Fall 2025

Summary: Integers

1 Well ordering principle and prime factorization

Definition 1.1. *Natural numbers*: $\mathbb{N} = \{0, 1, 2, \ldots\}$ is the set of natural numbers.

Axiom 1.2. *(Well-ordering principle).*
Every nonempty subset of natural numbers has a least element.

Axiom 1.3. *(Induction principle).*
Let $S \subset \mathbb{N}$ be such that (1) $0 \in S$, and (2) $n \in S \Rightarrow n+1 \in S$. Then $S = \mathbb{N}$.

Proposition 1.4. *The well-ordering principle is equivalent to the induction principle.*

Definition 1.5. If $a, b \in \mathbb{Z}$ and $a \neq 0$, we say that a divides b if there exists $c \in Z$ such that $b = a \cdot c$. Notation: $a \mid b$. Then we say that a is a divisor of b.

Definition 1.6. A number $p \in \mathbb{Z}^+$ is called a prime if $p > 1$ and if the only positive divisors of p are 1 and p. Non-prime elements of $\mathbb{Z}^+$ different from 1 are called composite.

Theorem 1.7. *(Fundamental theorem of arithmetic)*

(a) Any integer greater than 1 is a product of primes.

(b) The prime factorization is unique up to the order of factors.

2 Euclidean division and Bezout's identity

Definition 2.1. If $a, b \in \mathbb{Z}^*$, then $d \in \mathbb{Z}^+$ is the greatest common divisor of a and b if (1) $d \mid a$, $d \mid b$, and (2) if $e \mid a$, $e \mid b$, then $e \mid d$. Notation: $\gcd(a, b)$. If $\gcd(a, b) = 1$, we say that a and b are coprime.

Definition 2.2. If $a, b \in \mathbb{Z}^*$, then $l \in \mathbb{Z}^+$ is the least common multiple of a and b if (1) $a \mid l$, $b \mid l$, and (2) if $a \mid m$, $b \mid m$, then $l \mid m$. Notation: $\mathrm{lcm}(a, b)$.

Theorem 2.3. *(Euclidean division) Let $n \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$. There exist two integers $q, r \in \mathbb{Z}$ such that $n = qd + r$, and $0 \leq r < d$. The integers q, r are unique.*

Lemma 2.4. *If $n, q \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$ are such that $n = qd + r$, then $\gcd(n, d) = \gcd(d, r)$.*

Example 2.5. (Euclidean algorithm for finding gcd of two integers). Let $d_1, d_2 \in \mathbb{Z}^+$ and $d_1 > d_2$. To find $\gcd(d_1, d_2)$ we can use the following algorithm.

1. Use Euclidean division to find $0 \leq d_3 < d_2$ such that $d_1 = q_1 d_2 + d_3$. If $d_3 = 0$, then $d_2 = \gcd(d_1, d_2)$.
2. If $d_3 \neq 0$, then find $0 \leq d_4 < d_3$ such that $d_2 = q_2 d_3 + d_4$. If $d_4 = 0$, then $d_3 = \gcd(d_2, d_3) = \gcd(d_1, d_2)$.
3. If $d_4 \neq 0$, continue to find d_5 such that $d_3 = q_3 d_4 + d_5$, and so on. The algorithm terminates after a finite number of steps because $0 \leq \ldots d_5 < d_4 < d_3 < d_2$.

Remark 2.6. Since the divisors of a and $-a$ are the same, one can run the Euclidean algorithm for $|a|, |b|$ to find the $\gcd(a, b)$.

Corollary 2.7. *For any $a, b \in \mathbb{Z}^*$ there exist $x, y \in \mathbb{Z}$ such that*

$$\gcd(a, b) = ax + by.$$

Corollary 2.8. *If $a, b \in \mathbb{Z}^*$ and $d = \gcd(a, b)$, then the equation $ax + by = c$, $c \in \mathbb{Z}$ has integer solutions for x, y if and only if $c \in d\mathbb{Z}$.*

Corollary 2.9. *(Bezout's identity).*
If $a, b \in \mathbb{Z}^*$ are coprime, then there exist $x, y \in \mathbb{Z}$ such that $ax + by = 1$.

Definition 2.10. Euler's totient function $\varphi(n)$ is defined for any positive integer n as the number of positive integers $a \ : \ 1 \leq a \leq n$ such that $\gcd(a, n) = 1$.

Remark 2.11. For two integers n and m such that $\gcd(n, m) = 1$, we have $\varphi(nm) = \varphi(n)\varphi(m)$.