many prime numbers.

**Lemma 1.5:** Every integer greater than 1 has a prime divisor.

**Proof:**

**Example 5:**

\[ 7 \div 2 = 3.5 \]

\[ 7 \div 2 = 3.5 \]
Example 7

Given the positive integer $n$, consider the composite positive integers $1 + u$ for any integer $u$ in the set of positive integers. 

Proof: Given the positive integer $n$, there are at least two composite positive integers $1 + u$ for any integer $u$ in the set of positive integers. 

Proposition I.8: For any integer $n$ in the set of positive integers, there are at least two composite positive integers $1 + u$ for any integer $u$ in the set of positive integers. 

Proof: Given the positive integer $n$, consider the composite positive integers $1 + u$. 

Biography 

Section I.2 Prime Numbers
Theorem 1:9. (Prime Number Theorem) \[ \lim_{x \to \infty} \frac{\pi(x)}{x/\log x} = 1 \]

We may now state the Prime Number Theorem.

From Example 2, we have that the number of prime numbers less than or equal to 1.5 is 3.

Example 2: (Gouldbach's Conjecture) Even even integers greater than 2 can be expressed as the sum of two (not necessarily distinct) prime numbers.

**Great Leonardo's Prime Number Theory**

The distribution of prime numbers was conjectured by Christian Goldbach in a letter to the Bernoulli brothers. The conjecture states that every even number greater than 2 can be expressed as the sum of two prime numbers.

Definitio 6: Let \( x \in \mathbb{R} \) with \( x < 0 \). Then \( f(x) \) is the absolute value of \( x \).

The most known part of a prime number is \( 1700597 \) and \( 27503000 \). The number of prime numbers less than or equal to 10 is 4, and \( \pi(x) \) is the function that gives the number of primes less than or equal to \( x \).

<table>
<thead>
<tr>
<th>x</th>
<th>( \pi(x) )</th>
<th>( \frac{x}{\log x} )</th>
<th>( \frac{\pi(x)}{x/\log x} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>1.5</td>
<td>1.333</td>
</tr>
<tr>
<td>5</td>
<td>3</td>
<td>2</td>
<td>1.5</td>
</tr>
<tr>
<td>7</td>
<td>4</td>
<td>2.857</td>
<td>1.416</td>
</tr>
<tr>
<td>11</td>
<td>5</td>
<td>3.618</td>
<td>1.386</td>
</tr>
<tr>
<td>13</td>
<td>6</td>
<td>4.535</td>
<td>1.327</td>
</tr>
<tr>
<td>17</td>
<td>7</td>
<td>5.849</td>
<td>1.269</td>
</tr>
<tr>
<td>19</td>
<td>8</td>
<td>6.907</td>
<td>1.227</td>
</tr>
<tr>
<td>23</td>
<td>9</td>
<td>8.453</td>
<td>1.185</td>
</tr>
<tr>
<td>29</td>
<td>10</td>
<td>10.293</td>
<td>1.155</td>
</tr>
</tbody>
</table>

**Theorem 1:9. (Prime Number Theorem)** \( \lim_{x \to \infty} \frac{\pi(x)}{x/\log x} = 1 \)

We may now state the Prime Number Theorem.
A. Exercises 1.2

1. Determine whether the following positive integers are prime or composite.

Section 1.2 Prime Numbers

B. Definition 6: Any prime number expressible in the form $2n + 1$ is a Fermat prime.

C. Definition 7: The second form for prime numbers is named after French mathematician Pierre de Fermat.

D. Conjecture 3: There are infinitely many Fermat primes. In any given sequence of positive integers, no matter what sequence of integers is chosen, there are infinitely many prime numbers expressible in the form $2n + 1$.
Proposition 7.1: Let $a, b \in \mathbb{Z}$ with $a$ and $b$ not both zero. Then
\[
|a - b| = \text{gcd}(a, b)
\]

Proof: Let $d \in \mathbb{Z}$ be such that $d$ is the greatest common divisor of $a$ and $b$. Then $d$ divides both $a$ and $b$, so $d$ is the greatest number that can divide both $a$ and $b$. Moreover, if $c$ divides both $a$ and $b$, then $c$ must divide $d$. Thus $d$ is the greatest number that can divide both $a$ and $b$. Therefore, $d = \text{gcd}(a, b)$.

Proposition 7.2: Let $a, b \in \mathbb{Z}$ with $a$ and $b$ not both zero. Then
\[
|a + b| = \text{gcd}(a, b)
\]

Proof: The proof is similar to Proposition 7.1.

Proposition 7.3: Let $a, b, c \in \mathbb{Z}$ with $a$ and $b$ not both zero. Then
\[
|a - b| = \text{gcd}(a, b)
\]

Proof: The proof is similar to Proposition 7.1.

Example 7.1: Find the greatest common divisor of $24$ and $36$.

Solution: The greatest common divisor of $24$ and $36$ is $12$.

Section 1.3: Greatest Common Divisors

Definition 7.4: A prime number is a natural number that has exactly two distinct positive divisors: $1$ and the number itself.

Theorem 7.5: Every natural number greater than $1$ is either a prime number or can be written as a product of prime numbers.

Proof: The proof is by induction on the natural numbers.

Theorem 7.6: Every natural number greater than $1$ is either a prime number or can be written as a product of prime numbers.

Proof: The proof is by induction on the natural numbers.

Theorem 7.7: Every natural number greater than $1$ is either a prime number or can be written as a product of prime numbers.

Proof: The proof is by induction on the natural numbers.

Theorem 7.8: Every natural number greater than $1$ is either a prime number or can be written as a product of prime numbers.

Proof: The proof is by induction on the natural numbers.

Theorem 7.9: Every natural number greater than $1$ is either a prime number or can be written as a product of prime numbers.

Proof: The proof is by induction on the natural numbers.

Theorem 7.10: Every natural number greater than $1$ is either a prime number or can be written as a product of prime numbers.

Proof: The proof is by induction on the natural numbers.

Theorem 7.11: Every natural number greater than $1$ is either a prime number or can be written as a product of prime numbers.

Proof: The proof is by induction on the natural numbers.
Example 12:

**Definition 10:** Let \( a \) be any positive integer. The *least common multiple* of \( a \) and \( b \) is the smallest positive integer that is a multiple of both \( a \) and \( b \).

The concept of greatest common divisor can be extended in two ways:

1. **Extended Euclidean Algorithm:** This method computes the greatest common divisor of more than two integers.
2. **Least Common Multiple (LCM):** Given two integers, the LCM is the smallest positive integer that is a multiple of both integers.

**Example 13:**

In Exercise 3, we proved that if \( p \) is a prime number, then \( p \) is a prime in \( \mathbb{Z}_p \).

The integers \( a \) and \( b \) are relatively prime (meaning \( \gcd(a, b) = 1 \)). Then for some integers \( x \) and \( y \), we have \( ax + by = 1 \). We now show that if \( p \) is a prime number, then \( p \) is prime in \( \mathbb{Z}_p \).

**Proof:** Suppose \( p \) is not prime in \( \mathbb{Z}_p \). Then there exists a non-unit \( a \) and a unit \( b \) such that \( p \mid ab \), so \( p \mid a \) or \( p \mid b \). Since \( p \) is prime in \( \mathbb{Z}_p \), we conclude that \( p \mid x \) or \( p \mid y \). But this means that \( p \) divides some multiple of \( a \), contradicting the fact that \( p \) is prime in \( \mathbb{Z}_p \). Therefore, \( p \) must be prime in \( \mathbb{Z}_p \).
Section 1.4  The Euclidean Algorithm

The Euclidean Algorithm

Let $a \in \mathbb{Z}$ and $b \in \mathbb{Z}$. Suppose that $a > b$. Then, $a = bq + r$, where $0 \leq r < b$. If $r = 0$, then $b$ divides $a$ and we are done. Otherwise, we use the division algorithm on $b$ and $r$ to obtain $b = rq + s$, where $0 \leq s < r$. We continue this process until we reach a remainder of 0.

Theorem 1.13  The Euclidean Algorithm

1. Let $a$ and $b$ be positive integers. Then, $\gcd(a, b)$ exists and is the greatest common divisor of $a$ and $b$.
2. Let $a$ and $b$ be positive integers. Then, $\gcd(a, b) = \gcd(b, a-b)$.
3. Let $a = bq + r$, where $0 \leq r < b$. Then, $\gcd(a, b) = \gcd(b, r)$.
4. Let $a$ and $b$ be positive integers. Then, $\gcd(a, b) = \gcd(b, a-b)$.
5. Let $a$ and $b$ be positive integers. Then, $\gcd(a, b) = \gcd(b, a-b)$.

Proof: The proof is straightforward application of the division algorithm.

Lemma 1.12  The Euclidean Algorithm

Let $a$, $b$, and $c$ be positive integers. Suppose that $a$ divides $b$ and $a$ divides $c$. Then, $a$ divides $b + c$.

Proof: Suppose that $a$ divides $b$ and $a$ divides $c$. Then, there exist integers $m$ and $n$ such that $b = am$ and $c = an$. Therefore, $b + c = am + an = a(m + n)$. Hence, $a$ divides $b + c$.

Theorem 1.14  The Euclidean Algorithm

Let $a$ and $b$ be positive integers. Then, there exist integers $x$ and $y$ such that $ax + by = \gcd(a, b)$.

Proof: We use the extended Euclidean algorithm.

Algorithm 1: The Euclidean Algorithm

1. Let $a$ and $b$ be positive integers. If $b = 0$, then $\gcd(a, b) = a$. Otherwise, let $r = a \mod b$.
2. If $r = 0$, then $\gcd(a, b) = b$. Otherwise, replace $a$ with $b$ and $b$ with $r$ and return to step 1.

Example: Let $a = 34$ and $b = 12$. Then, $34 \mod 12 = 10$, so we replace $a$ with $12$ and $b$ with $10$. Then, $12 \mod 10 = 2$, so we replace $a$ with $10$ and $b$ with $2$. Then, $10 \mod 2 = 0$, so we have found that $\gcd(34, 12) = 2$. Hence, $34 \cdot 1 + 12 \cdot (-3) = 2$.

Theorem 1.15  The Euclidean Algorithm

Let $a$ and $b$ be positive integers. Then, $\gcd(a, b) = ax + by$, where $x$ and $y$ are the integers found in the extended Euclidean algorithm.

Proof: We use the properties of the greatest common divisor.

Theorem 1.16  The Euclidean Algorithm

Let $a$ and $b$ be positive integers. Then, $\gcd(a, b) = \gcd(b, a-b)$.

Proof: We use the properties of the greatest common divisor.
Exercise Set 1.4

A useful programming project related to Example 1.4 and 1.5 appears as

will how more to 8 in this to use Excel 5.

many expressions for a general integer combination of 8 and 15. We

11 = 696 - 592 = 99 - 696 is another useful expression. In fact, these are

of 89 and 154 above is not unique. For example, the result may vary

Section 1.4 The Euclidean Algorithm

Example 1.5:

The Euclidean algorithm provides a systematic procedure for obtaining such a

1. Write the problem statement. T114 = 114 = 114 + 52 = 114 + 37 = 114 + 25 = 114 + 17 = 114 + 14 = 114 + 9 = 114 + 3 = 114 + 1 = 114

Example 1.4: By using the Euclidean algorithm,

the division algorithm.

For example, a = 89 and b = 154.

other combinations are quite possible to this case of initial. We now

24 Chapter 1 Divisibility and Factorization
We now state and prove the Fundamental Theorem of Arithmetic.

**Theorem 1.16 (Fundamental Theorem of Arithmetic).** Every integer greater than 1 can be expressed in the form of a product of prime numbers, and this expression is unique up to the order of the factors. Assume by way of contradiction that \( \mathbb{N} \) contains two such representations:

\[
\prod_{p \in S} p = \prod_{q \in T} q
\]

where \( S \) and \( T \) are finite sets of prime numbers and \( |S| = |T| \). Then \( \mathbb{N} \) contains two such representations:

\[
\prod_{p \in S} p = \prod_{q \in T} q
\]

where \( S \) and \( T \) are finite sets of prime numbers and \( |S| = |T| \). Then \( \mathbb{N} \) contains two such representations:

\[
\prod_{p \in S} p = \prod_{q \in T} q
\]

where \( S \) and \( T \) are finite sets of prime numbers and \( |S| = |T| \). Then \( \mathbb{N} \) contains two such representations:

\[
\prod_{p \in S} p = \prod_{q \in T} q
\]

where \( S \) and \( T \) are finite sets of prime numbers and \( |S| = |T| \). Then \( \mathbb{N} \) contains two such representations:

\[
\prod_{p \in S} p = \prod_{q \in T} q
\]

where \( S \) and \( T \) are finite sets of prime numbers and \( |S| = |T| \). Then \( \mathbb{N} \) contains two such representations:

\[
\prod_{p \in S} p = \prod_{q \in T} q
\]

where \( S \) and \( T \) are finite sets of prime numbers and \( |S| = |T| \). Then \( \mathbb{N} \) contains two such representations:

\[
\prod_{p \in S} p = \prod_{q \in T} q
\]

where \( S \) and \( T \) are finite sets of prime numbers and \( |S| = |T| \). Then \( \mathbb{N} \) contains two such representations:

\[
\prod_{p \in S} p = \prod_{q \in T} q
\]

where \( S \) and \( T \) are finite sets of prime numbers and \( |S| = |T| \). Then \( \mathbb{N} \) contains two such representations:

\[
\prod_{p \in S} p = \prod_{q \in T} q
\]

where \( S \) and \( T \) are finite sets of prime numbers and \( |S| = |T| \). Then \( \mathbb{N} \) contains two such representations:

\[
\prod_{p \in S} p = \prod_{q \in T} q
\]

where \( S \) and \( T \) are finite sets of prime numbers and \( |S| = |T| \). Then \( \mathbb{N} \) contains two such representations:

\[
\prod_{p \in S} p = \prod_{q \in T} q
\]

where \( S \) and \( T \) are finite sets of prime numbers and \( |S| = |T| \). Then \( \mathbb{N} \) contains two such representations:

\[
\prod_{p \in S} p = \prod_{q \in T} q
\]

where \( S \) and \( T \) are finite sets of prime numbers and \( |S| = |T| \). Then \( \mathbb{N} \) contains two such representations:

\[
\prod_{p \in S} p = \prod_{q \in T} q
\]

where \( S \) and \( T \) are finite sets of prime numbers and \( |S| = |T| \). Then \( \mathbb{N} \) contains two such representations:

\[
\prod_{p \in S} p = \prod_{q \in T} q
\]

where \( S \) and \( T \) are finite sets of prime numbers and \( |S| = |T| \). Then \( \mathbb{N} \) contains two such representations:

\[
\prod_{p \in S} p = \prod_{q \in T} q
\]

where \( S \) and \( T \) are finite sets of prime numbers and \( |S| = |T| \). Then \( \mathbb{N} \) contains two such representations:

\[
\prod_{p \in S} p = \prod_{q \in T} q
\]

where \( S \) and \( T \) are finite sets of prime numbers and \( |S| = |T| \). Then \( \mathbb{N} \) contains two such representations:

\[
\prod_{p \in S} p = \prod_{q \in T} q
\]

where \( S \) and \( T \) are finite sets of prime numbers and \( |S| = |T| \). Then \( \mathbb{N} \) contains two such representations:

\[
\prod_{p \in S} p = \prod_{q \in T} q
\]

where \( S \) and \( T \) are finite sets of prime numbers and \( |S| = |T| \). Then \( \mathbb{N} \) contains two such representations:

\[
\prod_{p \in S} p = \prod_{q \in T} q
\]

where \( S \) and \( T \) are finite sets of prime numbers and \( |S| = |T| \). Then \( \mathbb{N} \) contains two such representations:

\[
\prod_{p \in S} p = \prod_{q \in T} q
\]

where \( S \) and \( T \) are finite sets of prime numbers and \( |S| = |T| \). Then \( \mathbb{N} \) contains two such representations:

\[
\prod_{p \in S} p = \prod_{q \in T} q
\]

where \( S \) and \( T \) are finite sets of prime numbers and \( |S| = |T| \). Then \( \mathbb{N} \) contains two such representations:

\[
\prod_{p \in S} p = \prod_{q \in T} q
\]

where \( S \) and \( T \) are finite sets of prime numbers and \( |S| = |T| \). Then \( \mathbb{N} \) contains two such representations:

\[
\prod_{p \in S} p = \prod_{q \in T} q
\]

where \( S \) and \( T \) are finite sets of prime numbers and \( |S| = |T| \). Then \( \mathbb{N} \) contains two such representations:

\[
\prod_{p \in S} p = \prod_{q \in T} q
\]

where \( S \) and \( T \) are finite sets of prime numbers and \( |S| = |T| \). Then \( \mathbb{N} \) contains two such representations:

\[
\prod_{p \in S} p = \prod_{q \in T} q
\]

where \( S \) and \( T \) are finite sets of prime numbers and \( |S| = |T| \). Then \( \mathbb{N} \) contains two such representations:

\[
\prod_{p \in S} p = \prod_{q \in T} q
\]

where \( S \) and \( T \) are finite sets of prime numbers and \( |S| = |T| \). Then \( \mathbb{N} \) contains two such representations:

\[
\prod_{p \in S} p = \prod_{q \in T} q
\]

where \( S \) and \( T \) are finite sets of prime numbers and \( |S| = |T| \). Then \( \mathbb{N} \) contains two such representations:

\[
\prod_{p \in S} p = \prod_{q \in T} q
\]

where \( S \) and \( T \) are finite sets of prime numbers and \( |S| = |T| \). Then \( \mathbb{N} \) contains two such representations:

\[
\prod_{p \in S} p = \prod_{q \in T} q
\]

where \( S \) and \( T \) are finite sets of prime numbers and \( |S| = |T| \). Then \( \mathbb{N} \) contains two such representations:

\[
\prod_{p \in S} p = \prod_{q \in T} q
\]

where \( S \) and \( T \) are finite sets of prime numbers and \( |S| = |T| \). Then \( \mathbb{N} \) contains two such representations:

\[
\prod_{p \in S} p = \prod_{q \in T} q
\]
The positive multiples of 6 are 6, 12, 18, 24, 30, 36, 42, 48, 54, 60, ... From the above, it's a matter of fact that 54 is the least common multiple of 6 and 9.

Example 17:

Find the prime factorization of 75.

We have

\[ 75 = 3 \times 3 \times 5 \times 5 \]

By Theorem 14, we have 75 = \( 3 \times 3 \times 5 \times 5 \) by using prime factorization.

Example 16:

From which we deduce that 6 and 9 are in the same equivalence class modulo 3. However, their quotient 2 is not in the same equivalence class. So

\[ a = b \pmod{p} \quad \text{for some } \neq c \]
We conclude this chapter with another illustration of the power of the

**Proposition.** Let \( a \in \mathbb{Z} \) with \( a \neq 0 \) and \( (a, q) = 1 \). Then the alternative

\[
\text{Theorem 1.22: Dirichlet's Theorem on Prime Numbers in Arithmetic Progressions.}
\]

The result of this theorem is beyond the scope of this book.

**Theorem 1.19.** The border is not sufficient as the next corollary shows.

**Theorem 1.7:** When we consider the linear equations in the integers, the

\[
\text{Lemma 1.19: Let } a \in \mathbb{Z} \text{ with } a, q \in \mathbb{Z}, q > 0. \text{ Then } \begin{cases} (b, q) = 1 \end{cases} \text{ if and only if}
\]

Proposition: \( (a, q) = 1 \) when \( a \), \( q \) and \( (a, q) = 1 \) are relatively prime.

We start with an exercise for the reader.

![Image of a person with a mathematical expression]

**Corollary 1.20.** Let \( a \in \mathbb{Z} \) with \( a, q \in \mathbb{Z}, q > 0 \). Then \( (a, q) = 1 \) if and only if

\[
\text{Example 1.1:}
\]

The reader is invited to prove here to complete \( \mathcal{O}(3, 14) \) using \( \mathcal{O}(3, 149) \).

**Theorem 1.17:** Which gives us the linear equations in the integers. The

\[
\text{The reader is invited to prove here to complete \( \mathcal{O}(3, 14) \) using \( \mathcal{O}(3, 149) \).}
\]

The reader is invited to prove here to complete \( \mathcal{O}(3, 14) \) using \( \mathcal{O}(3, 149) \). The

**Proposition 1.17:** Which gives us the linear equations in the integers. The

\[
\text{The reader is invited to prove here to complete \( \mathcal{O}(3, 14) \) using \( \mathcal{O}(3, 149) \).}
\]

**Theorem 1.19:** The border is not sufficient as the next corollary shows.

**Theorem 1.7:** When we consider the linear equations in the integers, the

\[
\text{Lemma 1.19: Let } a \in \mathbb{Z} \text{ with } a, q \in \mathbb{Z}, q > 0. \text{ Then } \begin{cases} (b, q) = 1 \end{cases} \text{ if and only if}
\]

Proposition: \( (a, q) = 1 \) when \( a \), \( q \) and \( (a, q) = 1 \) are relatively prime.

We start with an exercise for the reader.

![Image of a person with a mathematical expression]
Find the least common multiple below.

69. Definition: Let \(\mathbb{Z}^+\) denote the set of positive integers and \(\mathbb{Z}\) denote the set of integers. The least common multiple of \(a, b \in \mathbb{Z}\) is the least positive integer \(c\) such that \(c \mid a, b\).

\[ \text{L.C.M.}(a, b) = \min(c \in \mathbb{Z}^+ : c \mid a, b) \]

Exercises Set I.5

Exercise 8: Prove Proposition 1.2.

Exercise 9: Find the least common multiple of each pair of integers.

Exercise 10: Prove Proposition 1.3.

Proof: Consider the set of all multiples of \(a\) and \(b\), which is \(\{ka : k \in \mathbb{Z}^+\}\) and \(\{kb : k \in \mathbb{Z}^+\}\) respectively. The least common multiple of \(a\) and \(b\) is the smallest positive integer in the intersection of these sets.

Lemma 1.2: Let \(n \in \mathbb{Z}^+\). If \(a, b \mid n\), then \(\text{G.C.D.}(a, b) \mid n\).

Proof: Assume \(a, b \mid n\) and \(\text{G.C.D.}(a, b) = d\). Since \(d\) is the greatest common divisor of \(a\) and \(b\), it divides any linear combination of \(a\) and \(b\), including \(n\). Thus, \(d \mid n\).

Lemma 1.3: Let \(a, b \in \mathbb{Z}\). If \(a\) and \(b\) are not both zero, then \(a, b \mid n\) if and only if \(\text{G.C.D.}(a, b) \mid n\).

Proof: If \(a, b \mid n\), then \(\text{G.C.D.}(a, b) \mid n\) by the definition of the greatest common divisor. Conversely, if \(\text{G.C.D.}(a, b) \mid n\), then \(a, b \mid n\) by the same property.
Theorem 15.1: The Fundamental Theorem of Arithmetic

Let \(\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \ldots\}\) and let \(n \in \mathbb{Z}\) be a positive integer. Then there exists a unique finite sequence of primes\(p_1, p_2, \ldots, p_r\), such that

\[
\frac{n}{\prod_{i=1}^{r} p_i} = q
\]

where \(q\) is a positive integer and \(\prod_{i=1}^{r} p_i\) is the product of the primes in the sequence.

Proof: By the Well-Ordering Principle, there exists a least positive integer \(n\) such that the theorem is not true. Let \(n\) be the smallest such integer.

If \(n = 1\), then the theorem is true. If \(n > 1\), then there exists a prime \(p\) such that \(p \mid n\). Define \(q = n/p\). Then \(q < n\) and \(q\) is a positive integer. By the Well-Ordering Principle, there exists a smallest positive integer \(q\) such that \(q < n\) and \(q\) is a positive integer.

Since \(\mathbb{Z}\) is closed under multiplication and division, \(q\) is also a positive integer. By the Well-Ordering Principle, there exists a smallest positive integer \(q\) such that \(q < n\) and \(q\) is a positive integer.

Let \(r = n/p\). Then \(r < n\) and \(r\) is a positive integer. By the Well-Ordering Principle, there exists a smallest positive integer \(r\) such that \(r < n\) and \(r\) is a positive integer.

Since \(\mathbb{Z}\) is closed under multiplication and division, \(r\) is also a positive integer. By the Well-Ordering Principle, there exists a smallest positive integer \(r\) such that \(r < n\) and \(r\) is a positive integer.

Then \(\frac{n}{\prod_{i=1}^{r} p_i} = q\), and the theorem is true. Therefore, there exists a unique finite sequence of primes\(p_1, p_2, \ldots, p_r\), such that

\[
\frac{n}{\prod_{i=1}^{r} p_i} = q
\]

where \(q\) is a positive integer and \(\prod_{i=1}^{r} p_i\) is the product of the primes in the sequence.

Q.E.D.
Chapter 1: Divisibility and Factorization

Student Projects

1. Proving a property of binomial coefficients.

2. Proving a property of integers and expressing it as an integer linear combination.

3. Proving a property of prime numbers.

4. Proving a property of factorials.