Contents

1 preface **3**
1.1 Aim . . . 3
1.2 Ref . . . 3

2 **5**
2.1 . . . 5

I The integers $\mathbb{Z}$ **7**
2.2 Addition: . . . 9
2.3 multiplication . . . 9

3 The fundamental theorem of arithmetic **11**
3.1 Def . . . 11
3.2 Theorem: The division algorithm . . . 11
3.3 Def . . . 12
3.4 Corollary of 3.2 . . . 12
3.5 Def . . . 12
3.6 Euclid's Lemma . . . 12
3.7 The fundamental theorem of arithmetic . . . 13
3.8 Corollary . . . 13

4 Congruence in $\mathbb{Z}$ **15**
4.1 Def . . . 15
4.2 Lemma . . . 16
4.3 Remark . . . 16
4.4 Theorem(The structure of $\mathbb{Z}/n\mathbb{Z}$, p prime) . . . 16

Chapter 1

preface

1.1 Aim

- abstract algebraic structures on math objects.
- Basic language of modern math.

1.2 Ref

- Dummit & Foote: Abstract algebra, 3rd edition.
- 聂灵沼 & 丁石孙: 代数学引论 (第二版)

Chapter 2

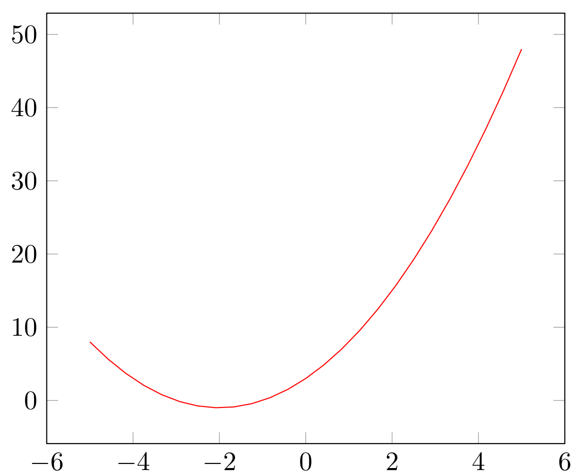
2.1

for an equation:

$$x^2 + 4x + 3 = 0$$

Analysis $x^2 + 4x + 3 = 0 \Rightarrow (x+3)(x+1) = 0 \Rightarrow x = -1$ or $x = -3$

Algebra Vary the coefficients, consider $ax^2 + bx + c = 0$ general solution is $x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$

Geometry 

For the analysis, we solve the problem itself, for algebra,, we abstract the problem (using abstract def and notations) and for geometry, we care about the graph and shapes.

Part I

The integers $\mathbb{Z}$

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \cdots\}$$

There are two binary operations: addition and multiplication.

2.2 Addition:

$\exists!$(exists uniquely) $0 \in \mathbb{Z}$ such that

$$n + 0 = n$$

$\forall n, \exists -n \in \mathbb{Z}$ s.t. $n + (-n) = 0$
and

$$n + m = m + n$$

2.3 multiplication

$\exists! 1 \in \mathbb{Z}$ s.t.

$$n \cdot 1 = n$$

and

$$m \cdot n = n \cdot m \quad \forall m, n \in \mathbb{Z}$$

Only ± 1 have multiplication inverses.

Chapter 3

The fundamental theorem of arithmetic

3.1 Def

For $a, b \in \mathbb{Z}$ a divides b (written as $a \mid b$) if

$$\exists c \text{ s.t } b = ac$$

3.2 Theorem: The division algorithm

Let $a, b \in \mathbb{Z}$ with $b > 0$. Then $\exists!(q, r) \in \mathbb{Z}^2$ such that

$$a = b \cdot q + r \text{ and } 0 \leq r < b$$

Proof

Let $S = \{a - bk \mid k \in \mathbb{Z}, a - bk \geq 0\} \subseteq \mathbb{N}$ If $0 \in S$ then $b \mid a$, then $q = \frac{a}{b}, r = 0$ Now assume $0 \notin S (\Rightarrow a \neq 0)$. Since $S \neq \varnothing$, by well ordering principle of $\mathbb{N}$, we have a smallest number, say $r = a - bq > 0$. It remains to show $r < b$. If $r \geq b$

$$a - b(q+1) = a - bq - b = r - b \geq 0$$

and

$$a - b(q+1) = r - b < r$$

contradiction.

For uniqueness, assume $a = bq + r$ and $a = bq' + r'$. Suppose $r' \geq r$ then

$$bq + r = a = bq' \;\Rightarrow\; b(q - q') = r' - r \geq 0$$

$\Rightarrow b \mid r' - r$ and $0 \leq r' - r \leq r' < b$, thus we have

$$r' - r = 0$$

so as $q = q'$

3.3 Def

- $\gcd(a, b)$ is the greatest common divisor of a and b
- If $\gcd(a, b) = 1$ then we say a and b are relative prime or coprime.

3.4 Corollary of 3.2

Let $a, b \in \mathbb{Z}$ no both zero, and let $c = \gcd(a, b)$. Then $\exists (xx, y) \in \mathbb{Z}^2$ such that $ax + by = c$

Proof

Let $S = \{ax + by \mid (x, y) \in \mathbb{Z}^2\} \cap \mathbb{Z}_{>0} \neq \varnothing$. Let $d = \min S$. We claim that

$$d = c = \gcd(a, b)$$

First note that $c \mid a \& c \mid b \Rightarrow c \mid ax + by \quad \forall x, y \in \mathbb{Z} \Rightarrow c \mid d$. With division algorithm, we write

$$a = dq + r \qquad = \leq r < d$$

Note that $r \in S$ Hence $r = 0$ i.e. $d \mid a$ similarly $d \mid b \Rightarrow d \mid c$ They are positive hence $d = c$

3.5 Def

For $a \in \mathbb{Z} \setminus \{0, \pm 1\}$

- a is called **irreducible** in $\mathbb{Z}$, if $\forall$ factorization $a = bc$, we have

$$b \in \pm 1 \text{ or } c \in \pm 1$$

- a is called **prime** in $\mathbb{Z}$, if $a \mid bc \Rightarrow a \mid b$ or $a \mid c$

3.6 Euclid's Lemma

In $\mathbb{Z}$, irreducible $\Leftrightarrow$ prime.

Proof

$\subseteq$

Assume a is irreducible and $a \mid bc$. Without loss of generality(WLOG), we assume $a > 0$ and $a \not| b$. We show $a \mid c$ in the following way:

$$\left.\begin{aligned} a\text{irreducible} \\ a > 0 \\ a \not| b \end{aligned}\right\} \Rightarrow gcd(a,b) = 1$$

$$\begin{aligned} &\overset{3.4}{\Rightarrow} \exists x, y \in \mathbb{Z} s.t. ax + by = 1 \\ &\Rightarrow c = acx + acy = a(cx + \frac{bc}{a}y) \\ &\Rightarrow a \mid c \end{aligned}$$

$\supseteq$

Assume a is prime and $a = bc$. WLOG, assume that $a \mid b$, then

$$|b| \overset{a=bc}{=} \text{gcd}(a,b) \overset{a|b}{=} |a| \Rightarrow c = \pm 1$$

3.7 The fundamental theorem of arithmetic

$\forall n \in \mathbb{Z}_{\geq 2}$ is a product of positive primes. This prime factorization is unique in the following sense:

- if $n = p_1 \cdots p_s$ and $n = q_1 \cdots q_t$ with p_i, q_j are primes. Then $s = t$ and after reordering and relabeling, $p_i = q_i \forall i$

Proof

For existence, using induction on n. For $n = 2$, 2 is prime. Assume that the prime factorization exists for any integer k that $k < n$

If n is prime, done. If n not a prime, using Euclid's lemma 3.6, $n = bc$ with $1 < b < n, 1 < c < n$ By induction hypothesis, n is also a product of primes.

For uniqueness, using induction on $l = \max\{s,t\}$ If $l = 1$, $n = p_1 = q_1$. If $p_s \mid q_1 \cdots q_t \Rightarrow \exists i$ s.t. $p_s \mid q_i$ But q_i is prime, so $p_s = p_i$. Reindex and we may assume $p_s = q_t$. Cancel p_s with q_t we get

$$p_1 \cdots p_{s-1} = q_1 \cdots q_{t-1}$$

. By induction hypothesis, $s - 1 = t - 1$ and after reindex, $p_i = q_i \forall i$

3.8 Corollary

$\forall n \in \mathbb{Z} \setminus \{0, \pm 1\}$, $n = \pm p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ with p_i are primes and $\alpha_i \in \mathbb{Z}_{\geq 0}$

Chapter 4

Congruence in $\mathbb{Z}$

4.1 Def

Let $a, b, n \in \mathbb{Z}$ with $n > 0$ a is **congruent** ot b **modulo** n, written as

$$a \equiv b \mod n$$

if $n \mid a - b$

Remark

- It is an equivalence relation.
- Reflexive: $a \equiv a \mod n$
- Symmetric: $a \equiv b \mod n \Rightarrow b \equiv a \mod n$
- Transitive: $a \equiv b \mod n \& b \equiv c \mod n \Rightarrow a \equiv c \mod n$
- $$\begin{matrix} a \equiv b \mod n \\ c \equiv d \mod n \end{matrix} \Rightarrow \begin{matrix} a + c \equiv b + d \mod n \\ ac \equiv bd \mod n \end{matrix}$$

So we can have congruence class modulo n:

$$[a]_n := \{b \in \mathbb{Z} \mid b \equiv a \mod n\} = a + n\mathbb{Z}$$

They are only n disjoint congruence class modulo n:

$$[0]_n, \cdots, [n-1]_n$$

The set of congruence classes modulo n is denoted as $\mathbb{Z}/n\mathbb{Z}$

4.2 Lemma

If $[a]_n = [i]_n, [b]_n = [j]_n$ thenn

$$[a+b]_n = [i+j]_n \quad [ab]_n = [ij]_n \quad [a-b]_n = [i-j]_n$$

Therefore, we define the following binary operations on $\mathbb{Z}/n\mathbb{Z}$:

$$[i]_n + [j]_n := [i+j]_n$$
$$[i]_n \cdot [j]_n := [ij]_n$$

We have addition and multiplication satisfying associativity law, distribution law, additive inverse.

4.3 Remark

In $\mathbb{Z}$, if a, b are non-zero, then $ab \neq 0$. But in $\mathbb{Z}/n\mathbb{Z}$, $[a]_n[b]_n = [0]_n$ if $n \mid ab$. In $\mathbb{Z}$ for $2x = 1$ it have no solution. But in $\mathbb{Z}/3\mathbb{Z}$,$[2]_3 x = [1]_3 \Rightarrow x = [2]_3$

4.4 Theorem(The structure of $\mathbb{Z}/n\mathbb{Z}$, p prime)

For $p \in \mathbb{Z}_{\geq 2}$. The following are equivalent(TFAE):

1 p is prime

2 $\forall a \neq 0$ in $\mathbb{Z}/p\mathbb{Z}$, $ax = 1$ has a solution in $\mathbb{Z}/p\mathbb{Z}$

3 whenever $bc = 0$ in $\mathbb{Z}/p\mathbb{Z}$, $b = 0$ or $c = 0$

Proof

$1 \Rightarrow 2$

$0 \neq [a]_p \Rightarrow p \neq a$ so $\gcd(a, p) = 1$ then $\exists (x, y) \in \mathbb{Z}$ s.t. $ax + py = 1$. So moduloing p we get $ax \equiv 1 \mod p$. then $ax = 1$ in $\mathbb{Z}/p\mathbb{Z}$ has a solution

$2 \Rightarrow 3$

Suppose $bc = 0$ in $\mathbb{Z}/p\mathbb{Z}$, WLOG, we assume $b \neq 0$ in $\mathbb{Z}/p\mathbb{Z}$, $\exists \in \mathbb{Z}/p\mathbb{Z}$ s.t. $xb = 1$.

$$\Rightarrow c = c \cdot 1 = xbc = 0$$

$3 \Rightarrow 1$

$bc = 0$ in $\mathbb{Z}/p\mathbb{Z} \Rightarrow p \mid bc$ Hence it follows from the define of prime.