1.2 Properties of Integers

1.2.1 The Well Ordering Principle and the Division Algorithm

We now focus on a special set, the integers, denoted $\mathbb{Z}$, as this set plays an important role in abstract algebra. We begin with an important result we will use often, the Well Ordering Principle. We will state it as an axiom, as it cannot be proven using the usual properties of arithmetic.

**Axiom 23 (Well Ordering Principle)** Every nonempty set of positive integers contains a smallest element.

**Example 24** $S = \{1, 3, 5, 7, 9\}$ is a set of positive integers. Its smallest element is 1.

Can we say the same about sets of positive real numbers?

Next, we look at the concept of divisibility, an important concept in number theory.

**Definition 25** A nonzero integer $t$ is a **divisor** of an integer $s$ and we write $t \mid s$ (read "$t$ divides $s$") if there exists an integer $k$ such that $s = kt$. In this case, we also say that $s$ is a **multiple** of $t$. When $t$ is not a divisor of $s$, we write $t \nmid s$.

**Definition 26** A **prime** is a positive integer greater than 1 whose only positive divisors are 1 and itself.

**Example 27** The divisors of 8 are $\pm 1, \pm 2, \pm 4$ and $\pm 8$.

**Example 28** The divisors of 7 are $\pm 1$ and $\pm 7$. So, 7 is prime.

**Example 29** What are the divisors of 0?

A fundamental property of the integers is the division algorithm. Its proof involves the Well Ordering Principle. We now state and prove this result which we will use often.

**Theorem 30 (Division Algorithm)** Let $a$ and $b$ be integers with $b > 0$. Then, there exists unique integers $q$ and $r$ with the property that

$$a = bq + r$$

(1.1)

where $0 \leq r < b$

**Proof.** First we prove existence, then uniqueness.

- **Existence.** With $a$ and $b$ as given, consider the set $S = \{a - bk \mid k \text{ is an integer and } a - bk \geq 0\}$. Either $0 \in S$ or $0 \notin S$. 

1.2. PROPERTIES OF INTEGERS

The Euclidean algorithm is a method for finding the greatest common divisor (gcd) of two integers. It is based on the principle that the gcd of two integers also divides their difference. We repeat the process with the smaller integer and the remainder until we get a remainder of zero. The last non-zero remainder is the gcd.

**Remark 31** This is the division you have been doing since you were little. $r$ is the remainder. If $r = 0$, then $b \mid a$.

**Example 32** For $a = 20$ and $b = 3$, the algorithm gives $20 = 3 \cdot 6 + 2$.

### 1.2.2 Greatest Common Divisor, Relatively Prime Integers

**Definition 33 (Greatest Common Divisor)** Let $m$ and $n$ be two nonzero integers. The **greatest common divisor** of $m$ and $n$, denoted $\gcd(m, n)$, is defined to be the largest of all common divisors of $m$ and $n$.

**Definition 34 (Relatively Prime)** Two nonzero integers $m$ and $n$ are said to be relatively prime if $\gcd(m, n) = 1$.

There are different techniques to find $\gcd(a, b)$. We illustrate one known as the **Euclidean algorithm**. We begin with some remarks. Suppose we are given integers $a$ and $b$, assume $a \geq b$. Then, by the division algorithm, there exists unique integers $q_1$ and $r_1$, $0 \leq r_1 < b$ such that $a = bq_1 + r_1$. Any integer dividing $a$ and $b$ will also divide $b$ and $r_1$ (see problems) hence $\gcd(a, b) = \gcd(b, r_1)$

We repeat the process with $b$ and $r_1$. There exists unique integers $q_2$ and $r_2$, $0 \leq r_2 < r_1$ such that $b = r_1q_2 + r_2$. As before, $\gcd(b, r_1) = \gcd(r_1, r_2)$. We
repeat the process with \( r_1 \) and \( r_2 \) to obtain unique integers \( q_3 \) and \( r_3 \), \( 0 \leq r_3 < r_2 \) such that \( r_1 = r_2 q_3 + r_3 \). As before \( \gcd (r_1, r_2) = \gcd (r_2, r_3) \). Continuing this way, we obtain a sequence of remainders \( r_1 > r_2 > r_3 \ldots \) where each \( r_i \geq 0 \). By the well ordering principle, this process has to stop and some \( r_i \) must eventually be 0. We have

\[
\gcd (a, b) = \gcd (b, r_1) = \gcd (r_1, r_2) = \ldots = \gcd (r_i, 0) = r_i
\]

See the problems for the last equality. Thus, \( \gcd (a, b) \) is the last nonzero remainder arising from our repeated division. We illustrate this with an example.

Example 35  Let’s find \( \gcd (100, 64) \).

\[
\begin{align*}
100 & = 64 \cdot 1 + 36 \\
64 & = 36 \cdot 1 + 28 \\
36 & = 28 \cdot 1 + 8 \\
28 & = 8 \cdot 3 + 4 \\
8 & = 4 \cdot 2 + 0
\end{align*}
\]

Thus \( \gcd (100, 64) = 4 \).

Remark 36  If a number is written as a product of prime factors, then finding the greatest common divisor is simply a matter of gathering the common prime factors which are common to both. More specifically, if \( a = p_1^{h_1} p_2^{h_2} \ldots p_n^{h_n} \) and \( b = p_1^{k_1} p_2^{k_2} \ldots p_n^{k_n} \) where \( p_i \) are primes, with the understanding that some of the \( k_i \) or \( h_i \) might be 0 (if the corresponding prime is not present) and if we define \( s_i = \min (h_i, k_i) \) for each \( i = 1 \ldots n \), then

\[
\gcd (a, b) = p_1^{s_1} p_2^{s_2} \ldots p_n^{s_n}
\]

Example 37  Find \( \gcd (2^3 \cdot 3^2 \cdot 5^4, 2 \cdot 5^2 \cdot 7) \)

\[
\begin{align*}
\gcd (2^3 \cdot 3^2 \cdot 5^4, 2 \cdot 5^2 \cdot 7) &= 2 \cdot 5 \cdot 7 \\
&= 70
\end{align*}
\]

Theorem 38  For any nonzero integers \( a \) and \( b \), there exists integers \( s \) and \( t \) such that

\[
\gcd (a, b) = as + bt
\]

Moreover, \( \gcd (a, b) \) is the smallest positive integer of the form \( as + bt \).

Proof.  There are different ways to prove the existence part. We outline them here.

Method 1:  Here, we only show that \( \gcd (a, b) = as + bt \). We use the Euclidean algorithm developed above. So, this is a constructive proof. It will show
us how to find \( s \) and \( t \). Let us assume that the Euclidean algorithm gave us the following:

\[
\begin{align*}
a &= bq_1 + r_1 \\
b &= r_1q_2 + r_2 \\
r_1 &= r_2q_3 + r_3 \\
&\vdots \\
r_{i-3} &= r_{i-2}q_{i-1} + r_{i-1} \\
r_{i-2} &= r_{i-1}q_i + r_i \\
r_{i-1} &= r_iq_{i+1} + 0
\end{align*}
\]

Thus \( \gcd(a, b) = r_i \). But using \( r_{i-2} = r_{i-1}q_i + r_i \), we can write \( r_i = r_{i-2} - r_{i-1}q_i \) thus writing \( r_i \) as a linear combination of \( r_{i-1} \) and \( r_{i-2} \). Using the previous equation, we can write \( r_{i-1} = r_{i-3} - r_{i-2}q_{i-1} \) thus we can express \( r_i \) as a linear combination of \( r_{i-2} \) and \( r_{i-3} \). Using all the equations in the Euclidean algorithm in reverse order, we can express \( r_i \) as a linear combination of \( a \) and \( b \).

**Method 2:** This proof involves the division algorithm and the Well Ordering Principle. It is similar in some ways to the proof of the division algorithm. Here, we will prove everything stated in the theorem. But this proof is not constructive, it does not tell us how to find \( s \) and \( t \). Consider the set \( S = \{am + bn \mid am + bn > 0 \text{ and } m \text{ and } n \text{ are integers}\} \). Since \( a, b, m, n \) are all integers, \( am + bn \) is an integer. So, \( S \) is a set of positive integers. It is not empty because if \( am + bn < 0 \) then \( a(-m) + b(-n) > 0 \). Thus, by the Well Ordering Principle, \( S \) has a smallest member, say \( d = as + bt \).

We now prove that \( d = \gcd(a, b) \). For this, we first prove that \( d \) is a divisor of both \( a \) and \( b \) and then that it is in fact, the largest common divisor.

- **\( d \) is a divisor of both \( a \) and \( b \).** First, we establish \( d \) divides \( a \). Using the division algorithm, we can write \( a = dq + r \) with \( 0 \leq r < d \).
  If we had \( r > 0 \), then

\[
\begin{align*}
r &= a - dq \\
&= a - (as + bt)q \\
&= a - asq - btq \\
&= a(1 - sq) + b(-tq)
\end{align*}
\]

Thus we would have \( a(1 - sq) + b(-tq) \in S \) contradicting \( d \) is the smallest member of \( S \). Thus \( r = 0 \) hence \( a = dq \) or \( d \mid a \). We can carry a similar argument for \( d \mid b \). Hence, \( d \) is a common divisor to both \( a \) and \( b \).

- **\( d \) is the largest common divisor to both \( a \) and \( b \).** Suppose \( d' \) is another common divisor to both \( a \) and \( b \) that is \( a = d'h \) and \( b = d'k \).
Then, \( d = as + bt = d'h + d'kt = d'(hs + kt) \) so \( d' \) is a divisor of \( d \), hence \( d > d' \). Thus \( d \) is the greatest common divisor.

There is an important corollary of this theorem, which we will often use.

**Remark 39** The proof shown in method 1: also gives a way to find what that combination is.

**Example 40** Find \( s \) and \( t \) such that \( \gcd(100, 64) = 100s + 64t \).

Recall from above that \( \gcd(100, 64) = 4 \). Using our computations above, we have

\[
4 = 28 - 8 \cdot 3 \\
= 28 - 3 \cdot (36 - 28 \cdot 1) \\
= 4 \cdot 28 - 3 \cdot 36 \\
= 4 \cdot (64 - 36) - 3 \cdot 36 \\
= 4 \cdot 64 - 7 \cdot 36 \\
= 4 \cdot 64 - 7(100 - 64) \\
= -7 \cdot 100 + 11 \cdot 64
\]

**Corollary 41** If \( a \) and \( b \) are relatively prime, then there exists integers \( s \) and \( t \) such that \( as + bt = 1 \).

The next lemma is very important and often used.

**Lemma 42 (Euclid’s Lemma)** Let \( a \) and \( b \) be integers. If \( p \) is prime and \( p \mid ab \) then \( p \mid a \) or \( p \mid b \).

**Proof.** It is enough to prove that if \( p \nmid a \) then we must have \( p \mid b \). So, suppose \( p \mid ab \) and \( p \nmid a \). Then \( a \) and \( p \) are relatively prime and therefore there exist integers \( s \) and \( t \) such that \( 1 = as + pt \). Then, \( b = abs + bpt \). Since \( p \) divides the right hand side, it must also divide \( b \). ■

This fact is used in particular when proving that \( \sqrt{p} \) is irrational when \( p \) is prime.

Prime numbers are extremely important when dealing with integers. They are their building blocks, as the next result shows.

**Theorem 43 (Fundamental Theorem of Arithmetic)** Every integer greater than 1 is either prime or a product of primes. This product is unique, except for the order of the factors.

**Proof.** We will prove this result later in the chapter. ■

**Example 44** \( 66 = 2 \times 3 \times 11 \)

**Example 45** \( 100 = 2^25^2 \)
1.2. PROPERTIES OF INTEGERS

We finish this section with the notion of least common multiple.

**Definition 46 (Least Common Multiple)** The least common multiple of two nonzero integers is the smallest positive integer that is a multiple of both integers. It is denoted \(\text{lcm}(a, b)\).

**Remark 47** One way to compute \(\text{lcm}(a, b)\) is to factor \(a\) and \(b\) as a product of primes and gather all the primes with the highest power which appear. More specifically, if \(a = p_1^{h_1}p_2^{h_2}...p_n^{h_n}\) and \(b = p_1^{k_1}p_2^{k_2}...p_n^{k_n}\) where \(p_i\) are primes, with the understanding that some of the \(k_i\) or \(h_i\) might be 0 (if the corresponding prime is not present) and if we define \(m_i = \max(h_i, k_i)\) for each \(i = 1..n\), then

\[
\text{lcm}(a, b) = p_1^{m_1}p_2^{m_2}...p_n^{m_n}
\]

**Example 48** Find \(\text{lcm}(2^2 \cdot 3^2 \cdot 5, 2 \cdot 3^3 \cdot 7^2)\)

\[
\text{lcm}(2^2 \cdot 3^2 \cdot 5, 2 \cdot 3^3 \cdot 7^2) = 2^2 \cdot 3^3 \cdot 5 \cdot 7^2 = 26460
\]

**Example 49** Find \(\text{lcm}(100, 64)\)

First, write \(100 = 2^2 \cdot 5^2\) and \(64 = 2^6\). Therefore, \(\text{lcm}(100, 64) = 2^6 \cdot 5^2 = 1600\).

1.2.3 Modular Arithmetic

Before we give a formal definition let us look at simple examples we all have done in the past, without being aware we were performing modular arithmetic. Loosely speaking, **modular arithmetic** is a system of arithmetic for integers, where integers wrap around after they reach a certain value, called the **modulus**.

**Example 50** Suppose your electricity was out for 27 hours and all your clocks are off by that amount. Assume you have analogue clocks. To reset your clocks, you could of course, advance them by 27 hours. But you know it would be a waste of time. After you would have advanced it 27 hours, you would be at the same place. Hence, it would have been enough to advance them by 3 hours. Mathematically, this amounts to noticing that \(27 = 24 + 3\).

**Example 51** Suppose you need to know which day of the week will be 23 days from Wednesday. It is not necessary to count 23 days. Knowing that days repeat themselves every 7 days, and the fact that \(23 = 7 \cdot 3 + 2\), we see it is enough to add 2 days to Wednesday and we get Friday.

Thus, in both cases, the answer was obtained by finding the remainder of a division. We can now state a more formal definition

**Definition 52** Let \(a\) and \(n\) be integers. Suppose that when we perform the division algorithm we get \(a = nq + r\) where \(q\) is the quotient and \(r\) the remainder with \(0 \leq r < n\). Then, we write:

\[a \mod n = r\]
we also write
\[ a \equiv r \pmod{n} \]
and read "\( a \) is congruent to \( r \mod{n} \)". We will use the latter notation in the very near future.

**Remark 53** In other words, \( a \mod{n} = r \iff a = nq + r \) for some integer \( q \). Also, \( a \mod{n} \) is the remainder of the division of \( a \) by \( n \).

**Example 54** \( 25 \mod 12 = 1 \) since \( 25 = 12 \times 2 + 1 \).

**Example 55** \( 100 \mod 64 = 36 \) since \( 100 = 64 \times 1 + 36 \).

**Example 56** \( 32 \mod 45 = 0 \) since \( 32 = 45 \times 0 + 32 \).

**Example 57** \( -2 \mod 15 = 13 \) since \( -2 = 15 \times (-1) + 13 \).

In other words, when doing modular arithmetic (\( \mod{n} \)), the following happens. Suppose we start counting from 0. Until we reach \( n - 1 \), it is the same as regular arithmetic. However, with modular arithmetic, \( \mod{n} \), when we reach \( n \), we restart at 0. The table below illustrates this with \( n = 5 \).

<table>
<thead>
<tr>
<th>( i \mod 5 )</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>( i )</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
</tr>
</tbody>
</table>

We see that \( i \mod 5 \) (\( a \mod{n} \) in general) is simply the remainder of the division by 5 (\( n \) in the general case). The same idea applies when we do modular arithmetic. We use normal arithmetic, then apply modular arithmetic to the result. With this in mind, we can define addition and multiplication modulo \( n \) as follows:

**Definition 58 (Addition modulo \( n \))** Let \( a \) and \( b \) be two integers. Addition modulo \( n \) is defined to be regular addition \( \mod{n} \) that is \( (a + b) \mod{n} \). If \( a+b < n \) then \( (a + b) \mod{n} = a + b \). If \( a + b > n \) then \( (a + b) \mod{n} \) is the remainder of the division of \( a + b \) by \( n \).

**Definition 59 (Multiplication modulo \( n \))** This is defined similarly. Let \( a \) and \( b \) be two integers. Multiplication modulo \( n \) is defined to be regular multiplication \( \mod{n} \) that is \( (ab) \mod{n} \). If \( ab < n \) then \( (ab) \mod{n} = ab \). If \( ab > n \) then \( (ab) \mod{n} \) is the remainder of the division of \( ab \) by \( n \).

**Example 60** Suppose that \( n = 5 \). Then

\[
(2 + 1) \mod{5} = 2 + 1 = 3
\]

But

\[
(3 + 4) \mod{5} = 7 \mod{5} = 2
\]
1.2. PROPERTIES OF INTEGERS

Similarly

\[(4 + 1) \text{ mod } 5 = 5 \text{ mod } 5 = 0\]

**Example 61** Suppose that \( n = 7 \). Then,

\[3 \cdot 2 \text{ mod } 7 = 6 \text{ mod } 7 = 6\]

and

\[4 \cdot 3 \text{ mod } 7 = 12 \text{ mod } 7 = 5\]

Here are some properties of modular arithmetic.

**Proposition 62** Suppose that \( a, b, a', b' \) are integers and \( n \) is a positive integer. Then, the following results are true:

1. If \( a \text{ mod } n = a' \) and \( b \text{ mod } n = b' \) then \( (a + b) \text{ mod } n = (a' + b') \text{ mod } n \).
2. If \( a \text{ mod } n = a' \) and \( b \text{ mod } n = b' \) then \( (a - b) \text{ mod } n = (a' - b') \text{ mod } n \).
3. If \( a \text{ mod } n = a' \) and \( b \text{ mod } n = b' \) then \( (ab) \text{ mod } n = (a'b') \text{ mod } n \).
4. \( a \text{ mod } n = b \text{ mod } n \iff n \mid (a - b) \)

**Proof.** See problems ■

1.2.4 Important things to Remember

We list the important results students must know. These results come from the notes and the problems assigned.

- Well Ordering Principle.
- Division algorithm. If \( a \) and \( b \) are integers, \( b > 0 \), then there exist unique integers \( q \) and \( r \) with \( 0 \leq r < b \) such that \( a = bq + r \).
- If \( d = \gcd(a, b) \) then there exists integers \( s \) and \( t \) such that \( d = sa + bt \) and the greatest common divisor of \( a \) and \( b \) is the smallest positive integer of this form.
- \( a \) and \( b \) are relatively prime if and only if there exist integers \( s \) and \( t \) such that \( 1 = as + bt \).
- Fundamental theorem of arithmetic.
- \( p \) prime and \( p \mid ab \) then \( p \mid a \) or \( p \mid b \).
• Properties of modular arithmetic.

• If $a$ and $b$ are positive integers then $ab = \gcd(ab) \lcm(a, b)$.

• If $a$ and $b$ are relatively prime integers which divide another integer $c$ then $ab$ also divides $c$.

• Let $a$ and $n$ be positive integers. $ax \mod n = 1$ has a solution $\iff \gcd(a, n) = 1$.

• $\gcd(a, bc) = 1 \iff \gcd(a, b) = 1$ and $\gcd(a, c) = 1$.

1.2.5 Exercises

1. Prove that if $a = bq + r$ and $k$ is an integer then $k$ divides $a$ and $b$ if and only if $k$ divides $b$ and $r$. Conclude that $\gcd(a, b) = \gcd(b, r)$.

2. Prove that $\gcd(m, 0) = m$.

3. Prove that $\sqrt{p}$ is irrational if $p$ is prime (hint: assume it is not).


5. In your book, at the end of chapter 0, do # 1, 2, 4, 7, 8, 9, 10, 12, 13, 19.