Fall 2024

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.*

Proof: exercise (see lecture 1).

Definition 1.5. $\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$ is the set of integer numbers
$\mathbb{Z}^+ = \{1, 2, \ldots\}$ is the set of positive integers
$\mathbb{Z}^* = \{\pm 1, \pm 2, \ldots\}$ is the set of nonzero integers

Definition 1.6. 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 1.7. 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 1.8. *(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.

Proof:

(a) Exercise. Use the well-ordering principle. Assume there exists a non-empty set A of natural numbers greater than 1 that are not products of primes. Then A contains a least element $m \in A$. Derive a contradiction.

(b) This also uses the well-ordering principle, but requires more work. Suppose $n = p_1 \ldots p_m = q_1 \ldots q_k$ is the smallest positive integer with two different prime factorizations. If $p_i = q_j$ for some i, j, then the number $m = n/p_i = n/q_j$ would be a smaller positive integer with this property, therefore we can assume that all $\{p_1, \ldots p_m\}$ are distinct from all $\{q_1, \ldots q_k\}$. Without loss of generality, suppose that $p_1 < q_1$ and set

$$t = (q_1 - p_1)q_2 \ldots q_k.$$

Then $t > 1$ and $t = q_1 \ldots q_k - p_1 q_2 \ldots q_k = n - p_1 q_2 \ldots q_k$, therefore $t < n$. Then by our assumption t has a unique prime factorization. We have

$$t = q_1 q_2 \ldots q_k - p_1 q_2 \ldots q_k = p_1 p_2 \ldots p_m - p_1 q_2 \ldots q_k = p_1(p_2 \ldots p_m - q_2 \ldots q_k).$$

Therefore p_1 divides $t = (q_1 - p_1)q_2 \ldots q_k$. Since $p_1 \neq q_j$ for all j, we have that p_1 divides $(q_1 - p_1)$. But then $q_1 - p_1 = p_1 s \implies q_1 = p_1(s+1)$ for a positive integer s, but q_1 is a prime. Contradiction.

2 Euclidean division and Bezout's identity

Lemma 2.1. *(Euclid's lemma) If p is a prime and $p \mid (ab)$ for some $a, b \in \mathbb{Z}^+$, then $p \mid a$ or $p \mid b$.*

Proof: exercise (follows directly from the prime factorization).

Definition 2.2. 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 2.3. 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: $\mathrm{lcm}(a, b)$.

Exercise 2.4. *If p is a prime, then $\sqrt{p}$ is irrational.*

Theorem 2.5. *(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.*

Proof: exercise. Consider the set $\{n - kd\}_{k \in \mathbb{Z}} \cap \mathbb{N}$ and use the well-ordering principle to find its least element. Show that it satisfies the conditions for $0 \leq r < d$.

Lemma 2.6. *If $n, q \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$ are such that $n = qd + r$, then $\gcd(n, d) = \gcd(d, r)$.*

Proof: exercise.

Example 2.7. (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 $0 \leq ...d_5 < d_4 < d_3 < d_2$.

Remark 2.8. Since the divisors of a and $-a$ are the same, one can run the Euclidean algorithm for $|a|, |b|$ to find the $\gcd(a, b)$.

Example 2.9. Find $\gcd(123, 87)$.
Let $d_1 = 123$, $d_2 = 87$. We have $123 = 87 + 36$, so $d_3 = 36$. Now $87 = 2 \cdot 36 + 15$, so $d_4 = 15$. Then $36 = 2 \cdot 15 + 6$, so $d_5 = 6$. Then $15 = 2 \cdot 6 + 3$, so $d_6 = 3$. Finally $6 = 2 \cdot 3 + 0$, so the greatest common divisor is $3 = \gcd(15, 6) = \gcd(36, 15) = \gcd(87, 36) = \gcd(123, 87)$.

Corollary 2.10. *For any $a, b \in \mathbb{Z}^*$ there exist $x, y \in \mathbb{Z}$ such that*

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

Proof: Run the Euclidean algorithm backwards.

Exercise 2.11. *Find $x, y \in \mathbb{Z}$ such that $123x + 87y = \gcd(123, 87) = 3$ (see Example 2.9).*

Corollary 2.12. *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 $c \in d\mathbb{Z}$.*

Proof: exercise (see PS1).

Corollary 2.13. *(Bezout's identity).*
If $a, b \in \mathbb{Z}^*$ are coprime, then there exist $x, y \in \mathbb{Z}$ such that $ax + by = 1$.

Proof: the case of $\gcd(a, b) = 1$ in Corollary 2.12

Definition 2.14. 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 $\gcd(a, n) = 1$.

Exercise 2.15. *(a) Show that $\varphi(p) = p - 1$ for any prime p.*

(b) Find $\varphi(18)$ by a direct computation.

(c) Find $\varphi(8)$, $\varphi(9)$ and $\varphi(16)$. Guess the formula for $\varphi(p^k)$ where k is a positive integer, and prove it (see PS2).

Remark 2.16. Later we will prove using ring theory that for any coprime integers n and m, we have $\varphi(nm) = \varphi(n)\varphi(m)$.