1. Integers

The integers
\[ \mathbb{Z} = \{ \cdots, -3, -2, -1, 0, 1, 2, 3, \cdots \} \]
have addition and multiplication which satisfy familiar rules. They are ordered (\( m < n \) if \( m \) is less than \( n \)). The absolute value \( |n| \) of an integer \( n \) is
\[ |n| = \begin{cases} 
  n & \text{if } n \geq 0 \\
  -n & \text{if } n < 0 
\end{cases} \]

The natural numbers (nonnegative integers) are
\[ \mathbb{N} = \{ n \in \mathbb{Z} \mid n \geq 0 \} \]
The positive integers are
\[ \mathbb{Z}^+ = \{ n \in \mathbb{Z} \mid n \geq 1 \} \]
The integers satisfy the cancellation law of multiplication; that is, if \( a, b, c \) are integers with \( c \neq 0 \), and \( ca = cb \), then \( a = b \).

The integers \( \mathbb{Z} \) are “well ordered”: Suppose that \( S \) is a nonempty subset of \( \mathbb{Z} \) which is bounded from below (there exists \( c \in \mathbb{Z} \) such that \( x \geq c \) for all \( x \in S \)). Then \( S \) has a smallest element.

**Theorem 1.1.** (Principle of Mathematical Induction) Suppose that \( P(n) \) are propositions for \( n \in \mathbb{N} \) such that
1. \( P(0) \) is true and
2. If \( P(n) \) is true for some \( n \in \mathbb{N} \) then \( P(n+1) \) is true.

Then \( P(n) \) is true for all \( n \in \mathbb{N} \).

**Proof.** Let \( S = \{ n \in \mathbb{N} \mid P(n) \text{ is not true} \} \). We must prove that \( S = \emptyset \). Suppose not. Then there exists a smallest element \( m \in S \) (by well ordering of the integers). Since \( P(0) \) is true, \( m > 0 \), so \( m \geq 1 \), and thus \( m - 1 \in \mathbb{N} \). But then \( P(m - 1) \) is true so \( P(m) \) must be true, and thus \( m \not\in S \), a contradiction. Thus \( S = \emptyset \). \( \square \)

A useful variation on this theorem is the following.

**Theorem 1.2.** Suppose that \( c \in \mathbb{Z} \) and \( T = \{ n \in \mathbb{Z} \mid n \geq c \} \). Suppose that \( P(n) \) are propositions for \( n \in T \) such that
1. \( P(c) \) is true and
2. If \( P(n) \) is true for some \( n \in T \) then \( P(n+1) \) is true.

Then \( P(n) \) is true for all \( n \in T \).
From the fact that the integers are ordered and the well ordering axiom we can deduce the following important property of the integers, which is very important in writing proofs:

Suppose that $m, n$ are integers and $n > m$. Then $n \geq m + 1$.

**Theorem 1.3. (Euclidean Division)** Suppose $m, n \in \mathbb{Z}$ with $m > 0$. Then there exists a unique expression $n = qm + r$ with $q, r \in \mathbb{Z}$ and $0 \leq r < m$.

**Proof.** We first prove existence. Let

$$S = \{ n - am \mid a \in \mathbb{Z} \text{ and } n - am \text{ is nonnegative} \}.$$ 

We will establish that $S$ is nonempty. We have that $1 \leq m$ since $m > 0$. Thus $-|n|m \leq -|n| \leq n$, and $n + |n|m \in S$. Thus $S$ is nonempty. $S$ is a nonempty set which is bounded from below, so it has a smallest element, $r$.

We will assume $r \geq m$ and derive a contradiction. We have an expression $r = n - qm$ for some $q \in \mathbb{Z}$.

$$0 \leq r - m < r.$$ 

Thus $r - m \in S$, a contradiction to our assumption that $r$ was the smallest element of $S$. We thus have that $0 \leq r < m$. We have an expression $n = qm + r$ with $0 \leq r < m$.

We now prove uniqueness. Suppose we have expressions $n = qm + r$ with $0 \leq r < m$ and $n = q_1m + r_1$ with $0 \leq r_1 < m$. We will prove that $r = r_1$ and $q = q_1$. If $r = r_1$, then $0 = (q - q_1)m$ and $m \neq 0$ implies $q = q_1$. Suppose $r \neq r_1$. Without loss of generality, we may suppose that $r > r_1$. Since $r_1 \geq 0$ and $r < m$ we have that $r - r_1 < m$. We also have that $0 < r - r_1 = m(q_1 - q)$. Thus $q_1 - q > 0$ and we have $q_1 - q \geq 1$. So $r - r_1 \geq m$, a contradiction. We thus have that $r = r_1$, and $q = q_1$. $\square$

An integer $b$ divides an integer $a$ if $a = cb$ for some integer $c$. Write $b \mid a$ if $b$ divides $a$. We will also say that $a$ is a multiple of $b$.

**Lemma 1.4.** Suppose that $m$, $n$, $q$ are integers. Then:

- a) $1 \mid n$.
- b) $m\mid 0$.
- c) If $m \mid n$ and $n \mid q$ then $m \mid q$.
- d) If $m \mid n$ and $m \mid q$ then $m$ divides $un + vq$ for all integers $u, v$.
- e) If $m \mid 1$ then $m = 1$ or $m = -1$.
- f) If $m \mid n$ and $n \mid m$ then $m = \pm n$.

**Proof of c:** Suppose that $m \mid n$ and $n \mid q$. Then there exist integers $c$ and $d$ such that $n = cm$ and $q = dn$. Thus $q = dcm$. Since $dc$ is an integer, $m$ divides $q$.

**Proof of d:** Suppose that $m \mid n$ and $m \mid q$. Then $n = cm$ and $q = dm$ for some integers $c$ and $d$. Thus, for $u, v \in \mathbb{Z}$, $un + vq = ucm + vdm = (uc + vd)m$, which implies that $m$ divides $un + vq$.

**Definition 1.5.** Suppose that $a, b \in \mathbb{Z}$. A greatest common divisor $c$ of $a$ and $b$ is $c \in \mathbb{Z}$ such that

1. $c > 0$.
2. $c \mid a$ and $c \mid b$.  

2
3. If \(d\) is an integer such that \(d|a\) and \(d|b\) then \(d|c\).

**Theorem 1.6.** Suppose that \(a, b \in \mathbb{Z}\) are not both zero. Then their greatest common divisor \(c\) exists and is unique. Moreover, \(c = m_0a + n_0b\) for suitable integers \(m_0\) and \(n_0\).

**Proof.** We first prove existence. Since \(a, b\) are not both zero,

\[ A = \{ma + nb \mid m, n \in \mathbb{Z}\} \]

has nonzero elements. Further, \(A\) has positive elements, since if \(x \in A\) and \(-x < 0\) then \(-x \in A\). By the well ordering of the integers, there is a smallest positive integer \(c \in A\). We now will show that \(c\) satisfies 1,2 and 3 of the definition of a greatest common divisor. 1 follows since \(c\) is positive. We now establish 3. Suppose that \(d \in \mathbb{Z}\) such that \(d|a\) and \(d|b\). Then \(d\) divides \(c = m_0a + n_0b\) by d) of Lemma 1.4. Now we establish 2. By Euclidean division, \(a = qc + r\) with \(0 \leq r < c\), so that \(a = q(m_0a + n_0b) + r\), which implies

\[ r = -qm_0b + (1 - qn_0)a \in A. \]

Since \(0 \leq r < c\), we have by the minimality of \(c\) in the set of positive elements of \(A\) that \(r = 0\). Thus \(a = qc\) so that \(c|a\). Similarly, \(c|b\).

Thus \(c\) is a greatest common divisor of \(a\) and \(b\).

We now prove uniqueness. Suppose that \(c\) and \(t\) are two integers, both of which are greatest common divisors of \(a\) and \(b\). Then \(c|t\) since \(c\) is a common divisor of \(a\) and \(b\) and \(t\) is a greatest common divisor, and \(t|c\) since \(t\) is a common divisor of \(a\) and \(b\) and \(c\) is a greatest common divisor. Thus \(t = \pm c\) by f) of Lemma 1.4. Since \(c\) and \(t\) are both positive, \(c = t\). □

If \(a, b \in \mathbb{Z}\) are not both zero, write \(\gcd(a, b)\) for the greatest common divisor of \(a\) and \(b\). The proof of Theorem 1.6 shows that:

**Theorem 1.7.** Suppose that \(a, b \in \mathbb{Z}\) are not both zero. Let \(d = \gcd(a, b)\). Then

\[ a\mathbb{Z} + b\mathbb{Z} = \{ma + nb \mid m, n \in \mathbb{Z}\} = \{dl \mid l \in \mathbb{Z}\} = d\mathbb{Z}. \]

**Observation:** If \(a = qb + r\) with \(0 \leq r < b\), then \(\gcd(a, b) = \gcd(b, r)\).

As an example, we compute \(\gcd(91, 196)\), using the “Euclidean Algorithm”.

\[
\gcd(91, 196) = \gcd(196, 91) \\
= \gcd(91, 14) \quad \text{since } 196 = 2 \times 91 + 14 \\
= \gcd(14, 7) \quad \text{since } 91 = 6 \times 14 + 7 \\
= \gcd(7, 0) \quad \text{since } 14 = 2 \times 7 + 0 \\
= 7
\]

We can now work back through the computation to find:

\[
\gcd(91, 196) = 7 = 91 - 6 \times 14 = 91 - 6 \times (-2 \times 91 + 196) = 13 \times 91 - 6 \times 196.
\]

We say that two nonzero integers \(a\) and \(b\) are relatively prime if \(\gcd(a, b) = 1\). Relatively prime integers \(a\) and \(b\) have the following very important property.
Theorem 1.8. Suppose that $a, b \in \mathbb{Z}$ are nonzero and $gcd(a, b) = 1$. Suppose that $c \in \mathbb{Z}$ and $a \mid bc$. Then $a \mid c$.

Proof. By Theorem 1.6, there exist $s, t \in \mathbb{Z}$ such that $1 = sa + tb$. Since $a \mid bc$ by assumption, $bc = qa$ for some $q \in \mathbb{Z}$. We have

$$c = 1c = (sa + tb)c = sac + tbc = a(sc + tq).$$

Thus $a \mid c$. □

Definition 1.9. Suppose that $m$ and $n$ are nonzero integers. The least common multiple of $m$ and $n$ is the smallest positive integer $v$ such that $m \mid v$ and $n \mid v$.

We will write $lcm(m, n)$ for the least common multiple of two nonzero integers $m$ and $n$.

Lemma 1.10. Suppose that $m, n$ are positive integers. Then

1. $gcd(m,n)lcm(m,n) = mn$.
2. If $w \in \mathbb{Z}$ is such that $m \mid w$ and $n \mid w$ then $lcm(m,n) \mid w$.

Definition 1.11. A prime $p$ is an integer $p \geq 2$ such that given a factorization $p = mn$ with positive integers $m, n$, then $m = 1$ or $n = 1$.

Theorem 1.12. Suppose that $p$ is a prime number and $a, b \in \mathbb{Z}$ are such that $p \mid ab$. Then $p \mid a$ or $p \mid b$.

Proof. Assume that $p \not\mid a$. Since $gcd(a, p)$ divides $p$ and $p$ is a prime, we have that $gcd(a, p) = 1$ or $gcd(a, p) = p$. Since $p \not\mid a$, we have $gcd(a, p) = 1$. Now $p \mid b$ by Theorem 1.8. □

We now prove the “fundamental theorem of arithmetic”.

Theorem 1.13. Suppose that $n > 1$ is an integer. Then there is a unique factorization

(1) $n = p_1^{a_1}p_2^{a_2} \cdots p_k^{a_k}$

where $k$ is a positive integer, $p_1 < p_2 < \cdots < p_k$ are primes and $a_1, \ldots, a_k$ are positive integers.

Proof. We first prove the existence of such a factorization for every integer $n > 1$. We assume that the existence of such a factorization is false, and will derive a contradiction. Let $S$ be the set of all integers $n > 1$ for which there is not a factorization (1). By our assumption, $S$ is nonempty. Since $S$ is bounded below, it has a smallest element $m$, by well ordering of the integers. Now $m$ is not a prime, since otherwise it could not be in $S$. Thus $m$ has a positive divisor $a$ which is not 1 and not $m$. We have $m = ab$ for appropriate $b \in \mathbb{Z}$ which is also not 1 and not $m$. We thus have $1 < a < m$ and $1 < b < m$. Since $m$ is the least element of $S$, we must have $a \notin S$ and $b \notin S$. Thus both $a$ and $b$ have factorizations of the form of (1), so that their product $m = ab$ also has a factorization of the form of (1). This gives a contradiction to our assumption that $S$ is nonempty. We conclude that every integer $n > 1$ must have a factorization into products of primes of the form of (1).

Now we prove the uniqueness of the expression (1). We will assume that uniqueness is false, and derive a contradiction. Let $T$ be the set of integers which are greater than 1 and which do not have a unique factorization of the form (1). Since we are assuming that $T$ is nonempty, and $T$ is bounded from below, there is a smallest element $m$ of $T$, by well
ordering of the integers. \( m \) necessarily has two distinct factorizations into primes of the form (1), say
\[
m = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}
\]
and
\[
m = q_1^{b_1} q_2^{b_2} \cdots q_l^{b_l}.
\]
Thus \( p_1 \) divides \( m = q_1^{b_1} \cdots q_l^{b_l} \). By Theorem 1.12, we have that \( p_1 \) divides \( q_1^{b_1} \) or \( p_1 \) divides \( q_2^{b_2} \cdots q_l^{b_l} \). Repeating this argument at most \( l-1 \) times, we conclude that \( p_1 \) divides \( q_i^{b_i} \) for some \( i \). Now we conclude by further application of Theorem 1.12 that \( p_1 | q_i \). Since \( q_i \) is a prime, and \( p_1 > 1 \), we must have that \( p_1 = q_i \). Dividing \( p_1 \) out of the expressions (2) and (3), we have two distinct factorizations
\[
\frac{m}{p_1} = p_2^{a_2-1} p_3^{a_3} \cdots p_k^{a_k} = q_1 q_2^{b_2-1} \cdots q_l^{b_l-1},
\]
so that we either have that \( \frac{m}{p_1} \in T \), which is impossible since \( m > \frac{m}{p_1} \) is the smallest element of \( T \), or \( m = p_1 \). But in this case \( m = q_1 = p_1 \), giving a contradiction to the assumption that the factorizations (2) and (3) are distinct. \( \square \)

**Theorem 1.14.** (Euclid) There are infinitely many primes.

**Proof.** Suppose that the theorem is false. Then there are only finitely many primes, \( p_1, p_2, \ldots, p_m \). Let \( q = p_1 p_2 \cdots p_m + 1 \). Since \( q > p_i \) for \( 1 \leq i \leq m \), \( q \) cannot be a prime. If a prime \( p_i \) divided \( q \), then \( p_i \) would have to divide 1, which is impossible, by e) of Lemma 1.4. Thus \( q \) is an integer which is greater than 1 and is not divisible by a prime. But this is impossible, since \( q \) is divisible by a prime by Theorem 1.13. \( \square \)