Chapter 5 Very Elementary Number Theory

Su

北京邮电大学

2023 年 10 月 11 日

Contents

Introduction

Introduction

What is the Number theory?

Introduction

What is the Number theory?

- *Number theory is the branch of mathematics concerned with the integers and its related algebraic and geometric objects.*

5.1 Factoring Integers

5.1 Factoring Integers

5.1 Factoring Integers

- *In this section, we will recall some basic terminologies and properties of* $\mathbb{Z}$.

5.1 Factoring Integers

- *In this section, we will recall some basic terminologies and properties of* $\mathbb{Z}$.

Definition. *We say that*

5.1 Factoring Integers

- *In this section, we will recall some basic terminologies and properties of* $\mathbb{Z}$.

Definition. *We say that*

- d *divides(整除)* n *if there exists an integer* q *satisfying* $n = dq$.

5.1 Factoring Integers

- *In this section, we will recall some basic terminologies and properties of* $\mathbb{Z}$.

Definition. *We say that*

- d *divides*(整除) n *if there exists an integer* q *satisfying* $n = dq$.
- *We call* q *the quotient*(商) *and* d *a divisor*(除子) *or factor of* n.

5.1 Factoring Integers

- *In this section, we will recall some basic terminologies and properties of* $\mathbb{Z}$.

Definition. *We say that*

- d *divides(整除)* n *if there exists an integer* q *satisfying* $n = dq$.
- *We call* q *the quotient(商) and* d *a divisor(除子) or factor of* n.
- *If* d *divides* n, *we write* $d \mid n$. *If* d *does not divide* n, *we write* $d \nmid n$.

Quotient-Remainder Theorem

If d and n are integers, $d > 0$, there exist integers q (quotient) and r (remainder) satisfying

$$n = dq + r \quad 0 \leq r < d.$$

Quotient-Remainder Theorem

If d and n are integers, $d > 0$, there exist integers q (quotient) and r (remainder) satisfying

$$n = dq + r \quad 0 \leq r < d.$$

Furthermore, q and r are unique; that is, if

$$n = dq_1 + r_1 \quad 0 \leq r_1 < d \ \text{and} \ n = dq_2 + r_2 \quad 0 \leq r_2 < d,$$

then $q_1 = q_2$ and $r_1 = r_2$.

Definition

- *An integer greater than* 1 *whose only positive divisors are itself and* 1 *is called* **prime**(质数或素数).
- *An integer greater than 1 that is not prime is called* **composite**(合数).

Fundamental Theorem of Arithmetic

Fundamental Theorem of Arithmetic

- *Except for the order of the prime factors, the prime factors are unique.*

Fundamental Theorem of Arithmetic

- *Except for the order of the prime factors, the prime factors are unique.*

Proposition. *Any integer n can be written as a product of power of primes and ± 1, i.e.,*

$$n = (\pm 1) p_1^{k_1} p_2^{k_2} \cdots p_\ell^{k_\ell},$$

where p_i's are distinct primes.

Fundamental Theorem of Arithmetic

Proposition.

Fundamental Theorem of Arithmetic

Proposition. *Moreover, if the primes are written in nondecreasing order, the factorization is unique. In symbols, if where the* p_k *are primes and* $p_1 \leq p_2 \leq \cdots \leq p_\ell$, *and*

$$n = (\pm 1) q_1^{w_1} q_2^{w_2} \cdots q_j^{w_j},$$

where the q_k *are primes and* $q_1 \leq q_2 \leq \cdots \leq q_j$, *then* $j = \ell$ *and*

$$w_i = k_i,\ p_i = q_i \quad \textit{for all } i = 1, \ldots, \ell.$$

Fundamental Theorem of Arithmetic

Proposition. *Moreover, if the primes are written in nondecreasing order, the factorization is unique. In symbols, if where the p_k are primes and $p_1 \le p_2 \le \cdots \le p_\ell$, and*

$$n = (\pm 1) q_1^{w_1} q_2^{w_2} \cdots q_j^{w_j},$$

where the q_k are primes and $q_1 \le q_2 \le \cdots \le q_j$, then $j = \ell$ and

$$w_i = k_i,\ p_i = q_i \quad \text{for all } i = 1, \ldots, \ell.$$

Proposition. *The number of primes is infinite.*

Fundamental Theorem of Arithmetic

Proposition. *Moreover, if the primes are written in nondecreasing order, the factorization is unique. In symbols, if where the* p_k *are primes and* $p_1 \leq p_2 \leq \cdots \leq p_\ell$, *and*

$$n = (\pm 1) q_1^{w_1} q_2^{w_2} \cdots q_j^{w_j},$$

where the q_k *are primes and* $q_1 \leq q_2 \leq \cdots \leq q_j$, *then* $j = \ell$ *and*

$$w_i = k_i, \ p_i = q_i \quad \text{for all } i = 1, \ldots, \ell.$$

Proposition. *The number of primes is infinite.*

Remark. *we will give the proof in 5.3.*

Greatest common divisor (最大公约数)

- *The* **greatest common divisor** *of two integers m and n (not both zero) is the largest positive integer* $\gcd(m, n)$ *that divides both m and n.*

Greatest common divisor (最大公约数)

Proposition. *Let m and n be integers, $m > 1$, $n > 1$, with prime factorizations*

$$m = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}, \text{ and } n = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}.$$

(If the prime p_i is not a factor of m, we let $a_i = 0$. Similarly, if the prime p_i is not a factor of n, we let $b_i = 0$.) Then

$$\gcd(m, n) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \cdots p_k^{\min(a_k, b_k)}$$

Least common multiple (最小公倍数)

Least common multiple (最小公倍数)

Definition. *Let m and n be positive integers.*

- *A common multiple of m and n is an integer that is divisible by both m and n.*

Least common multiple (最小公倍数)

Definition. *Let m and n be positive integers.*

- *A common multiple of m and n is an integer that is divisible by both m and n.*
- *The least common multiple, written $\operatorname{lcm}(m, n)$, is the smallest positive common multiple of m and n.*

Least common multiple (最小公倍数)

Proposition. *Let m and n be integers, $m > 1, n > 1$, with prime factorizations*

$$m = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}, \text{ and } n = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}.$$

(If the prime p_i is not a factor of m, we let $a_i = 0$. Similarly, if the prime p_i is not a factor of n, we let $b_i = 0$.) Then

$$\operatorname{lcm}(m, n) = p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \cdots p_k^{\max(a_k,b_k)}.$$

Least common multiple (最小公倍数)

Proposition. *Let m and n be integers, $m > 1, n > 1$, with prime factorizations*

$$m = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}, \text{ and } n = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}.$$

(If the prime p_i is not a factor of m, we let $a_i = 0$. Similarly, if the prime p_i is not a factor of n, we let $b_i = 0$.) Then

$$\operatorname{lcm}(m, n) = p_1^{\max(a_1, b_1)} p_2^{\max(a_2, b_2)} \cdots p_k^{\max(a_k, b_k)}.$$

Proposition. *For any positive integers m and n,*

$$\gcd(m, n) \cdot \operatorname{lcm}(m, n) = mn.$$

5.2 Representations of Integers

5.2 Representations of Integers

In this section, we discuss

5.2 Representations of Integers

In this section, we discuss

- *the* **binary number system**(二进制数习题), *which represents integers using bits (i.e. 0,1),*

5.2 Representations of Integers

In this section, we discuss

- *the* **binary number system***(二进制数习题), which represents integers using bits (i.e. 0,1),*
- *the m-***number system***, which represents integers using m symbols.*

- *In the decimal number system(十进制数系统), to represent integers we use the 10 symbols* 0, 1, 2, 3, 4, 5, 6, 7, 8, *and* 9.

- *In the decimal number system(十进制数系统), to represent integers we use the 10 symbols* $0, 1, 2, 3, 4, 5, 6, 7, 8,$ *and* 9.
- *For example,*

$$3854 = 3 \cdot 10^3 + 8 \cdot 10^2 + 5 \cdot 10^1 + 4 \cdot 10^0.$$

Here $3, 8, 5, 4$ *are in* $\{0, 1, \ldots, 9\}$.

5.2 Representations of Integers

- *In general, let m be a positive integer, an m-number system(m 进制数) is a number system represents integers using* $\{0, 1, \ldots, m-1\}$.

- *In general, let m be a positive integer, an m-number system(m 进制数) is a number system represents integers using $\{0, 1, \ldots, m-1\}$.*
- *That is if n is a positive integer, we have*

$$n = n_t \cdot m^t + n_{t-1} \cdot m^{t-1} + \cdots + n_1 \cdot m + n_0$$

with $n_i \in \{0, 1, \ldots, m-1\}$.

Example. *The binary number* 101101_2 *may be expressed*

$$101101_2 = 1 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0.$$

Example. *The binary number* 101101_2 *may be expressed*

$$101101_2 = 1 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0.$$

Computing the right-hand side in decimal, we find that

$$\begin{aligned} 101101_2 &= 1 \cdot 32 + 0 \cdot 16 + 1 \cdot 8 + 1 \cdot 4 + 0 \cdot 2 + 1 \cdot 1 \\ &= 32 + 8 + 4 + 1 = 45_{10}. \end{aligned}$$

How to write a positive integer n in the m-number system?

How to write a positive integer n in the m-number system?

Observation: $n = (n_t \cdot m^{t-1} + n_{t-1} \cdot m^{t-2} + \cdots + n_1) \cdot m + n_0$

How to write a positive integer n in the m-number system?

Observation: $n = (n_t \cdot m^{t-1} + n_{t-1} \cdot m^{t-2} + \cdots + n_1) \cdot m + n_0$

- *This means, if we let n be divided by m, the we have quotient* $q_1 = n_t \cdot m^{t-1} + n_{t-1} \cdot m^{t-2} + \cdots + n_1$*, and remainder* n_0.

How to write a positive integer n in the m-number system?

Observation: $n = (n_t \cdot m^{t-1} + n_{t-1} \cdot m^{t-2} + \cdots + n_1) \cdot m + n_0$

- *This means, if we let n be divided by m, the we have quotient $q_1 = n_t \cdot m^{t-1} + n_{t-1} \cdot m^{t-2} + \cdots + n_1$, and remainder n_0.*
- *Ditto for q_1, we see that n_1 is the remainder of q_1 divided by m.*

How to write a positive integer n in the m-number system?

Observation: $n = (n_t \cdot m^{t-1} + n_{t-1} \cdot m^{t-2} + \cdots + n_1) \cdot m + n_0$

- *This means, if we let n be divided by m, the we have quotient* $q_1 = n_t \cdot m^{t-1} + n_{t-1} \cdot m^{t-2} + \cdots + n_1$, *and remainder* n_0.
- *Ditto for* q_1, *we see that* n_1 *is the remainder of* q_1 *divided by* m.
- *We then denote the quotient by* q_2.

How to write a positive integer n in the m-number system?

Observation: $n = (n_t \cdot m^{t-1} + n_{t-1} \cdot m^{t-2} + \cdots + n_1) \cdot m + n_0$

- *This means, if we let n be divided by m, the we have quotient* $q_1 = n_t \cdot m^{t-1} + n_{t-1} \cdot m^{t-2} + \cdots + n_1$, *and remainder* n_0.
- *Ditto for* q_1, *we see that* n_1 *is the remainder of* q_1 *divided by* m.
- *We then denote the quotient by* q_2.
- *We divide* q_2 *by* m *and get quotient* q_3 *and remainder* n_2.
- ...

Summary. *To write a positive integer n in the m-number system:*

Summary. *To write a positive integer n in the m-number system:*

- *We divide n by m and the related quotient q_i by m.*

Summary. *To write a positive integer n in the m-number system:*

- *We divide n by m and the related quotient q_i by m.*
- *At each time, we get the remainder n_i and the next quotient q_{i+1}.*

Summary. *To write a positive integer n in the m-number system:*

- *We divide n by m and the related quotient q_i by m.*
- *At each time, we get the remainder n_i and the next quotient q_{i+1}.*
- *When $q_{t+1} = 0$, we stop and get*

$$n = n_t \cdot m^t + n_{t-1} \cdot m^{t-1} + \cdots + n_1 \cdot m + n_0.$$

Summary. *To write a positive integer n in the m-number system:*

- *We divide n by m and the related quotient q_i by m.*
- *At each time, we get the remainder n_i and the next quotient q_{i+1}.*
- *When $q_{t+1} = 0$, we stop and get*

$$n = n_t \cdot m^t + n_{t-1} \cdot m^{t-1} + \cdots + n_1 \cdot m + n_0.$$

- *We call the value on which the system is based (10 in the case of the decimal system) the base of the number system.*

Example. *Write the decimal number 130 in binary.*

Example. *Write the decimal number 130 in binary.*

SOL. *The computation shows the successive divisions by 2 with the remainders recorded at the right.*

Example. *Write the decimal number 130 in binary.*

SOL. *The computation shows the successive divisions by 2 with the remainders recorded at the right.*

$$\underline{130}\ \textit{remainder} = 0$$
$$\underline{65}\ \textit{remainder} = 1$$
$$\underline{32}\ \textit{remainder} = 0$$
$$\underline{16}\ \textit{remainder} = 0$$
$$\underline{8}\ \textit{remainder} = 0$$
$$\underline{4}\ \textit{remainder} = 0$$
$$\underline{2}\ \textit{remainder} = 0$$
$$\underline{1}\ \textit{remainder} = 1$$
$$\underline{0}\ \textit{stop}$$

Example. *Write the decimal number 130 in binary.*

SOL. *The computation shows the successive divisions by 2 with the remainders recorded at the right.*

$$\underline{130}\ remainder = 0$$
$$\underline{65}\ remainder = 1$$
$$\underline{32}\ remainder = 0$$
$$\underline{16}\ remainder = 0$$
$$\underline{8}\ remainder = 0$$

$$\underline{4}\ remainder = 0$$
$$\underline{2}\ remainder = 0$$
$$\underline{1}\ remainder = 1$$
$$\underline{0}\ stop$$

We obtain

$$130_{10} = 10000010_2.$$

5. $2\frac{1}{2}$ Representations of Integers

5. $2\frac{1}{2}$ Representations of Integers

- *In this section, we will construct the induced operations on the quotient sets.*

5. $2\frac{1}{2}$ *Modular Arithmetic*

Example. $\mathbb{Z}$ *has addition* $+$ *and multiplication* $\times$.

Example. $\mathbb{Z}$ *has addition* $+$ *and multiplication* $\times$.

- $\mathbb{Z}$ *can be divided into disjoint union* $\mathbb{Z} = \text{Even} \sqcup \text{Odd}$.

Example. $\mathbb{Z}$ *has addition* $+$ *and multiplication* $\times$.

- $\mathbb{Z}$ *can be divided into disjoint union* $\mathbb{Z} = \mathrm{Even} \sqcup \mathrm{Odd}$.
- *Here* $\sqcup$ *means disjoint union.*

Example. $\mathbb{Z}$ *has addition* $+$ *and multiplication* $\times$.

- $\mathbb{Z}$ *can be divided into disjoint union* $\mathbb{Z} = \mathrm{Even} \sqcup \mathrm{Odd}$.
- *Here* $\sqcup$ *means disjoint union.*
- *On the two elements set* $\{\mathrm{Even}, \mathrm{Odd}\}$, *there induces the operations* $+'$ *and* $\times'$ *form* $\mathbb{Z}$,

Example. $\mathbb{Z}$ *has addition* $+$ *and multiplication* $\times$.

- $\mathbb{Z}$ *can be divided into disjoint union* $\mathbb{Z} = \text{Even} \sqcup \text{Odd}$.
- *Here* $\sqcup$ *means disjoint union.*
- *On the two elements set* $\{\text{Even}, \text{Odd}\}$, *there induces the operations* $+'$ *and* $\times'$ *form* $\mathbb{Z}$,
- *given by:* $\text{Odd} +' \text{Odd} = \text{Even}$, $\text{Even} +' \text{Odd} = \text{Odd}$, $\text{Even} \times' \text{Odd} = \text{Even}$ *and so on.*

Example. $\mathbb{Z}$ *has addition* $+$ *and multiplication* $\times$.

- $\mathbb{Z}$ *can be divided into disjoint union* $\mathbb{Z} = \text{Even} \sqcup \text{Odd}$.
- *Here* $\sqcup$ *means disjoint union.*
- *On the two elements set* $\{\text{Even}, \text{Odd}\}$, *there induces the operations* $+'$ *and* $\times'$ *form* $\mathbb{Z}$,
- *given by:* $\text{Odd} +' \text{Odd} = \text{Even}$, $\text{Even} +' \text{Odd} = \text{Odd}$, $\text{Even} \times' \text{Odd} = \text{Even}$ *and so on.*
- *The induced operations are called* **modular arithemetic.**

To make it precise, we have the following problems

To make it precise, we have the following problems

- *What is the precise definition of an operation?*

To make it precise, we have the following problems

- *What is the precise definition of an operation?*
- *How to define the quotient set as* $\{\text{Even}, \text{Odd}\}$*?*

To make it precise, we have the following problems

- *What is the precise definition of an operation?*
- *How to define the quotient set as* $\{\text{Even}, \text{Odd}\}$*?*
- *How does it induce operations?*

Recall the definition of a **mapping***(or* **function***).*

Recall the definition of a **mapping***(or* **function***).*

Definition.
Let X and Y be certain sets. We say that there is a **function** *defined on X with values in Y if, by virtue of some rule f, to each element $x \in X$ there corresponds an element $y \in Y$.*

Recall the definition of a **mapping** *(or* **function** *).*

Definition.
Let X and Y be certain sets. We say that there is a **function** *defined on X with values in Y if, by virtue of some rule f, to each element $x \in X$ there corresponds an element $y \in Y$.*

In this case

Recall the definition of a **mapping** *(or* **function***).*

Definition.
Let X and Y be certain sets. We say that there is a **function** *defined on X with values in Y if, by virtue of some rule f, to each element $x \in X$ there corresponds an element $y \in Y$.*

In this case

- *the set X is called the domain of the function,* *Recall the definition of a* **mapping** *(or* **function***).*

Definition.
Let X and Y be certain sets. We say that there is a **function** *defined on X with values in Y if, by virtue of some rule f, to each element $x \in X$ there corresponds an element $y \in Y$.*

In this case

- *the set X is called the domain of the function,*
- *the set Y is called the codomain or target of the function,*

Recall the definition of a **mapping** *(or* **function** *).*

Definition.
Let X and Y be certain sets. We say that there is a **function** *defined on X with values in Y if, by virtue of some rule f, to each element $x \in X$ there corresponds an element $y \in Y$.*

In this case

- *the set X is called the domain of the function,*
- *the set Y is called the codomain or target of the function,*
- *the set $f(X) = \{y \mid \text{exist } x \in X, \text{ such that } y = f(x)\}$ is called the image of the function.*

Definition. *Let W be a subset of Y, the set $f^{-1}(W) = \{x \in X \mid f(x) \in W\}$ is called the* **preimage** *of W. Inparticualr, if W is a point y in Y, then we also call the preimage set $f^{-1}(y)$ as the* **fiber** *of f over $y \in Y$.*

Definition. *Let W be a subset of Y, the set $f^{-1}(W) = \{x \in X \mid f(x) \in W\}$ is called the* **preimage** *of W. Inparticualr, if W is a point y in Y, then we also call the preimage set $f^{-1}(y)$ as the* **fiber** *of f over $y \in Y$.*

Remark. *it is possible that the preimage set is empty. e.g.*
$f : \mathbb{R} \to \mathbb{R}, x \mapsto x^2$, *then* $f^{-1}(-1) = \emptyset$.

Definition. *Let W be a subset of Y, the set $f^{-1}(W) = \{x \in X \mid f(x) \in W\}$ is called the* **preimage** *of W. Inparticualr, if W is a point y in Y, then we also call the preimage set $f^{-1}(y)$ as the* **fiber** *of f over $y \in Y$.*

Remark. *it is possible that the preimage set is empty. e.g. $f : \mathbb{R} \to \mathbb{R}, x \mapsto x^2$, then $f^{-1}(-1) = \emptyset$.*

Remark. *More precisely, the rule f can be under stand as a special kind of subsets of $X \times Y$ such that $(x, y_1), (x, y_2) \in f$ implies that $y_1 = y_2$, i.e. for each x, there is only one $f(x) \in Y$ such that $(s, f(x)) \in f$.*

Example.

Example.

- *Addition:* $+ : \mathbb{R} \times \mathbb{R} \to \mathbb{R},\ (a, b) \mapsto a + b$ *is a function/mapping.*

Example.

- *Addition*: $+ : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$, $(a, b) \mapsto a + b$ *is a function/mapping.*
- *Multiplication*: $\times : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$, $(a, b) \mapsto a \times b$ *is a function/mapping.*

Definition. *Let X, Y be two sets, a function from $X \times Y$ to Y is called an* **algebraic operation** *of X on Y, and a function from $X \times X$ to X is called a* **binary operation** *on X.*

Definition. *Let X, Y be two sets, a function from $X \times Y$ to Y is called an* **algebraic operation** *of X on Y, and a function from $X \times X$ to X is called a* **binary operation** *on X.*

Remark. *For binary operation, for example $f : X \times X \to X$, we also denote $f(x_1, x_2)$ as $x_1 f x_2$ especially when f is some addtion or multiplication operation.*

Definition. *Let X, Y be two sets, a function from $X \times Y$ to Y is called an* **algebraic operation** *of X on Y, and a function from $X \times X$ to X is called a* **binary operation** *on X.*

Remark. *For binary operation, for example $f : X \times X \to X$, we also denote $f(x_1, x_2)$ as $x_1 f x_2$ especially when f is some addtion or multiplication operation.*

Example. *Let V be an $\mathbb{R}$-vector space, then the multiplication of scalars is an algebraic operation of $\mathbb{R}$ on V and the addition of vectors is a binary operation on V.*

We will always consider the following structures, which are sets with one binary operation.

We will always consider the following structures, which are sets with one binary operation.

Definition. *If a set with one binary operation* $(V, \star)$ *satisfy the following conditions, we call it a* **commutative monoid(交换幺半群)** *or* **abelian monoid**.

We will always consider the following structures, which are sets with one binary operation.

Definition. *If a set with one binary operation* $(V, \star)$ *satisfy the following conditions, we call it a* **commutative monoid(交换幺半群)** *or* **abelian monoid**.

- $\star$ *is associative, for all* $a, b, c \in V$ $(a \star b) \star c = a(b \star c)$;

We will always consider the following structures, which are sets with one binary operation.

Definition. *If a set with one binary operation* $(V, \star)$ *satisfy the following conditions, we call it a* **commutative monoid(交换幺半群)** *or* **abelian monoid**.

- $\star$ *is associative, for all* $a, b, c \in V$ $(a \star b) \star c = a(b \star c)$;
- $\star$ *is commutative, for all* $a, b \in V$ $a \star b = b \star a$;

We will always consider the following structures, which are sets with one binary operation.

Definition. *If a set with one binary operation* $(V, \star)$ *satisfy the following conditions, we call it a* **commutative monoid(交换幺半群)** *or* **abelian monoid**.

- $\star$ *is associative, for all* $a, b, c \in V$ $(a \star b) \star c = a(b \star c)$;
- $\star$ *is commutative, for all* $a, b \in V$ $a \star b = b \star a$;
- $\star$ *has a unit element, there exist a* $e \in V$ *such that for all* $a \in V$, *one has* $a \star e = e \star a = a$.

Definition. *If a set with one binary operation* $(V, \star)$ *satisfy the following conditions, we call it a commutative monoid(交换幺半群) or abelian monoid.*

- $\star$ *is associative, for all* $a, b, c \in V$ $(a \star b) \star c = a(b \star c)$;
- $\star$ *is commutative, for all* $a, b \in V$ $a \star b = b \star a$;
- $\star$ *has a unit element, there exist a* $e \in V$ *such that for all* $a \in V$, *one has* $a \star e = e \star a = a$.

Definition. *If a set with one binary operation* $(V, \star)$ *satisfy the following conditions, we call it a commutative monoid(交换幺半群) or abelian monoid.*

- $\star$ *is associative, for all* $a, b, c \in V$ $(a \star b) \star c = a(b \star c)$;
- $\star$ *is commutative, for all* $a, b \in V$ $a \star b = b \star a$;
- $\star$ *has a unit element, there exist a* $e \in V$ *such that for all* $a \in V$, *one has* $a \star e = e \star a = a$.

Definition. *A* **sub-commutative monoid** *(***sub-commutative group***) of a commutative monoid is a subset that is closed under the operation and that contains the unit element e.*

Definition. *If a set with one binary operation $(V, \star)$ satisfy the following conditions, we call it a commutative monoid(交换幺半群) or abelian monoid.*
$\star$ *is associative, for all* $a, b, c \in V$ $(a \star b) \star c = a(b \star c)$;
$\star$ *is commutative, for all* $a, b \in V$ $a \star b = b \star a$;
$\star$ *has a unit element, there exist a* $e \in V$ *such that for all* $a \in V$, *one has* $a \star e = e \star a = a$.

Example. *For example,* $(\mathbb{R}, +)$ $(\mathbb{R}, \times)$, $(\mathbb{Q}, \times)$ *and* $(\mathbb{Z}, \times)$ *and so on are all commutative monoids.*

Definition. *If a set with one binary operation* $(V, \star)$ *satisfy the following conditions, we call it a commutative monoid(交换幺半群) or abelian monoid.*
$\star$ *is associative, for all* $a, b, c \in V$ $(a \star b) \star c = a(b \star c)$;
$\star$ *is commutative, for all* $a, b \in V$ $a \star b = b \star a$;
$\star$ *has a unit element, there exist a* $e \in V$ *such that for all* $a \in V$, *one has* $a \star e = e \star a = a$.

Remark.

Definition. *If a set with one binary operation* $(V, \star)$ *satisfy the following conditions, we call it a commutative monoid(交换幺半群) or abelian monoid.*
$\star$ *is associative, for all* $a, b, c \in V$ $(a \star b) \star c = a(b \star c)$;
$\star$ *is commutative, for all* $a, b \in V$ $a \star b = b \star a$;
$\star$ *has a unit element, there exist a* $e \in V$ *such that for all* $a \in V$, *one has* $a \star e = e \star a = a$.

Remark. *The unit elemet is unique.*

Definition. *If a set with one binary operation* $(V, \star)$ *satisfy the following conditions, we call it a commutative monoid(交换幺半群) or abelian monoid.*

$\star$ *is associative, for all* $a, b, c \in V$ $(a \star b) \star c = a(b \star c)$;

$\star$ *is commutative, for all* $a, b \in V$ $a \star b = b \star a$;

$\star$ *has a unit element, there exist a* $e \in V$ *such that for all* $a \in V$, *one has* $a \star e = e \star a = a$.

Remark. *The unit elemet is unique.*

Because if e_1, e_2 *are all unit elemets,*

Definition. *If a set with one binary operation* $(V, \star)$ *satisfy the following conditions, we call it a commutative monoid(交换幺半群) or abelian monoid.*

$\star$ *is associative, for all* $a, b, c \in V$ $(a \star b) \star c = a(b \star c)$;

$\star$ *is commutative, for all* $a, b \in V$ $a \star b = b \star a$;

$\star$ *has a unit element, there exist a* $e \in V$ *such that for all* $a \in V$*, one has* $a \star e = e \star a = a$.

Remark. *The unit elemet is unique.*

Because if e_1, e_2 *are all unit elemets,*

$\triangleright$ *by the unit property of* e_1, $e_1 \star e_2 = e_2$.

Definition. *If a set with one binary operation* $(V, \star)$ *satisfy the following conditions, we call it a commutative monoid(交换幺半群) or abelian monoid.*

$\star$ *is associative, for all* $a, b, c \in V$ $(a \star b) \star c = a(b \star c)$;

$\star$ *is commutative, for all* $a, b \in V$ $a \star b = b \star a$;

$\star$ *has a unit element, there exist a* $e \in V$ *such that for all* $a \in V$, *one has* $a \star e = e \star a = a$.

Remark. *The unit elemet is unique.*

Because if e_1, e_2 *are all unit elemets,*

$\triangleright$ *by the unit property of* e_1, $e_1 \star e_2 = e_2$.

$\triangleright$ *by the unit property of* e_2, $e_1 \star e_2 = e_1$.

Definition. *If a set with one binary operation* $(V, \star)$ *satisfy the following conditions, we call it a commutative monoid(交换幺半群) or abelian monoid.*
$\star$ *is associative, for all* $a, b, c \in V$ $(a \star b) \star c = a(b \star c)$;
$\star$ *is commutative, for all* $a, b \in V$ $a \star b = b \star a$;
$\star$ *has a unit element, there exist a* $e \in V$ *such that for all* $a \in V$, *one has* $a \star e = e \star a = a$.

Remark. *The unit elemet is unique.*
Because if e_1, e_2 *are all unit elemets,*
$\triangleright$ *by the unit property of* e_1, $e_1 \star e_2 = e_2$.
$\triangleright$ *by the unit property of* e_2, $e_1 \star e_2 = e_1$.
Thus $e_1 = e_1 \star e_2 = e_2$.

Definition. *If a set with one binary operation* $(V, \star)$ *satisfy the following conditions, we call it a commutative monoid(交换幺半群) or abelian monoid.*

$\star$ *is associative, for all* $a, b, c \in V$ $(a \star b) \star c = a(b \star c)$;

$\star$ *is commutative, for all* $a, b \in V$ $a \star b = b \star a$;

$\star$ *has a unit element, there exist a* $e \in V$ *such that for all* $a \in V$*, one has* $a \star e = e \star a = a$.

Definition. *If a set with one binary operation* $(V, \star)$ *satisfy the following conditions, we call it a commutative monoid(交换幺半群) or abelian monoid.*

$\star$ *is associative, for all* $a, b, c \in V$ $(a \star b) \star c = a(b \star c)$;

$\star$ *is commutative, for all* $a, b \in V$ $a \star b = b \star a$;

$\star$ *has a unit element, there exist a* $e \in V$ *such that for all* $a \in V$, *one has* $a \star e = e \star a = a$.

Definition. *Moreover, if a commutative monoid* $(V, \star)$ *satisfy the inverse property, we call it as a* **commutative group** *or an abelian group.*

Definition. *If a set with one binary operation* $(V, \star)$ *satisfy the following conditions, we call it a commutative monoid(交换幺半群) or abelian monoid.*

$\star$ *is associative, for all* $a, b, c \in V$ $(a \star b) \star c = a(b \star c)$;

$\star$ *is commutative, for all* $a, b \in V$ $a \star b = b \star a$;

$\star$ *has a unit element, there exist a* $e \in V$ *such that for all* $a \in V$, *one has* $a \star e = e \star a = a$.

Definition. *Moreover, if a commutative monoid* $(V, \star)$ *satisfy the inverse property, we call it as a* **commutative group** *or an abelian group.*

The inverse property: for any $a \in V$ *there exist* $b \in V$ *such that* $a \star b = b \star a = e$.

Example.

Example.

- $(\mathbb{R}, +)$ *is a commutative group with unit element* 0.

Example.

- $(\mathbb{R}, +)$ *is a commutative group with unit element* 0.
- $(\mathbb{Z}, \times)$ *is a commutative monoid with unit* 1 *but not a commutative group.*

Example.

- $(\mathbb{R}, +)$ *is a commutative group with unit element* 0.
- $(\mathbb{Z}, \times)$ *is a commutative monoid with unit* 1 *but not a commutative group.*
- $(\mathbb{Q} - \{0\}, \times)$ *is a commutative group.*

Example.

- $(\mathbb{R}, +)$ *is a commutative group with unit element* 0.
- $(\mathbb{Z}, \times)$ *is a commutative monoid with unit* 1 *but not a commutative group.*
- $(\mathbb{Q} - \{0\}, \times)$ *is a commutative group.*
- *A vector space* $(V, +)$ *over* $\mathbb{R}$ *is a commutative group with unit the zero vector.*

Definition. *Let V_1, V_2 be two commutative monoids(groups), a monoid(group)* **homomorphism(同态)** *form V_1 to V_2 is a map $\varphi : V_1 \to V_2$, such that it preserves the operation. That is*

$$\varphi(v_1 \star v_2) = \varphi(v_1) \star \varphi(v_2).$$

Definition. *A commutative group with finitely may element is called a* **finite commutative group**.

Definition. *A commutative group with finitely may element is called a* **finite commutative group.**

- *Let* $(H, \star)$ *be a finite commutative group, for every* $x \in H$,

Definition. *A commutative group with finitely may element is called a* **finite commutative group**.

- *Let* $(H, \star)$ *be a finite commutative group, for every* $x \in H$,
- *consider* $x^{\star n}, n \in \mathbb{Z}_+$.

Definition. *A commutative group with finitely may element is called a* **finite commutative group.**

- *Let* $(H, \star)$ *be a finite commutative group, for every* $x \in H$,
- *consider* $x^{\star n}, n \in \mathbb{Z}_+$.
- *Since* H *is finite, there must be* $n_1 \neq n_2$ *s.t.* $x^{\star n_1} = x^{\star n_2}$.

Definition. *A commutative group with finitely may element is called a* **finite commutative group.**

- *Let* $(H, \star)$ *be a finite commutative group, for every* $x \in H$,
- *consider* $x^{\star n}$, $n \in \mathbb{Z}_+$.
- *Since* H *is finite, there must be* $n_1 \neq n_2$ *s.t.* $x^{\star n_1} = x^{\star n_2}$.
- *Assume* $n_1 > n_2$, *then because* $\star$ *is invertible, we have* $x^{\star(n_1 - n_2)} = 1$.

- *This means that for any element x in a commutative group H,*

- *This means that for any element x in a commutative group H,*
- *there is a power such that $x^m = e$.*

- *This means that for any element x in a commutative group H,*
- *there is a power such that $x^m = e$.*
- *We call the smallest positive power as the* **order** *of x.*

- *This means that for any element x in a commutative group H,*
- *there is a power such that $x^m = e$.*
- *We call the smallest positive power as the* **order** *of x.*
- *We have $x^{\mathrm{ord}(x)} = e$ and $\mathrm{ord}(x) \leq \#H$.*

- *This means that for any element x in a commutative group H,*
- *there is a power such that $x^m = e$.*
- *We call the smallest positive power as the* **order** *of x.*
- *We have $x^{\operatorname{ord}(x)} = e$ and $\operatorname{ord}(x) \leq \#H$.*
- *This is because $x^0 = e, x, \ldots, x^{\#H}$ are $H + 1$ elements,*

- *This means that for any element x in a commutative group H,*
- *there is a power such that $x^m = e$.*
- *We call the smallest positive power as the* **order** *of x.*
- *We have $x^{\operatorname{ord}(x)} = e$ and $\operatorname{ord}(x) \leq \#H$.*
- *This is because $x^0 = e, x, \ldots, x^{\#H}$ are $H + 1$ elements,*
- *Thus there must be two of them coincide, and this shows* $\operatorname{ord}(x) \leq \#H$.

5. $2\frac{1}{2}$ Modular Arithmetic

5. $2\frac{1}{2}$ *Modular Arithmetic*

Rings are **algebraic structures** *closed under* **addition, subtraction(减法), and multiplication**, *but not under division. The integers form our basic model for this concept.*

Rings are **algebraic structures** *closed under* **addition, subtraction(减法), and multiplication**, *but not under division. The integers form our basic model for this concept.*

Definition. *A* **ring(环)** *R is a set with two binary operations $+$ and $\times$, called addition and multiplication, that satisfy these axioms:*

Rings are **algebraic structures** *closed under* **addition, subtraction(减法), and multiplication**, *but not under division. The integers form our basic model for this concept.*

Definition. *A* **ring(环)** *R is a set with two binary operations $+$ and $\times$, called addition and multiplication, that satisfy these axioms:*

(a) *With the law of composition, $(R, +)$ is an abelian group; its identity is denoted by 0.*

Rings are **algebraic structures** *closed under* **addition, subtraction(减法), and multiplication**, *but not under division. The integers form our basic model for this concept.*

Definition. *A* **ring**(环) *R is a set with two binary operations $+$ and $\times$, called addition and multiplication, that satisfy these axioms:*

(a) With the law of composition, $(R, +)$ is an abelian group; its identity is denoted by 0.

(b) With the law of multiplication, $(R, \times)$ is a commutative monoid, and has an identity denoted by 1.

Rings are **algebraic structures** *closed under* **addition, subtraction(减法), and multiplication**, *but not under division. The integers form our basic model for this concept.*

Definition. *A* **ring(环)** *R is a set with two binary operations $+$ and $\times$, called addition and multiplication, that satisfy these axioms:*

(a) *With the law of composition, $(R, +)$ is an abelian group; its identity is denoted by* 0.

(b) *With the law of multiplication, $(R, \times)$ is a commutative monoid, and has an identity denoted by* 1.

(c) *distributive law: For all a, b, and c in R, $(a+b)\times c = a\times c + b\times c$.*

Definition. *A* **ring**(环) *R is a set with two binary operations + and* $\times$, *called addition and multiplication, that satisfy these axioms:*

(a) *With the law of composition,* $(R, +)$ *is an abelian group; its identity is denoted by* 0.

(b) *With the law of multiplication,* $(R, \times)$ *is a commutative monoid, and has an identity denoted by* 1.

(c) *distributive law: For all* a, b, *and* c *in* R, $(a + b) \times c = a \times c + b \times c$.

Definition. *A* **subring**(子环) *of a ring is a subset that is closed under the operations of addition, subtraction, and multiplication and that contains the element 1.*

Definition. *A* **ring(环)** *R is a set with two binary operations + and $\times$, called addition and multiplication, that satisfy these axioms:*

(a) *With the law of composition, $(R, +)$ is an abelian group; its identity is denoted by* 0.

(b) *With the law of multiplication, $(R, \times)$ is a commutative monoid, and has an identity denoted by* 1.

(c) *distributive law: For all a, b, and c in R, $(a + b) \times c = a \times c + b \times c$.*

Examples.

Definition. *A* **ring(环)** *R is a set with two binary operations $+$ and $\times$, called addition and multiplication, that satisfy these axioms:*

(a) *With the law of composition, $(R, +)$ is an abelian group; its identity is denoted by 0.*

(b) *With the law of multiplication, $(R, \times)$ is a commutative monoid, and has an identity denoted by 1.*

(c) *distributive law: For all a, b, and c in R, $(a+b)\times c = a \times c + b \times c$.*

Examples.

- *Continuous funtions on $[a, b]$, $C[a, b]$ is a ring but not a field.*

Definition. *A* **ring(环)** *R is a set with two binary operations + and ×, called addition and multiplication, that satisfy these axioms:*

(a) *With the law of composition,* $(R, +)$ *is an abelian group; its identity is denoted by* 0.

(b) *With the law of multiplication,* $(R, \times)$ *is a commutative monoid, and has an identity denoted by* 1.

(c) *distributive law: For all* a, b, *and* c *in* R, $(a + b) \times c = a \times c + b \times c$.

Examples.

- *Continuous funtions on* $[a, b]$, $C[a, b]$ *is a ring but not a field.*
- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ *are fields.*

Definition. *A* **ring(环)** *R is a set with two binary operations + and $\times$, called addition and multiplication, that satisfy these axioms:*

(a) *With the law of composition, $(R, +)$ is an abelian group; its identity is denoted by 0.*

(b) *With the law of multiplication, $(R, \times)$ is a commutative monoid, and has an identity denoted by 1.*

(c) *distributive law: For all a, b, and c in R, $(a+b)\times c = a\times c + b\times c$.*

Examples.

- *Continuous funtions on $[a, b]$, $C[a, b]$ is a ring but not a field.*
- *$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields.*
- *$\mathbb{Z}$ is a ring but not a field.*

Definition *Let R_1, R_2 be two rings, a* **ring homomorphism**(环同态) *form R_1 to R_2 is a map $\varphi : R_1 \to R_2$, such that it preserves the ring operations. That is*

$$\varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2),$$
$$\varphi(r_1 r_2) = \phi(r_1)\phi(r_2).$$

Definition *Let* R_1, R_2 *be two rings, a* **ring homomorphism**(环同态) *form* R_1 *to* R_2 *is a map* $\varphi : R_1 \to R_2$, *such that it preserves the ring operations. That is*

$$\varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2),$$
$$\varphi(r_1 r_2) = \phi(r_1)\phi(r_2).$$

Examples.

Definition *Let* R_1, R_2 *be two rings, a* **ring homomorphism**(环同态) *form* R_1 *to* R_2 *is a map* $\varphi : R_1 \to R_2$, *such that it preserves the ring operations. That is*

$$\varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2),$$
$$\varphi(r_1 r_2) = \phi(r_1)\phi(r_2).$$

Examples.

- *The inclusion* $\mathbb{Q} \hookrightarrow \mathbb{R}$ *is a ring homomorphism.*

Definition *Let R_1, R_2 be two rings, a* **ring homomorphism**(环同态) *form R_1 to R_2 is a map $\varphi : R_1 \to R_2$, such that it preserves the ring operations. That is*

$$\varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2),$$
$$\varphi(r_1 r_2) = \phi(r_1)\phi(r_2).$$

Examples.

- *The inclusion $\mathbb{Q} \hookrightarrow \mathbb{R}$ is a ring homomorphism.*
- *$t \in [a, b]$, the evaluation map $\mathrm{ev}_t : C[a, b] \to \mathbb{R}$, $f \mapsto f(t)$ is a ring homomorphism.*

Definition *Let* R_1, R_2 *be two rings, a* **ring homomorphism** *(环同态) form* R_1 *to* R_2 *is a map* $\varphi : R_1 \to R_2$*, such that it preserves the ring operations. That is*

$$\varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2),$$
$$\varphi(r_1 r_2) = \phi(r_1)\phi(r_2).$$

Definition *Let R_1, R_2 be two rings, a* **ring homomorphism** *(环同态) form R_1 to R_2 is a map $\varphi : R_1 \to R_2$, such that it preserves the ring operations. That is*

$$\varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2),$$
$$\varphi(r_1 r_2) = \phi(r_1)\phi(r_2).$$

Proposition *Let R be a ring, we denote the multiplicative invertible elements by $R^\times$. Then $(R^\times, \times)$ forms a commutative group.*

Quotient set constructions

Quotient set constructions

Definition. *A* **partition** Π *of a set S is a subdivision of S into non-overlapping, nonempty subsets:*

$$S = \text{ union of disjoint nonempty subsets.}$$

Quotient set constructions

Definition. *A* **partition** Π *of a set S is a subdivision of S into non-overlapping, nonempty subsets: $S =$ union of disjoint nonempty subsets.*

Quotient set constructions

Definition. *A* **partition** Π *of a set S is a subdivision of S into non-overlapping, nonempty subsets: $S =$ union of disjoint nonempty subsets*.

Definition. *An* **equivalence relation** *on a set S is a relation that holds between certain pairs of elements. of S.*

Quotient set constructions

Definition. *A* **partition** Π *of a set S is a subdivision of S into non-overlapping, nonempty subsets: S* $=$ *union of disjoint nonempty subsets.*

Definition. *An* **equivalence relation** *on a set S is a relation that holds between certain pairs of elements. of S.*

- *We may write it as a* $\sim$ *b and*

Quotient set constructions

Definition. *A* **partition** Π *of a set S is a subdivision of S into non-overlapping, nonempty subsets:* $S =$ *union of disjoint nonempty subsets.*

Definition. *An* **equivalence relation** *on a set S is a relation that holds between certain pairs of elements. of S.*

- *We may write it as $a \sim b$ and*
- *speak of it as equivalence of a and b.*

Quotient set constructions

Definition. *A* **partition** Π *of a set S is a subdivision of S into non-overlapping, nonempty subsets:* $S =$ *union of disjoint nonempty subsets*.

Definition. *An* **equivalence relation** *on a set S is a relation that holds between certain pairs of elements. of S.*

- *We may write it as* $a \sim b$ *and*
- *speak of it as equivalence of a and b*.

An equivalence relation is required to be:

Quotient set constructions

Definition. *A* **partition** Π *of a set S is a subdivision of S into non-overlapping, nonempty subsets:* $S =$ *union of disjoint nonempty subsets*.

Definition. *An* **equivalence relation** *on a set S is a relation that holds between certain pairs of elements. of S.*

- *We may write it as* $a \sim b$ *and*
- *speak of it as equivalence of a and b.*

An equivalence relation is required to be:

- *transitive: If* $a \sim b$ *and* $b \sim c$*, then* $a \sim c$.

Quotient set constructions

Definition. *A* **partition** Π *of a set S is a subdivision of S into non-overlapping, nonempty subsets: $S =$ union of disjoint nonempty subsets.*

Definition. *An* **equivalence relation** *on a set S is a relation that holds between certain pairs of elements. of S.*

- *We may write it as $a \sim b$ and*
- *speak of it as equivalence of a and b.*

An equivalence relation is required to be:

- *transitive: If $a \sim b$ and $b \sim c$, then $a \sim c$.*
- *symmetric: If $a \sim b$, then $b \sim a$.*

Quotient set constructions

Definition. *A* **partition** Π *of a set* S *is a subdivision of* S *into non-overlapping, nonempty subsets:* $S =$ *union of disjoint nonempty subsets.*

Definition. *An* **equivalence relation** *on a set* S *is a relation that holds between certain pairs of elements. of* S*.*

- *We may write it as* $a \sim b$ *and*
- *speak of it as equivalence of* a *and* b*.*

An equivalence relation is required to be:

- *transitive: If* $a \sim b$ *and* $b \sim c$*, then* $a \sim c$*.*
- *symmetric: If* $a \sim b$*, then* $b \sim a$*.*
- *reflexive: For all* a*,* $a \sim a$*.*

Notation.

Notation. *Let $\sim$ be an equivalent relation on S and $a \in S$.*

Notation. *Let* $\sim$ *be an equivalent relation on* S *and* $a \in S$.

- *We denote* $C_a = \{b \in S \mid a \sim b\}$

Notation. *Let* $\sim$ *be an equivalent relation on* S *and* $a \in S$.

- *We denote* $C_a = \{b \in S \mid a \sim b\}$
- *this set consists of those elements equivalent to* a.

Notation. *Let $\sim$ be an equivalent relation on S and $a \in S$.*

- *We denote $C_a = \{b \in S \mid a \sim b\}$*
- *this set consists of those elements equivalent to a.*
- *This subset is called the equivalence class of a.*

Notation. *Let $\sim$ be an equivalent relation on S and $a \in S$.*

- *We denote $C_a = \{b \in S \mid a \sim b\}$*
- *this set consists of those elements equivalent to a.*
- *This subset is called the equivalence class of a.*
- *Since $\sim$ is an equivalent relation, for any $x \in C_a$, we have $C_x = C_a$.*

Notation. *Let* $\sim$ *be an equivalent relation on* S *and* $a \in S$.

- *We denote* $C_a = \{b \in S \mid a \sim b\}$
- *this set consists of those elements equivalent to* a.
- *This subset is called the equivalence class of* a.
- *Since* $\sim$ *is an equivalent relation, for any* $x \in C_a$*, we have* $C_x = C_a$.

Proposition. *Let* $\sim$ *be an equivalent relation on* S *and* C_a, C_b *be two equivalent classes, then either* $C_a = C_b$ *or* $C_a \cap C_b = \emptyset$.

Notation. *Let $\sim$ be an equivalent relation on S and $a \in S$.*

- *We denote $C_a = \{b \in S \mid a \sim b\}$*
- *this set consists of those elements equivalent to a.*
- *This subset is called the equivalence class of a.*
- *Since $\sim$ is an equivalent relation, for any $x \in C_a$, we have $C_x = C_a$.*

Proposition. *Let $\sim$ be an equivalent relation on S and C_a, C_b be two equivalent classes, then either $C_a = C_b$ or $C_a \cap C_b = \emptyset$.*

In other words, if there exist $x \in C_a \cap C_b$

Notation. *Let $\sim$ be an equivalent relation on S and $a \in S$.*

- *We denote $C_a = \{b \in S \mid a \sim b\}$*
- *this set consists of those elements equivalent to a.*
- *This subset is called the equivalence class of a.*
- *Since $\sim$ is an equivalent relation, for any $x \in C_a$, we have $C_x = C_a$.*

Proposition. *Let $\sim$ be an equivalent relation on S and C_a, C_b be two equivalent classes, then either $C_a = C_b$ or $C_a \cap C_b = \emptyset$.*

In other words, if there exist $x \in C_a \cap C_b$

then by the symmetry and transitive axiom,

Notation. *Let $\sim$ be an equivalent relation on S and $a \in S$.*

- *We denote $C_a = \{b \in S \mid a \sim b\}$*
- *this set consists of those elements equivalent to a.*
- *This subset is called the equivalence class of a.*
- *Since $\sim$ is an equivalent relation, for any $x \in C_a$, we have $C_x = C_a$.*

Proposition. *Let $\sim$ be an equivalent relation on S and C_a, C_b be two equivalent classes, then either $C_a = C_b$ or $C_a \cap C_b = \emptyset$.*

In other words, if there exist $x \in C_a \cap C_b$
then by the symmetry and transitive axiom,
we have $C_a = C_x$ and $C_b = C_x$, thus $C_a = C_b$.

Proposition. *An equivalence relation on a set S determines a partition of S, and conversely.*

Proposition. *An equivalence relation on a set S determines a partition of S, and conversely.*

Proof.

Proposition. *An equivalence relation on a set S determines a partition of S, and conversely.*

Proof.

- *Equivalence relation* $\Rightarrow$ *partition:*

$$S = \sqcup_{a \in S,\ \text{one for each eq. class}} C_a.$$

Proposition. *An equivalence relation on a set S determines a partition of S, and conversely.*

Proof.

- *Equivalence relation* $\Rightarrow$ *partition:*

$$S = \sqcup_{a \in S,\text{ one for each eq. class}} C_a .$$

- *Partition* $\Rightarrow$ *equivalence relation:* $S = \sqcup_i S_i$, *we define the relation R as aRb if and only if* $a, b \in S_i$ *for some* i.

Example.

Example. *We use the following notations*

Example. *We use the following notations*

- $m \in \mathbb{Z}$, *then* $m\mathbb{Z} = \{km \mid k \in \mathbb{Z}\} = \{\ldots, -2m, -m, 0, m, \ldots\}$.

Example. *We use the following notations*

- $m \in \mathbb{Z}$, *then* $m\mathbb{Z} = \{km \mid k \in \mathbb{Z}\} = \{\ldots, -2m, -m, 0, m, \ldots\}$.
- $1 + m\mathbb{Z} = \{\ldots, 1-2m, 1-m, 1, 1+m, \ldots\}$

Example. *We use the following notations*

- $m \in \mathbb{Z}$, then $m\mathbb{Z} = \{km \mid k \in \mathbb{Z}\} = \{\ldots, -2m, -m, 0, m, \ldots\}$.
- $1 + m\mathbb{Z} = \{\ldots, 1 - 2m, 1 - m, 1, 1 + m, \ldots\}$
- $1 + 3\mathbb{Z} = 4 + 3\mathbb{Z}$

Example. *We use the following notations*

- $m \in \mathbb{Z}$, *then* $m\mathbb{Z} = \{km \mid k \in \mathbb{Z}\} = \{\ldots, -2m, -m, 0, m, \ldots\}$.
- $1 + m\mathbb{Z} = \{\ldots, 1 - 2m, 1 - m, 1, 1 + m, \ldots\}$

Example. *We use the following notations*

- $m \in \mathbb{Z}$, *then* $m\mathbb{Z} = \{km \mid k \in \mathbb{Z}\} = \{\ldots, -2m, -m, 0, m, \ldots\}$.
- $1 + m\mathbb{Z} = \{\ldots, 1 - 2m, 1 - m, 1, 1 + m, \ldots\}$

We define the relation on $\mathbb{Z}$ *by:* $a \sim b$ *if and only if* $a - b \in m\mathbb{Z}$.

Example. *We use the following notations*

- $m \in \mathbb{Z}$, *then* $m\mathbb{Z} = \{km \mid k \in \mathbb{Z}\} = \{\ldots, -2m, -m, 0, m, \ldots\}$.
- $1 + m\mathbb{Z} = \{\ldots, 1-2m, 1-m, 1, 1+m, \ldots\}$

We define the relation on $\mathbb{Z}$ *by:* $a \sim b$ *if and only if* $a - b \in m\mathbb{Z}$.

- *Check that this is an equivalence relations*

Example. *We use the following notations*

- $m \in \mathbb{Z}$, *then* $m\mathbb{Z} = \{km \mid k \in \mathbb{Z}\} = \{\ldots, -2m, -m, 0, m, \ldots\}$.
- $1 + m\mathbb{Z} = \{\ldots, 1-2m, 1-m, 1, 1+m, \ldots\}$

We define the relation on $\mathbb{Z}$ *by:* $a \sim b$ *if and only if* $a - b \in m\mathbb{Z}$.

- *Check that this is an equivalence relations*
- *the correponding partition of* $\mathbb{Z}$ *is given by*

$$m\mathbb{Z} \sqcup 1 + m\mathbb{Z} \sqcup \cdots \sqcup (m-1) + m\mathbb{Z}$$

Example. *We use the following notations*

- $m \in \mathbb{Z}$, *then* $m\mathbb{Z} = \{km \mid k \in \mathbb{Z}\} = \{\dots, -2m, -m, 0, m, \dots\}$.
- $1 + m\mathbb{Z} = \{\dots, 1-2m, 1-m, 1, 1+m, \dots\}$

We define the relation on $\mathbb{Z}$ *by:* $a \sim b$ *if and only if* $a - b \in m\mathbb{Z}$.

- *Check that this is an equivalence relations*
- *the correponding partition of* $\mathbb{Z}$ *is given by*

$$m\mathbb{Z} \sqcup 1 + m\mathbb{Z} \sqcup \cdots \sqcup (m-1) + m\mathbb{Z}$$

- *We choose a representative element in each equivalence class* $m\mathbb{Z} = [0]$, $1 + m\mathbb{Z} = [1]$, ..., $(m-1) + m\mathbb{Z} = [m-1]$.

Example. *We use the following notations*

- $m \in \mathbb{Z}$, *then* $m\mathbb{Z} = \{km \mid k \in \mathbb{Z}\} = \{\dots, -2m, -m, 0, m, \dots\}$.
- $1 + m\mathbb{Z} = \{\dots, 1-2m, 1-m, 1, 1+m, \dots\}$

We define the relation on $\mathbb{Z}$ *by:* $a \sim b$ *if and only if* $a - b \in m\mathbb{Z}$.

- *Check that this is an equivalence relations*
- *the correponding partition of* $\mathbb{Z}$ *is given by*

$$m\mathbb{Z} \sqcup 1 + m\mathbb{Z} \sqcup \cdots \sqcup (m-1) + m\mathbb{Z}$$

- *We choose a representative element in each equivalence class* $m\mathbb{Z} = [0],\ 1 + m\mathbb{Z} = [1],\ \dots,\ (m-1) + m\mathbb{Z} = [m-1]$.
- *and we define* $\mathbb{Z}/_{m\mathbb{Z}} = \{[0], [1], \dots, [m-1]\}$.

Proposition. *Let* $(H,+)$ *be a finite commutative group and* $x \in H$*, then*

$$\operatorname{ord}(x) \mid \#H.$$

Proposition. *Let* $(H,+)$ *be a finite commutative group and* $x \in H$*, then*

$$\mathrm{ord}(x) \mid \#H.$$

Proof.

Proposition. *Let* $(H, +)$ *be a finite commutative group and* $x \in H$*, then*

$$\operatorname{ord}(x) \mid \#H.$$

Proof.

- *Denote* $X = \{mx \mid m \in \mathbb{Z}\} \subset H$.

Proposition. *Let $(H, +)$ be a finite commutative group and $x \in H$, then*

$$\operatorname{ord}(x) \mid \#H.$$

Proof.

- *Denote* $X = \{mx \mid m \in \mathbb{Z}\} \subset H$.
- *Check* $\#X = \operatorname{ord}(x)$.

Proposition. *Let $(H, +)$ be a finite commutative group and $x \in H$, then*

$$\mathrm{ord}(x) \mid \#H.$$

Proof.

- *Denote* $X = \{mx \mid m \in \mathbb{Z}\} \subset H$.
- *Check* $\#X = \mathrm{ord}(x)$.
- *We define the relation* $h_1 \sim h_2$ *if and only if* $h_1 - h_2 \in X$.

Proposition. *Let $(H,+)$ be a finite commutative group and $x \in H$, then*

$$\operatorname{ord}(x) \mid \#H.$$

Proof.

- *Denote* $X = \{mx \mid m \in \mathbb{Z}\} \subset H$.
- *Check* $\#X = \operatorname{ord}(x)$.
- *We define the relation* $h_1 \sim h_2$ *if and only if* $h_1 - h_2 \in X$.
- *Check that this is an equivalent relation.*

Proposition. *Let $(H,+)$ be a finite commutative group and $x \in H$, then*

$$\operatorname{ord}(x) \mid \#H.$$

Proof.

- *Denote* $X = \{mx \mid m \in \mathbb{Z}\} \subset H$.
- *Check* $\#X = \operatorname{ord}(x)$.
- *We define the relation* $h_1 \sim h_2$ *if and only if* $h_1 - h_2 \in X$.
- *Check that this is an equivalent relation.*
- *Check the isomorphism* $C_h \cong X$ *given by* $h + mx \mapsto (h + mx) - h$.

Proposition. *Let* $(H, +)$ *be a finite commutative group and* $x \in H$*, then*

$$\mathrm{ord}(x) \mid \#H.$$

Proof.

- *Denote* $X = \{mx \mid m \in \mathbb{Z}\} \subset H$.
- *Check* $\#X = \mathrm{ord}(x)$.
- *We define the relation* $h_1 \sim h_2$ *if and only if* $h_1 - h_2 \in X$.
- *Check that this is an equivalent relation.*
- *Check the isomorphism* $C_h \cong X$ *given by* $h + mx \mapsto (h + mx) - h$.

▶ *Thus* $H = X \sqcup C_{h_1} \sqcup \cdots \sqcup C_{h_\ell}$ *and each* C_{h_i} *has exactly* $\#X$ *elements.*

Proposition. *Let* $(H, +)$ *be a finite commutative group and* $x \in H$*, then*

$$\operatorname{ord}(x) \mid \#H.$$

Proof.

- *Denote* $X = \{mx \mid m \in \mathbb{Z}\} \subset H$.
- *Check* $\#X = \operatorname{ord}(x)$.
- *We define the relation* $h_1 \sim h_2$ *if and only if* $h_1 - h_2 \in X$.
- *Check that this is an equivalent relation.*
- *Check the isomorphism* $C_h \cong X$ *given by* $h + mx \mapsto (h + mx) - h$.

▶ *Thus* $H = X \sqcup C_{h_1} \sqcup \cdots \sqcup C_{h_\ell}$ *and each* C_{h_i} *has exactly* $\#X$ *elements.*

▶ *So* $\#H = \#(\text{eq.classes}) \cdot \#X$.

Definition. *When an equivalence relation on S is given,*

Definition. *When an equivalence relation on S is given, we obtain a new set(of equivalent classes)*

Definition. *When an equivalence relation on S is given, we obtain a new set(of equivalent classes)* $\bar{S} = \{C_a \mid a \in S\}$ *(also denote as* $S/_{\sim}$*) called* **the quotient set.**

Definition. *When an equivalence relation on S is given, we obtain a new set(of equivalent classes)* $\bar{S} = \{C_a \mid a \in S\}$ *(also denote as* $S/_{\sim}$*) called* **the quotient set.**

We can use symbol $[a]$ *to represent* C_a

Definition. *When an equivalence relation on S is given, we obtain a new set(of equivalent classes)* $\bar{S} = \{C_a \mid a \in S\}$ *(also denote as $S/_{\sim}$) called* **the quotient set.**

We can use symbol $[a]$ to represent C_a then $a \sim b$ if and only if $[a] = [b]$ if and only if $C_a = C_b$.

Definition. *When an equivalence relation on S is given, we obtain a new set(of equivalent classes)* $\bar{S} = \{C_a \mid a \in S\}$ *(also denote as $S/_{\sim}$) called* **the quotient set.**

We can use symbol $[a]$ to represent C_a then $a \sim b$ if and only if $[a] = [b]$ if and only if $C_a = C_b$.

Proposition. *For any equivalence relation, there is a natural surjective map*

$$\pi : S \to \bar{S},\ a \mapsto [a].$$

Operations on the quotient set

Operations on the quotient set

The advantage of [_] *notation is:* **we can induce operations on the quotient set.**

Operations on the quotient set

The advantage of [_] *notation is:* **we can induce operations on the quotient set.**

We define the induced addtion and multiplication on $\mathbb{Z}/_{m\mathbb{Z}}$ *as follows*

$$+ : ([a],[b]) \mapsto [a+b], \ \times : ([a],[b]) \mapsto [a \times b]$$

Operations on the quotient set

The advantage of $[\_]$ *notation is:* **we can induce operations on the quotient set.**
We define the induced addtion and multiplication on $\mathbb{Z}/_{m\mathbb{Z}}$ *as follows*

$$+ : ([a],[b]) \mapsto [a+b], \ \times : ([a],[b]) \mapsto [a \times b]$$

For example if $m = 4$,

$$[2] + [3] = [5] = [1],$$

Operations on the quotient set

The advantage of $[\_]$ notation is: **we can induce operations on the quotient set.**
We define the induced addtion and multiplication on $\mathbb{Z}/_{m\mathbb{Z}}$ as follows

$$+ : ([a], [b]) \mapsto [a + b], \ \times : ([a], [b]) \mapsto [a \times b]$$

For example if $m = 4$,

$$[2] + [3] = [5] = [1],$$

this is because $5 = 1 + 4$ thus $5 \sim 1$.

Operations on the quotient set

The advantage of $[\_]$ *notation is:* **we can induce operations on the quotient set.**
We define the induced addtion and multiplication on $\mathbb{Z}/_{m\mathbb{Z}}$ *as follows*

$$+ : ([a],[b]) \mapsto [a+b], \ \times : ([a],[b]) \mapsto [a \times b]$$

For example if $m = 4$,

$$[2] + [3] = [5] = [1],$$

this is because $5 = 1 + 4$ *thus* $5 \sim 1$.

$$[2] \times [3] = [6] = [2]$$

Operations on the quotient set

The advantage of [_] *notation is:* **we can induce operations on the quotient set.**
We define the induced addtion and multiplication on $\mathbb{Z}/_{m\mathbb{Z}}$ *as follows*

$$+ : ([a],[b]) \mapsto [a+b], \ \times : ([a],[b]) \mapsto [a \times b]$$

For example if $m = 4$,

$$[2] + [3] = [5] = [1],$$

this is because $5 = 1 + 4$ *thus* $5 \sim 1$.

$$[2] \times [3] = [6] = [2]$$

this is because $6 = 2 + 4$ *thus* $6 \sim 2$.

Remark. *The* **induced operations** *on the equivalent classes are well defined,*

Remark. *The* **induced operations** *on the equivalent classes are well defined, because they do not depend on the choise of representative elements.*

Remark. *The* **induced operations** *on the equivalent classes are well defined, because they do not depend on the choise of representative elements.*

- *Independent means if we choose* $a' \sim a, b' \sim b$, *then* $[a' + b'] = [a + b]$.

Remark. *The* **induced operations** *on the equivalent classes are well defined, because they do not depend on the choise of representative elements.*

- *Independent means if we choose* $a' \sim a, b' \sim b$, *then* $[a' + b'] = [a + b]$.
- *This is because equivalent elements are up to a multiple of* m.

Remark. *The* **induced operations** *on the equivalent classes are well defined, because they do not depend on the choise of representative elements.*

- *Independent means if we choose* $a' \sim a$, $b' \sim b$, *then* $[a' + b'] = [a + b]$.
- *This is because equivalent elements are up to a multiple of* m.

- *Let* $a' = a + c_1 m$, $b' = b + c_2 m$,

Remark. *The* **induced operations** *on the equivalent classes are well defined, because they do not depend on the choise of representative elements.*

- *Independent means if we choose $a' \sim a$, $b' \sim b$, then* $[a' + b'] = [a + b]$.
- *This is because equivalent elements are up to a multiple of m.*

▶ *Let $a' = a + c_1 m$, $b' = b + c_2 m$, then*

$$[a' + b'] = [a + b + (c_1 + c_2)m] = [a + b],$$

$$[a' \times b'] = [a \times b + (c_1 \times b + a \times c_2 + c_1 \times c_2)m] = [a \times b].$$

Proposition. *For any $m \in \mathbb{Z}$, the set $\mathbb{Z}/_{m\mathbb{Z}}$ of m-elements has an induced ring structure with addtion and multiplication defined as*

$$+ : ([a], [b]) \mapsto [a + b], \ \times : ([a], [b]) \mapsto [a \times b].$$

Proposition. *For any* $m \in \mathbb{Z}$*, the set* $\mathbb{Z}/_{m\mathbb{Z}}$ *of* m*-elements has an induced ring structure with addtion and multiplication defined as*

$$+ : ([a],[b]) \mapsto [a+b], \ \times : ([a],[b]) \mapsto [a \times b].$$

- *Moreover, the surjective map* $q_m : \mathbb{Z} \to \mathbb{Z}/_{m\mathbb{Z}}, \ a \mapsto [a]$ *is a ring homomorphism.*

Proposition. *For any $m \in \mathbb{Z}$, the set $\mathbb{Z}/_{m\mathbb{Z}}$ of m-elements has an induced ring structure with addtion and multiplication defined as*

$$+ : ([a],[b]) \mapsto [a+b], \ \times : ([a],[b]) \mapsto [a \times b].$$

- *Moreover, the surjective map $q_m : \mathbb{Z} \to \mathbb{Z}/_{m\mathbb{Z}}, \ a \mapsto [a]$ is a ring homomorphism.*
- *We call the induced operations on $\mathbb{Z}/_{m\mathbb{Z}}$ as the* **Modular Arithmetic** *(模算术).*

Remark.

Remark. *One also has the following definitions.*

Remark. *One also has the following definitions.*

- *If x is an integer and y is a positive integer, we define $x \mod y$ to be the remainder when x is divided by y.*

Remark. *One also has the following definitions.*

- *If x is an integer and y is a positive integer, we define $x \mod y$ to be the remainder when x is divided by y.*
- *Then $x \mod y = a$ if and only if $[x] = [a] \in \mathbb{Z}/_{y\mathbb{Z}}$ and $0 \leq a \leq y - 1$.*

Remark. *One also has the following definitions.*

- *If* x *is an integer and* y *is a positive integer, we define* $x \mod y$ *to be the remainder when* x *is divided by* y.
- *Then* $x \bmod y = a$ *if and only if* $[x] = [a] \in \mathbb{Z}/_{y\mathbb{Z}}$ *and* $0 \leq a \leq y - 1$.
- *Moreover, for any integers* x, a *s.t.* $x - a \in y\mathbb{Z}$ *we also denote this by* $x \equiv a \pmod{y}$.

5.3 The Euclidean Algorithm

5.3 The Euclidean Algorithm

- *In this section, we introduce the* **Euclidean algorithm** *to find the* **greatest common divisor.**

Recursive Euclidean Algorithm: $\mathrm{EA}(a, b)$ *(output: r_N)*

Recursive Euclidean Algorithm: $\mathrm{EA}(a, b)$ *(output: r_N)*

$$\begin{aligned}
a &= q_0 b + r_0 \\
b &= q_1 r_0 + r_1 \\
&\vdots \\
r_{N-3} &= q_{N-1} r_{N-2} + r_{N-1} \\
r_{N-2} &= q_N r_{N-1} + r_N \\
r_{N-1} &= q_{N+1} r_N + 0
\end{aligned}$$

$r_N \neq 0$ *and* $r_{N+1} = 0$
then stop.

Recursive Euclidean Algorithm: $\mathrm{EA}(a, b)$ *(output: r_N)*

$$
\begin{aligned}
a &= q_0 b + r_0 \\
b &= q_1 r_0 + r_1 \\
&\vdots \\
r_{N-3} &= q_{N-1} r_{N-2} + r_{N-1} \\
r_{N-2} &= q_N r_{N-1} + r_N \\
r_{N-1} &= q_{N+1} r_N + 0
\end{aligned}
$$

$r_N \neq 0$ *and* $r_{N+1} = 0$
then stop.

- *The remainder strictly decreases at each step.*

Recursive Euclidean Algorithm: EA(a, b) *(output: r_N)*

$$
\begin{aligned}
a &= q_0 b + r_0 \\
b &= q_1 r_0 + r_1 \\
&\vdots \\
r_{N-3} &= q_{N-1} r_{N-2} + r_{N-1} \\
r_{N-2} &= q_N r_{N-1} + r_N \\
r_{N-1} &= q_{N+1} r_N + 0
\end{aligned}
$$

$r_N \neq 0$ *and* $r_{N+1} = 0$
then stop.

- *The remainder strictly decreases at each step.*
- *Thus this algorithm stops at finite steps.*

Recursive Euclidean Algorithm: $\mathrm{EA}(a, b)$ *(output: r_N)*

$$
\begin{aligned}
a &= q_0 b + r_0 \\
b &= q_1 r_0 + r_1 \\
&\vdots \\
r_{N-3} &= q_{N-1} r_{N-2} + r_{N-1} \\
r_{N-2} &= q_N r_{N-1} + r_N \\
r_{N-1} &= q_{N+1} r_N + 0
\end{aligned}
$$

$r_N \neq 0$ *and* $r_{N+1} = 0$
then stop.

- *The remainder strictly decreases at each step.*
- *Thus this algorithm stops at finite steps.*

▷ *the last step:* $r_N \mid r_{N-1}$,

Recursive Euclidean Algorithm: $\mathrm{EA}(a, b)$ *(output: r_N)*

$$
\begin{aligned}
a &= q_0 b + r_0 \\
b &= q_1 r_0 + r_1 \\
&\vdots \\
r_{N-3} &= q_{N-1} r_{N-2} + r_{N-1} \\
r_{N-2} &= q_N r_{N-1} + r_N \\
r_{N-1} &= q_{N+1} r_N + 0
\end{aligned}
$$

$r_N \neq 0$ *and* $r_{N+1} = 0$ *then stop.*

- *The remainder strictly decreases at each step.*
- *Thus this algorithm stops at finite steps.*

▷ *the last step:* $r_N \mid r_{N-1}$,

▷ $r_N \mid (r_N + q_N r_{N-1}) = r_{N-2}$;
$r_N \mid r_{N-3}$;
...
$r_N \mid b$, $r_N \mid a$.

Recursive Euclidean Algorithm: $\mathrm{EA}(a, b)$ *(output: r_N)*

$$\begin{aligned} a &= q_0 b + r_0 \\ b &= q_1 r_0 + r_1 \\ &\vdots \\ r_{N-3} &= q_{N-1} r_{N-2} + r_{N-1} \\ r_{N-2} &= q_N r_{N-1} + r_N \\ r_{N-1} &= q_{N+1} r_N + 0 \end{aligned}$$

$r_N \neq 0$ *and* $r_{N+1} = 0$ *then stop.*

- *The remainder strictly decreases at each step.*
- *Thus this algorithm stops at finite steps.*

▷ *the last step:* $r_N \mid r_{N-1}$,

▷ $r_N \mid (r_N + q_N r_{N-1}) = r_{N-2}$;
$r_N \mid r_{N-3}$;
...
$r_N \mid b$, $r_N \mid a$.

▷ *This implies that r_N is the non-zero factor of* $\gcd(a, b)$.

Corollary. *For* $\gcd(a, b) = 1$, *if we run the Euclidean Algorithm for* a, b *then we get* $r_N = 1$.

Corollary. *For* $\gcd(a, b) = 1$, *if we run the Euclidean Algorithm for* a, b *then we get* $r_N = 1$.

- *Because the non-zero factor of* $\gcd(a, b) = 1$ *is only* 1.

Corollary. *For* $\gcd(a, b) = 1$, *if we run the Euclidean Algorithm for* a, b *then we get* $r_N = 1$.
- *Because the non-zero factor of* $\gcd(a, b) = 1$ *is only* 1.

Corollary. *For general* a, b, *each step of the Euclidean algorithm,*

$$\frac{1}{\gcd(a,b)}\mathrm{step}_i\mathrm{EA}(a,b) = \mathrm{step}_i\mathrm{EA}\left(\frac{b}{\gcd(a,b)}, \frac{b}{\gcd(a,b)}\right)$$

Corollary. *For* $\gcd(a,b)=1$, *if we run the Euclidean Algorithm for* a, b *then we get* $r_N = 1$.
- *Because the non-zero factor of* $\gcd(a,b)=1$ *is only* 1.

Corollary. *For general* a, b, *each step of the Euclidean algorithm,*

$$\frac{1}{\gcd(a,b)}\mathrm{step}_i\mathrm{EA}(a,b)=\mathrm{step}_i\mathrm{EA}\left(\frac{b}{\gcd(a,b)},\frac{b}{\gcd(a,b)}\right)$$

- *This is because the uniqueness in the quotient-remainder theorem.*

Corollary. *For* $\gcd(a,b)=1$, *if we run the Euclidean Algorithm for* a,b *then we get* $r_N=1$.

- *Because the non-zero factor of* $\gcd(a,b)=1$ *is only* 1.

Corollary. *For general* a, b, *each step of the Euclidean algorithm,*

$$\frac{1}{\gcd(a,b)}\mathrm{step}_i\mathrm{EA}(a,b)=\mathrm{step}_i\mathrm{EA}\left(\frac{b}{\gcd(a,b)},\frac{b}{\gcd(a,b)}\right)$$

- *This is because the uniqueness in the quotient-remainder theorem.*

Corollary. $\mathrm{EA}(a,b)$ *out put* $\gcd(a,b)$.

Corollary. $r_N = \gcd(a, b)$ *is a* $\mathbb{Z}$*-linear combination of* a *and* b.

$$\begin{aligned}
a &= q_0 b + r_0 \\
b &= q_1 r_0 + r_1 \\
&\vdots \\
r_{N-3} &= q_{N-1} r_{N-2} + r_{N-1} \\
r_{N-2} &= q_N r_{N-1} + r_N \\
r_{N-1} &= q_{N+1} r_N + 0
\end{aligned}$$

Corollary. *$r_N = \gcd(a, b)$ is a $\mathbb{Z}$-linear combination of a and b.*

$$
\begin{aligned}
a &= q_0 b + r_0 \\
b &= q_1 r_0 + r_1 \\
&\vdots \\
r_{N-3} &= q_{N-1} r_{N-2} + r_{N-1} \\
r_{N-2} &= q_N r_{N-1} + r_N \\
r_{N-1} &= q_{N+1} r_N + 0
\end{aligned}
$$

- $r_{N-2} = q_N r_{N-1} + r_N$ *implies that* $r_N = -q_N r_{N-1} + r_{N-2}$

Corollary. $r_N = \gcd(a, b)$ *is a* $\mathbb{Z}$*-linear combination of* a *and* b.

$$\begin{aligned} a &= q_0 b + r_0 \\ b &= q_1 r_0 + r_1 \\ &\vdots \\ r_{N-3} &= q_{N-1} r_{N-2} + r_{N-1} \\ r_{N-2} &= q_N r_{N-1} + r_N \\ r_{N-1} &= q_{N+1} r_N + 0 \end{aligned}$$

- $r_{N-2} = q_N r_{N-1} + r_N$ *implies that* $r_N = -q_N r_{N-1} + r_{N-2}$
- *Ditto for this,* r_{small} *is a* $\mathbb{Z}$*-linear combination of* r_{larger}

Corollary. *$r_N = \gcd(a, b)$ is a $\mathbb{Z}$-linear combination of a and b.*

$$
\begin{aligned}
a &= q_0 b + r_0 \\
b &= q_1 r_0 + r_1 \\
&\vdots \\
r_{N-3} &= q_{N-1} r_{N-2} + r_{N-1} \\
r_{N-2} &= q_N r_{N-1} + r_N \\
r_{N-1} &= q_{N+1} r_N + 0
\end{aligned}
$$

- $r_{N-2} = q_N r_{N-1} + r_N$ *implies that* $r_N = -q_N r_{N-1} + r_{N-2}$
- *Ditto for this,* r_{small} *is a* $\mathbb{Z}$*-linear combination of* r_{larger}
- *Thus* $r_N = \gcd(a, b)$ *is a* $\mathbb{Z}$*-linear combination of* a *and* b.

Corollary. *$r_N = \gcd(a, b)$ is a $\mathbb{Z}$-linear combination of a and b.*

$$
\begin{aligned}
a &= q_0 b + r_0 \\
b &= q_1 r_0 + r_1 \\
&\vdots \\
r_{N-3} &= q_{N-1} r_{N-2} + r_{N-1} \\
r_{N-2} &= q_N r_{N-1} + r_N \\
r_{N-1} &= q_{N+1} r_N + 0
\end{aligned}
$$

- *$r_{N-2} = q_N r_{N-1} + r_N$ implies that $r_N = -q_N r_{N-1} + r_{N-2}$*
- *Ditto for this, r_{small} is a $\mathbb{Z}$-linear combination of r_{larger}*
- *Thus $r_N = \gcd(a, b)$ is a $\mathbb{Z}$-linear combination of a and b.*

Corollary. *There exists $\lambda, \mu \in \mathbb{Z}$ such that $\gcd(a, b) = \lambda a + \mu b$.*

Corollary. $a, b \in \mathbb{Z} - \{0\}$ *are coprime if and only if there exists* $\lambda, \mu \in \mathbb{Z}$ *such that* $\lambda a + \mu b = 1$.

Corollary. $a, b \in \mathbb{Z} - \{0\}$ *are coprime if and only if there exists* $\lambda, \mu \in \mathbb{Z}$ *such that* $\lambda a + \mu b = 1$.

- *Coprime* $\Rightarrow$ *existence: the Euclidean algorithm,*

Corollary. $a, b \in \mathbb{Z} - \{0\}$ *are coprime if and only if there exists* $\lambda, \mu \in \mathbb{Z}$ *such that* $\lambda a + \mu b = 1$.

- *Coprime* $\Rightarrow$ *existence: the Euclidean algorithm,*
- *existence* $\Rightarrow$ *coprime:* $\gcd(a, b) \mid a$, $\gcd(a, b) \mid b$ *implies* $\gcd(a, b) \mid (\lambda a + \mu b) = 1$, *thus* $\gcd(a, b) = 1$.

Further corollaries.

Further corollaries.

Corollary. *Assume* a, m *coprime, then in* $\mathbb{Z}/_{m\mathbb{Z}}$, $[a]$ *is multiplicative invertible.*

Further corollaries.

Corollary. *Assume* a, m *coprime, then in* $\mathbb{Z}/_{m\mathbb{Z}}$, $[a]$ *is multiplicative invertible.*

Proof.

Further corollaries.

Corollary. *Assume a, m coprime, then in $\mathbb{Z}/_{m\mathbb{Z}}$, $[a]$ is multiplicative invertible.*

Proof.

- *there exists* $\lambda, \mu \in \mathbb{Z}$ *such that* $\lambda a + \mu m = 1.$

Further corollaries.

Corollary. *Assume a, m coprime, then in $\mathbb{Z}/_{m\mathbb{Z}}$, $[a]$ is multiplicative invertible.*

Proof.

- *there exists $\lambda, \mu \in \mathbb{Z}$ such that $\lambda a + \mu m = 1$.*
- *Do quotient in $\mathbb{Z}/_{m\mathbb{Z}}$, we get*

Further corollaries.

Corollary. *Assume a, m coprime, then in $\mathbb{Z}/_{m\mathbb{Z}}$, $[a]$ is multiplicative invertible.*

Proof.

- *there exists $\lambda, \mu \in \mathbb{Z}$ such that $\lambda a + \mu m = 1$.*
- *Do quotient in $\mathbb{Z}/_{m\mathbb{Z}}$, we get*
- $[1] = [\lambda a + \mu m] = [\lambda][a] + [0] = [\lambda][a]$.

Further corollaries.

Corollary. *Assume* a, m *coprime, then in* $\mathbb{Z}/_{m\mathbb{Z}}$, $[a]$ *is multiplicative invertible.*

Proof.

- *there exists* $\lambda, \mu \in \mathbb{Z}$ *such that* $\lambda a + \mu m = 1$.
- *Do quotient in* $\mathbb{Z}/_{m\mathbb{Z}}$, *we get*
- $[1] = [\lambda a + \mu m] = [\lambda][a] + [0] = [\lambda][a]$.
- *This means that* $[a]$ *is multiplicative invertible.*

Further corollaries.

Further corollaries.

Corollary. *Assume p is a prime number, then every non-zero element in $\mathbb{Z}/_{p\mathbb{Z}}$ is multiplicative invertible.*

Further corollaries.

Corollary. *Assume p is a prime number, then every non-zero element in $\mathbb{Z}/_{p\mathbb{Z}}$ is multiplicative invertible.*

- *Because every x, $1 \leq x \leq p-1$ is prime to p.*

Further corollaries.

Corollary. *Assume p is a prime number, then every non-zero element in $\mathbb{Z}/_{p\mathbb{Z}}$ is multiplicative invertible.*

- *Because every x, $1 \leq x \leq p-1$ is prime to p.*

Remark. *In other words, $(\mathbb{Z}/_{p\mathbb{Z}}, +, \times)$ is a field. (with finitely may elements)*

Further corollaries. *Fundamental Theorem of Arithmetic*

Further corollaries. *Fundamental Theorem of Arithmetic*

Proposition. *Any integer n can be written as a product of power of primes and ± 1, i.e.,*

$$n = (\pm 1) p_1^{k_1} p_2^{k_2} \cdots p_\ell^{k_\ell},$$

where p_i's are distinct primes.

Further corollaries. *Fundamental Theorem of Arithmetic*

Proposition. *Any integer n can be written as a product of power of primes and ± 1, i.e.,*

$$n = (\pm 1) p_1^{k_1} p_2^{k_2} \cdots p_\ell^{k_\ell},$$

where p_i's are distinct primes.
Moreover, if the p_k are primes and $p_1 \leq p_2 \leq \cdots \leq p_\ell$, and

$$n = (\pm 1) q_1^{w_1} q_2^{w_2} \cdots q_j^{w_j},$$

where the q_k are primes and $q_1 \leq q_2 \leq \cdots \leq q_j$,
then $j = \ell$ and $w_i = k_i$, $p_i = q_i$ for all $i = 1, \ldots, \ell$.

Further corollaries. *Fundamental Theorem of Arithmetic*

Proof.

Further corollaries. *Fundamental Theorem of Arithmetic*

Proof.

- *Assume* $p_1^{k_1} p_2^{k_2} \cdots p_\ell^{k_\ell} = q_1^{w_1} q_2^{w_2} \cdots q_j^{w_j}$ *by dividing the common factors,*

Further corollaries. *Fundamental Theorem of Arithmetic*

Proof.

- *Assume* $p_1^{k_1} p_2^{k_2} \cdots p_\ell^{k_\ell} = q_1^{w_1} q_2^{w_2} \cdots q_j^{w_j}$ *by dividing the common factors,*
- *We can assume that on the left hand side(LHS),*

Further corollaries. *Fundamental Theorem of Arithmetic*

Proof.

- *Assume* $p_1^{k_1} p_2^{k_2} \cdots p_\ell^{k_\ell} = q_1^{w_1} q_2^{w_2} \cdots q_j^{w_j}$ *by dividing the common factors,*
- *We can assume that on the left hand side(LHS),*
  there is a factor p^k *which do not appear in the RHS*

Further corollaries. *Fundamental Theorem of Arithmetic*

Proof.

- *Assume* $p_1^{k_1} p_2^{k_2} \cdots p_\ell^{k_\ell} = q_1^{w_1} q_2^{w_2} \cdots q_j^{w_j}$ *by dividing the common factors,*
- *We can assume that on the left hand side(LHS),*
  there is a factor p^k *which do not appear in the RHS*
- *the other primes are all distinct to* p.

Further corollaries. *Fundamental Theorem of Arithmetic*

Proof.

- *Assume* $p_1^{k_1} p_2^{k_2} \cdots p_\ell^{k_\ell} = q_1^{w_1} q_2^{w_2} \cdots q_j^{w_j}$ *by dividing the common factors,*
- *We can assume that on the left hand side(LHS),*
  there is a factor p^k *which do not appear in the RHS*
- *the other primes are all distinct to* p*.*

▷ *consider the quotient in* $\mathbb{Z}/p\mathbb{Z}$*,*

Further corollaries. *Fundamental Theorem of Arithmetic*

Proof.

- *Assume* $p_1^{k_1} p_2^{k_2} \cdots p_\ell^{k_\ell} = q_1^{w_1} q_2^{w_2} \cdots q_j^{w_j}$ *by dividing the common factors,*
- *We can assume that on the left hand side(LHS), there is a factor* p^k *which do not appear in the RHS*
- *the other primes are all distinct to* p.

▷ *consider the quotient in* $\mathbb{Z}/p\mathbb{Z}$,

- $[LHS] = [0]$ *because* p *is a factor.*

Further corollaries. *Fundamental Theorem of Arithmetic*

Proof.

- *Assume* $p_1^{k_1} p_2^{k_2} \cdots p_\ell^{k_\ell} = q_1^{w_1} q_2^{w_2} \cdots q_j^{w_j}$ *by dividing the common factors,*
- *We can assume that on the left hand side(LHS),*
  there is a factor p^k *which do not appear in the RHS*
- *the other primes are all distinct to* p.

▷ *consider the quotient in* $\mathbb{Z}/p\mathbb{Z}$,

- $[LHS] = [0]$ *because* p *is a factor.*
- $[LHS]$ *is non-zero because it is a multiple of invertible elements.*

Further corollaries. *Fundamental Theorem of Arithmetic*

Proof.

- *Assume* $p_1^{k_1}p_2^{k_2}\cdots p_\ell^{k_\ell} = q_1^{w_1}q_2^{w_2}\cdots q_j^{w_j}$ *by dividing the common factors,*
- *We can assume that on the left hand side(LHS),*
  there is a factor p^k *which do not appear in the RHS*
- *the other primes are all distinct to* p*.*

▷ *consider the quotient in* $\mathbb{Z}/p\mathbb{Z}$*,*

- $[LHS] = [0]$ *because* p *is a factor.*
- $[LHS]$ *is non-zero because it is a multiple of invertible elements.*
- *Contradiction.*

Further corollaries. Proposition. *The number of primes is infinite.*

Further corollaries. Proposition. *The number of primes is infinite.*

Proof.

Further corollaries. Proposition. *The number of primes is infinite.*

Proof.

- *It suffices to show that if p is a prime, there is a prime larger than p.*

Further corollaries. Proposition. *The number of primes is infinite.*

Proof.

- *It suffices to show that if p is a prime, there is a prime larger than p.*
- *Consider the integer*

$$m = p_1 p_2 \cdots p_n + 1$$

Further corollaries. Proposition. *The number of primes is infinite.*

Proof.

- *It suffices to show that if p is a prime, there is a prime larger than p.*
- *Consider the integer*

$$m = p_1 p_2 \cdots p_n + 1$$

- *Notice that when m is divided by p_i, the remainder is 1,*

Further corollaries. **Proposition.** *The number of primes is infinite.*

Proof.

- *It suffices to show that if p is a prime, there is a prime larger than p.*
- *Consider the integer*

$$m = p_1 p_2 \cdots p_n + 1$$

- *Notice that when m is divided by p_i, the remainder is 1,*
- *Thus coprime to each p_i and thus we get an other prime contradiction.*

RSA Public-Key Cryptosystem:

RSA Public-Key Cryptosystem:

Let m be a multiple of two very very big prime number $m = pq$.

RSA Public-Key Cryptosystem:

Let m be a multiple of two very very big prime number $m = pq$.

Fact: *for every $a \in \mathbb{Z}/m\mathbb{Z}$ and every $N \in \mathbb{Z}$, $a^{1+N(p-1)(q-1)} = a$.*

RSA Public-Key Cryptosystem:

Let m be a multiple of two very very big prime number $m = pq$.

Fact: *for every $a \in \mathbb{Z}/m\mathbb{Z}$ and every $N \in \mathbb{Z}$, $a^{1+N(p-1)(q-1)} = a$.*

- *Thus for s, t such that $st = 1 + N(p-1)(q-1)$, we have $a^{st} = a$.*

RSA Public-Key Cryptosystem:

Let m be a multiple of two very very big prime number $m = pq$.

Fact: *for every $a \in \mathbb{Z}/m\mathbb{Z}$ and every $N \in \mathbb{Z}$, $a^{1+N(p-1)(q-1)} = a$.*

- *Thus for s, t such that $st = 1 + N(p-1)(q-1)$, we have $a^{st} = a$.*
- *Thus we can choose good s and t, 甲 knows s and 乙 knows t.*

RSA Public-Key Cryptosystem:

Let m *be a multiple of two very very big prime number* $m = pq$.

Fact: *for every* $a \in \mathbb{Z}/m\mathbb{Z}$ *and every* $N \in \mathbb{Z}$, $a^{1+N(p-1)(q-1)} = a$.

- *Thus for* s, t *such that* $st = 1 + N(p-1)(q-1)$, *we have* $a^{st} = a$.
- *Thus we can choose good* s *and* t, 甲 *knows* s *and* 乙 *knows* t.
- *Then if* 甲 *wants to send* a *to* 乙, *he just have to send* a^s *to the public.*

RSA Public-Key Cryptosystem:

Let m be a multiple of two very very big prime number $m = pq$.

Fact: *for every $a \in \mathbb{Z}/m\mathbb{Z}$ and every $N \in \mathbb{Z}$, $a^{1+N(p-1)(q-1)} = a$.*

- *Thus for s, t such that $st = 1 + N(p-1)(q-1)$, we have $a^{st} = a$.*
- *Thus we can choose good s and t, 甲 knows s and 乙 knows t.*
- *Then if 甲 wants to send a to 乙, he just have to send a^s to the public.*
- *乙 receive a^s and do $(a^s)^t = a$, and get a.*

The End