Contents

Preface

Chapter 1

The integers

1.1 What are the integers?

Definition 1.1.1. The **integers** are a set $\mathbb{Z}$ of elements

$$\ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots$$

that have the usual operations[*] of $+$ and $\times$, the usual relation[†] $<$, and that satisfy the following properties, for all $a, b, c \in \mathbb{Z}$:

Z1. $a + (b + c) = (a + b) + c$,

Z2. $a + b = b + a$,

Z3. $0 + a = a + 0 = a$,

Z4. $-a \in \mathbb{Z}$ and $a + (-a) = 0$,

Z5. $a \times (b \times c) = (a \times b) \times c$,

Z6. $a \times b = b \times a$

Z7. $a \times 1 = a$

Z8. $a \times (b + c) = (a \times b) + (a \times c)$

Z9. if $a < b$ then $a + c < b + c$,

Z10. if $0 < a$ and $0 < b$ then $0 < ab$.

Z11. **Well-Ordering Axiom** If S is a nonempty subset of positive integers, and every element of S is ≥ 0, then S contains a smallest element.

[*] If we wanted to define the integers more formally, we would use a more precise statement of what "+" and "×" are.

[†] If we were being more formal, we'd list the hidden assumptions that we're making about "$<$": that it is total, meaning given any two integers we can say that one is smaller than the other, and that it is transitive, meaning that if $a < b$ and $b < c$ then $a < c$.

Theorem 1.1.2. *The following properties hold for any $a, b, c \in \mathbb{Z}$:*

(a) *If $a + b = a + c$ then $b = c$.*

(b) $0 \times a = a \times 0 = 0$.

(c) $-(-a) = a$.

(d) $a \times (-b) = (-a) \times b = -(a \times b)$.

(e) $(-a) \times (-b) = a \times b$.

(f) $a \times (b - c) = a \times b - a \times c$.

(g) *If $a \times b = a \times c$, and $a \neq 0$, then $b = c$.*

(h) *If $a < b$ and $0 < c$ then $ac < bc$.*

(i) *If $a \neq 0$ and $a \times b = a \times c$ then $b = c$.*

(j) $-a = -1 \times a$.

(k) $1 > 0$.

(l) *If $a < b$, and $c < 0$ then $a \times c > b \times c$.*

(m) *If $a < 0$ and $b > 0$ then $a \times b < 0$. If $a < 0$ and $b < 0$ then $a \times b > 0$.*

(n) *There does not exist $d \in \mathbb{Z}$ satisfying $a < d < a + 1$.*

(o) *There exists some $n \in \mathbb{Z}$ such that $n \times b > a$.*

Theorem 1.1.3 (Division algorithm)**.** *Let $a, b \in \mathbb{Z}$ with $b > 0$. There exist unique elements $q, r \in \mathbb{Z}$ such that $a = qb + r$ with $0 \leq r < b$.*

This is where we ended on Wednesday, September 3

1.2 Divisibility

Definition 1.2.1. Let $a, b \in \mathbb{Z}$. We say that a **divides** b if $b = ac$ for some $c \in Z$. We write this as $a|b$. Synonyms are "b is divisible by a", "b is a multiple of a", "a is a factor of b", etc.

This is where we ended on Monday, September 8

Definition 1.2.2. Let $a, b \in \mathbb{Z}$, not both 0. A **common divisor** of a and b is a number that divides a and divides b. We say that $d \in \mathbb{Z}$ is a **greatest common divisor** of a and b if d is a common divisor of a and b and d is $\geq$ any other common divisor of a and b. If $\gcd(a, b) = 1$ then we say that a and b are **relatively prime**.

Theorem 1.2.3 (GCD equals $\mathbb{Z}$-linear combination)**.** *Let $a, b \in \mathbb{Z}$, not both 0. Then*

$$\gcd(a, b) = na + mb$$

where (1) $n, m \in \mathbb{Z}$, (2) $na + mb \geq 0$, and (3) $na + mb$ is the smallest number satisfying (1) and (2). In other words, $\gcd(a, b)$ is the smallest positive $\mathbb{Z}$-linear combination of a and b.

This is where we ended on Wednesday, September 10

Theorem 1.2.4. *If $a|bc$ and $\gcd(a, b) = 1$, then $a|c$.*

1.3 Unique factorization and the integers

Definition 1.3.1. Let $p \in \mathbb{Z}$ with $p \neq 0, \pm 1$. We say that p is **prime** if the only integers that divide p are ± 1 and $\pm p$.

Definition 1.3.2. Let $n \in \mathbb{Z}$. We say that n is a product of primes if (1) n is prime or (2) $n = p_1 \dots p_r$ for some primes $p_1, \dots, p_r$.

Theorem 1.3.3 (Fundamental Theorem of Arithmetic I: Existence of factorization)**.** *Let $n \in \mathbb{Z}$ with $n \neq 0, \pm 1$. Then we can write n as a product of primes.*

Theorem 1.3.4 (Euclid's Lemma)**.** *Let $p \in \mathbb{Z}$ with $p \neq 0, \pm 1$. Then p is prime if and only if it satisfies this property:*

$$\forall a, b \in \mathbb{Z}, \text{ if } p|ab \text{ then } p|a \text{ or } p|b \qquad (*)$$

Theorem 1.3.5 (Fundamental Theorem of Arithmetic II: Uniqueness of factorization)**.** *Let $n \in \mathbb{Z}$, $n \neq 0, \pm 1$. Then the prime factorization given by Theorem 1.3.3 is unique. In other words, if*

$$n = p_1 \cdots p_r = q_1 \cdots q_s$$

where each p_i and each q_i is a prime, then $r = s$ and, if necessary, we may rearrange the factors on one side, so that $p_i = \pm q_i$ for each i.

1.3.1 Applications

Definition 1.3.6. The **prime cipher** encrypts text as follows:

- Encode letters as prime numbers as follows:

a=2	e=11	i=23	m=41	q=59	u=73	y=97
b=3	f=13	j=29	n=43	r=61	v=79	z=101
c=5	g=17	k=31	o=47	s=67	w=83	
d=7	h=19	l=37	p=53	t=71	x=89	

- Take a message in plain text, remove the spaces, break the letters up into blocks of 3, or as long as possible without including a repeated letter.
- For each block of text replace each letter with it's prime, and raise the prime to the n power where n is the position of the letter within the block.
- For each block, multiply the primes, including their powers, together. The resulting number is the encrypted version of the block, and the list of all blocks is the encrypted version of the message.
- To decrypt you factor each block, put each prime in the correct position using the power, and then turn the primes back into letters.

This is where we ended on Monday, September 15

Chapter 2

Congruence in $\mathbb{Z}$ and Modular Arithmetic

2.1 Congruence and Congruence Classes

Definition 2.1.1. Let $n \in \mathbb{Z}$, $n \geq 2$. For all $a, b \in \mathbb{Z}$, if $n|(a-b)$ then we write $a \equiv b \pmod{n}$ and we say that a is **congruent** to b modulo n. If the value of n is clear in context, then we will write just $a \equiv b$, dropping "$(\text{mod } n)$".

Theorem 2.1.2 (Congruence is an Equivalence Relation)**.** *Let $n \in \mathbb{Z}$, $n \geq 1$. The relation $a \equiv b \pmod{n}$ is an equivalence relation. In other words, $\forall a, b, c \in \mathbb{Z}$, we have the following:*

1. $a \equiv a \pmod{n}$ *(reflexive property),*
2. *if $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$ (symmetric property),*
3. *if $a \equiv b \pmod{n}$, and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$ (transitive property).*

Theorem 2.1.3. *Let $n \in \mathbb{Z}$ with $n \geq 1$. Let $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then the following hold:*

1. $a + c \equiv b + d \pmod{n}$*,*
2. $ac \equiv bd \pmod{n}$.

Definition 2.1.4. Let $n \in \mathbb{Z}$, $n \geq 1$. Given any $b \in \mathbb{Z}$ we define

$$[b] = \{a \in \mathbb{Z} \mid a \equiv b \pmod{n}\}.$$

For example, we have

$$\begin{aligned} [-2] &= \{a \in \mathbb{Z} \mid a \equiv -2 \pmod{n}\} \\ [0] &= \{a \in \mathbb{Z} \mid a \equiv 0 \pmod{n}\} \\ [3] &= \{a \in \mathbb{Z} \mid a \equiv 3 \pmod{n}\} \end{aligned}$$

In other words, $[b]$ is the set of all integers that are congruent to b modulo n. We call this set the **congruence class of b modulo n**.

Theorem 2.1.5. *Let $n \in \mathbb{Z}$, $n \geq 1$. For all $a, b \in \mathbb{Z}$ we have*

$$[a] = [b] \quad \textit{if and only if} \quad a \equiv b \pmod{n}.$$

This is where we ended on Monday, September 22

Definition 2.1.6. The set of all equivalence classes modulo n is denoted by $\mathbb{Z}_n$.

2.2 Modular Arithmetic

This is where we ended on Wednesday, September 24

Theorem 2.2.1. *Let $n \in \mathbb{Z}$, $n \geq 1$. Let A and C be equivalence classes in $\mathbb{Z}_n$. Let $a, b \in A$ and $c, d \in C$. Then*

$$[a + c] = [b + d] \textit{ and } [ac] = [bd].$$

In other words, it doesn't matter which elements we use in A and C to define addition and multiplicaiton.

Definition 2.2.2. Let $n \in \mathbb{Z}$, $n \geq 1$. Let $\mathbb{Z}_n$ be the collection of all equivalence classes of integers modulo n. The **canonical representatives** of $\mathbb{Z}_n$ are as follows:

$$\mathbb{Z}_n = \Big\{ [0], [1], \ldots, [n{-}1] \Big\}.$$

We define addition and multiplication in $\mathbb{Z}_n$ as follows:

$$[a] \oplus [c] = [a + c] \text{ and } [a] \odot [c] = [ac].$$

Theorem 2.2.3. *For all $[a]$, $[b]$, $[c]$ in $\mathbb{Z}_n$ the following hold:*

Zn 1. $[a] \oplus (b \oplus c) = ([a] \oplus b) \oplus c$,

Zn 2. $[a] \oplus b = b \oplus [a]$,

Zn 3. $[0] \oplus [a] = [a] \oplus [0] = [a]$,

Zn 4. $[a] \oplus [-a] = 0$,

Zn 5. $[a] \odot ([b] \odot [c]) = ([a] \odot [b]) \odot [c]$,

Zn 6. $[a] \odot [b] = [b] \odot [a]$

Zn 7. $[a] \odot [1] = [a]$

Zn 8. $[a] \odot ([b] \oplus [c]) = ([a] \odot [b]) \oplus ([a] \odot [c])$

Definition 2.2.4. Let $[a] \in \mathbb{Z}_n$ and let $k \in \mathbb{N}$. We define

$$k[a] = [a] \oplus \cdots \oplus [a] \text{ (repeated } k \text{ times)}$$
$$[a]^k = [a] \odot \cdots \odot [a] \text{ (repeated } k \text{ times)}$$

This is where we ended on Friday, September 26

2.3 The structure of $\mathbb{Z}_p$ and $\mathbb{Z}_n$

Definition 2.3.1. We define new notation for the elements of $\mathbb{Z}_n$:

$$\begin{aligned} \text{old notation: } & [0], [1], [a], \text{ etc.} \\ \text{new notation: } & 0, 1, a \end{aligned}$$

and addition and multiplcation:

$$\begin{aligned} \text{old notation: } & 1 \oplus 2, a \oplus b, 1 \odot 2, a \odot b, \text{ etc.} \\ \text{new notation: } & 1 + 2, a + b, 1 \cdot 2 \text{ or } 1 \times 2, ab, \text{ etc.} \end{aligned}$$

and even for equivalence:

$$\begin{aligned} \text{old notation: } & 2 + 5 \equiv 3 \pmod 4 \\ \text{new notation: } & 2 + 5 = 3. \end{aligned}$$

The new notation has the advantage that there's a lot less to write, and things look more similar to what we are used to with algebra in $\mathbb{Z}$ and $\mathbb{R}$. It has the disadvantage that we have to remember that we're not working over $\mathbb{Z}$ anymore, even though it looks like we are.

Definition 2.3.2. Let $a \in \mathbb{Z}_n$. If $ax = 1$ has a solution we call a a **unit**. If $ax = 0$ has a solution with $a \neq 0$ and $x \neq 0$ we call a a **zero divisor**

Theorem 2.3.3 ($\mathbb{Z}_p$ has only units, and no zero divisors)**.** *Let $p \in \mathbb{Z}$, $p > 1$ (we do not assume that p is prime). The following statements are equivalent:*

1. *p is prime,*

2. *for any $a \in \mathbb{Z}_p$, if $a \neq 0$ then the equation $ax = 1$ has a solution $x \in \mathbb{Z}_p$,*

3. *for all* $a, b \in \mathbb{Z}_p$, *if* $ab = 0$ *then* $a = 0$ *or* $b = 0$.

Theorem 2.3.4 (Classifying units and zero divisors in $\mathbb{Z}_n$). *Let* $a \in \mathbb{Z}_n$, *with* $a \neq 0$.

1. $ax = 1$ *has a solution* $x \in \mathbb{Z}_n$ *if and only if* $\gcd(a, n) = 1$.
2. $ax = 0$ *has a nonzero solution* $x \in \mathbb{Z}_n$ *if and only if* $\gcd(a, n) \neq 1$.