LECTURE 1. DIVISIBILITY OF INTEGERS

Please consider every proposition in this text as an exercise.

1. The Fundamental Theorem of Arithmetic

Definition 1.1. For $m, n \in \mathbb{Z}$, $n \neq 0$, we will say that n divides m if $\exists k \in \mathbb{Z}$ such that $m = kn$. In this case, we will write $n|m$. The number n is called a divisor of m. If n does not divide m, we will write $n \not| m$.

Proposition 1.2. *If $p|q$ and $q|r$, then $p|r$.*

Proposition 1.3. *If $p|q$ and $q|p$, then $p = q$ or $p = -q$.*

Proposition 1.4. *If $p|q$ and $p|r$, then $p|(qx + ry)$, $\forall x, y \in \mathbb{Z}$.*

Proposition 1.5. *For all $m, n \in \mathbb{Z} \setminus \{0\}$ there exist unique $q, r \in \mathbb{Z}$ such that*

$$m = qn + r \text{ and } 0 \leq r \leq |n| - 1. \tag{1.1}$$

The number r is called the remainder and the number q is called the quotient.

Definition 1.6. For arbitrary $m, n \in \mathbb{Z} \setminus \{0\}$ define the greatest common divisor of m and n by the following formula:

$$\mathrm{GCD(m, n)} := \max\{k \in \mathbb{Z}_+ \mid k|m, k|n\} \tag{1.2}$$

Definition 1.7. For arbitrary $m, n \in \mathbb{Z} \setminus \{0\}$ define the least common multiple of m and n by the following formula:

$$\mathrm{LCM(m, n)} := \min\{k \in \mathbb{Z}_+ \mid m|k, n|k\} \tag{1.3}$$

Proposition 1.8. *Suppose that $m, n, k \in \mathbb{Z} \setminus \{0\}$, $m|k$ and $n|k$. Then*

$$\mathrm{LCM(m, n)|k}. \tag{1.4}$$

Proposition 1.9 (Bézout's identity)**.** *For all $m, n \in \mathbb{Z} \setminus \{0\}$ there exist $x, y \in \mathbb{Z}$ such that*

$$\mathrm{GCD(m, n) = mx + ny}. \tag{1.5}$$

Proposition 1.10. *Suppose that $k, m, n \in \mathbb{Z} \setminus \{0\}$, $\mathrm{GCD(k, m)} = 1$ and $k|(mn)$. Then $k|n$.*

Proposition 1.11. *Suppose that $m, n, k \in \mathbb{Z} \setminus \{0\}$, $k|m$ and $k|n$. Then*

$$k|\mathrm{GCD(m, n)}. \tag{1.6}$$

Definition 1.12. A number $p \in \mathbb{Z}_+$ is called prime if $p > 1$ and its only positive divisors are 1 and p. A number $q \in \mathbb{Z}_+$ is called composite if $q > 1$ and q is not prime.

Date: February 6, 2026.

Proposition 1.13 (The Fundamental Theorem of Arithmetic)**.** *Every integer $n > 1$ can be factored as a product of primes: there exist a positive integer k, prime numbers*

$$p_1 < p_2 < \cdots < p_k, \tag{1.7}$$

and positive integers $s_1, s_2, \ldots, s_k$ such that

$$n = \prod_{j=1}^{k} p_j^{s_j}. \tag{1.8}$$

Such representation is unique.

Proposition 1.14. *The set of all prime numbers is infinite.*

Proposition 1.15. *For every $m, n \in \mathbb{Z}_+$ we have the equality*

$$\mathrm{GCD(m, n)} \cdot \mathrm{LCM(m, n)} = \mathrm{mn}. \tag{1.9}$$

2. The Integers Modulo n

Definition 2.1. Let $n \in \mathbb{Z}_+$. Define a binary relation $\sim$ on $\mathbb{Z}$ by

$$(k \sim m) \iff (n|(k-m)). \tag{2.1}$$

This is an equivalence relation. Denote by $\mathbb{Z}_n$ the corresponding set of equivalence classes. If $k \sim m$, we will write $k \equiv m \pmod{n}$.

Proposition 2.2. *Let $n \in \mathbb{Z}_+$. Denote by $p : \mathbb{Z} \to \mathbb{Z}_n$ the canonical projection of $\mathbb{Z}$ to the set of equivalence classes $\mathbb{Z}_n$, by $p \times p : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}_n \times \mathbb{Z}_n$ the map given by*

$$(p \times p)(k, m) := (p(k), p(m)), \tag{2.2}$$

and by $sum : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ the addition operation in $\mathbb{Z}$:

$$sum(k, m) := k + m. \tag{2.3}$$

Then there exists a unique map $sum' : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ such that

$$sum' \circ (p \times p) = p \circ sum. \tag{2.4}$$

$$\begin{array}{ccc} \mathbb{Z} \times \mathbb{Z} & \xrightarrow{sum} & \mathbb{Z} \\ \downarrow{\scriptstyle p \times p} & & \downarrow{\scriptstyle p} \\ \mathbb{Z}_n \times \mathbb{Z}_n & \xrightarrow{sum'} & \mathbb{Z}_n \end{array} \tag{2.5}$$

The map sum' is called addition in $\mathbb{Z}_n$.

Proposition 2.3. *Let $n \in \mathbb{Z}_+$. Denote by $p : \mathbb{Z} \to \mathbb{Z}_n$ the canonical projection of $\mathbb{Z}$ to the set of equivalence classes $\mathbb{Z}_n$, by $p \times p : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}_n \times \mathbb{Z}_n$ the map given by*

$$(p \times p)(k, m) := (p(k), p(m)), \tag{2.6}$$

and by $mult : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ the multiplication operation in $\mathbb{Z}$:

$$mult(k, m) := km. \tag{2.7}$$

Then there exists a unique map $mult' : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ such that

$$mult' \circ (p \times p) = p \circ mult. \tag{2.8}$$

$$\begin{array}{ccc} \mathbb{Z} \times \mathbb{Z} & \xrightarrow{mult} & \mathbb{Z} \\ \downarrow{\scriptstyle p \times p} & & \downarrow{\scriptstyle p} \\ \mathbb{Z}_n \times \mathbb{Z}_n & \xrightarrow{mult'} & \mathbb{Z}_n \end{array} \tag{2.9}$$

The map $mult'$ is called multiplication in $\mathbb{Z}_n$.

Relevant textbook chapters:

- Dummit, Foote, Sections 0.2, 0.3;
- Allenby, Sections 1.3-1.5;
- Gallian, pp. 1-10;
- Pinter, Chapters 21, 22.