Chapter 1

The Integers

Definition 1.1. Let $a, b \in \mathbb{Z}$. We say that 'b divides a', or 'b is a divisor of a', or 'a is a multiple of b', and write $b \mid a$, is an *integer* $c \in \mathbb{Z}$ such that $a = bc$.

Lemma 1.2. *If $b \mid a$ and $a \neq 0$, then $|b| \leq |a|$.*

Fact (Well-ordering Principle)**.** *Every nonempty set of nonnegative integers contains a least element.*

Theorem 1.3 (Division with remainder)**.** *Let $a, b \in \mathbb{Z}$ with $b \neq 0$. Then there exists a unique 'quotient' $q \in \mathbb{Z}$ and a unique 'remainder' $r \in \mathbb{Z}$ such that*

$$a = bq + r \qquad \textit{with } |r| < |b| \,.$$

Definition 1.5. Let $a, b \in \mathbb{Z}$. We say that a nonnegative integer d is the 'greatest common divisor' of a and b, denoted $\gcd(a, b)$ or simply (a, b), if

- $d \mid a$ and $d \mid b$; and
- if $c \mid a$ and c |b, then $c \mid d$.

Theorem 1.8. *Let $a, b \in \mathbb{Z}$. Then the greatest common divisor $d = \gcd(a, b)$ is an integer linear combination of a and b. That is, there exists integers m and n such that $d = ma + nb$.*

In fact, if a and b are not both 0, then $\gcd(a, b)$ is the smallest positive linear combination of a and b.

Corrollary 1.9. *Let $a, b \in \mathbb{Z}$. Then $\gcd(a, b) = 1$ if and only if 1 may be expressed as a linear combination of a and b.*

Definition 1.10. We say that a and b are *relatively prime* if $\gcd(a, b) = 1$.

Corrollary 1.11. *Let $a, b, c \in \mathbb{Z}$. If $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$.*

Theorem 1.14 (Euclidean Algorithm)**.** *Let $a, b, \in \mathbb{Z}$, with $b \neq 0$. Then with notation as above, $\gcd(a, b)$ equals the last nonzero remainder r_n.*
More explicitely: let $r_{-2} = a$ and $r_{-1} = b$; for $i \geq 0$, let r_i be the remainder of the division of r_{i-2} by r_{i-1}. Then there is an integer n such that $r_n \neq 0$ and $rn_{n+1} = 0$, and $\gcd(a, b) = r_n$.

Lemma 1.15. *Let $a, b, q, r \in \mathbb{Z}$, with $b \neq 0$, and assume that $a = bq + r$. Then $\gcd(a, b) = \gcd(b, r)$.*

Definition 1.17. An integer p is 'irreducable' if $p \neq \pm 1$ and the only divisors of p are $\pm 1, \pm p$.
An integer $\neq 0, \neq \pm 1$ is 'reducible' or 'composite' if it is not irreducable.

Lemma 1.18. *Assume that p is an irreducible integer and that b is not a multiple of p. Then b and p are relatively prime, that is, $\gcd(p, b) = 1$.*

Definition 1.19. An integer p is 'prime' if $p \neq \pm 1$ and whenver p divides the product bc of two integers b, c, then $p \mid b$ or $p \mid c$.

Theorem 1.21. *Let $p \in \mathbb{Z}, p \neq 0$. Then p is prime if and only if it is irreducable.*

Theorem 1.22 (Fundamental Theorem of Arithmetic)**.** *Every integer $n \neq 0, \neq \pm 1$ is a product of finitely many irredicubile integers: $\forall n \in \mathbb{Z}, n \neq 0, n \neq \pm 1$, there exists irreducible integers $q_1, \ldots, q_r$ such that*

$$n = q_1 \cdots q_r,$$

$$n = \prod_r q_r.$$

Further, this factorization is unique in the sense that if

$$n = q_1 \cdots q_r = p_1 \cdots p_s,$$

with all q_i, p_j irreducible, then necessarily $s = r$ and after reordering the factors we have $p_1 = \pm q_1, p_2 = \pm q_2, \ldots, p_r = \pm q_r$.

Proposition 1.25. *Let $a, b \in \mathbb{Z}^{\neq 0}$, and write*

$$a = \pm 2^{\alpha_2} 3^{\alpha_3} 5^{\alpha_5} 7^{\alpha_7} 11^{\alpha_{11}} \cdots,$$

$$b = \pm 2^{\beta_2} 3^{\beta_3} 5^{\beta_5} 7^{\beta_7} 11^{\beta_{11}} \cdots,$$

as above. Then the gcd *of a and b is the positive integer*

$$d = 2^{\delta_2} 3^{\delta_3} 5^{\delta_5} 7^{\delta_7} 11^{\delta_1 1} \cdots,$$

where $\delta_i = \min(\alpha_i, \beta_i)$ for all i.

Corrollary 1.27. *Two nonzero integers a, b are relatively prime if and only if they have no common irreducible factor.*

Chapter 2

Modular Arithmetic

Definition 2.1. Let $n \geq 0$ be an integer, and let $a, b \in \mathbb{Z}$. We say that 'a is congruent to b modulo n', denoted $a \equiv b \mod n$, if $b - a \in n\mathbb{Z}$.