初等数论
第一章：整除 & 第二章：不定方程

易少云

https://yishaoyun.github.io/syi/ENT2024fall.html

9 月 14 号, 2024

Review

- $(a,b)=1 \quad \Longleftrightarrow \quad \exists\, m,n\in\mathbb{Z}$ s.t. $am+bn=1$.
  1. 若 $(a,b)=1$ 且 $a\mid bc$，则 $a\mid c$.
  2. 若 $(a,b)=1$ 且 $a\mid c$，$b\mid c$，则 $ab\mid c$.
- $[a,b]=\dfrac{ab}{(a,b)}$
- 若 p 是一素数，a 是任一整数，则 $p\mid a$ 或 $(p,a)=1$.
- 标准分解式：$a=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$
- 埃拉托色尼筛法 (Sieve of Eratosthenes) $\rightsquigarrow p_{\min}(a)\le\sqrt{a}$
- 素数的个数是无穷的.
  1. 费马 (Fermat) 数 $F_n=2^{2^n}+1$，$n\in\mathbb{Z}_{\geq 0}$
  2. 梅森 (Mersenne) 数 $M_p=2^p-1$，p 是素数
  3. $\ldots$

An amazing prime with 1800 digits

111111111111111111111111111111111111111111111111111111111111
111111111111111111111111111111111111111111111111111111111111
111111111111111111111111111111111111111111111111111111111111
111111111111111111111111111111111111111111111111111111111111
111111111111111111111111111111111111111111111111111111111111
111111111111111111111111111111111111111111111111111111111111
111111111111188888888888111111111111111111888811111111111111
111111111111118888888888881111111111111188888111111111111111
111111111111111888811118888111111111118888811111111111111111
111111111111111118888111888811111111188881111111111111117111
111111111111111111888811188888111118888811111111111111111111
111111111111111111188888111888811888881111111111111111111111
111111111111111111111888811188888888111111111111111111111111
111111111111111111111188881118888811111111111111111111111111
111111111111111111111118888811188881111111111111111111111111
111111111111111111111111188881118888811111111111111111111111
111111111111111111111111188888811188881111111111111111111111
111111111111111111111118888888881118888111111111111111111111
111111111111111111111888881118888111888881111111111111111111
111111111111111111118888111111888881118888111111111111111111
111111111111111111888881111111118888111888811111111111111111
111111111111111188888111111111111888811118888111111111111111
111111111111118888811111111111111188888888888811111111111111
111111111111188881111111111111111111188888888888111111111111
111111111111111111111111111111111111111111111111111111111111
111111111111111111111111111111111111111111111111111111111111
111111111111111111111111111111111111111111111111111111111111
111111111111111111111111111111111111111111111111111111111111
111111111111111111111111111111111111111111111111111111111111
111111111111111111111111111111111111111111111111111111111111

高斯取整函数 $[x]$、小数部分函数 $\{x\}$

$$\{x\} = x - [x], \quad x = [x] + \{x\}.$$

高斯取整函数 $[x]$、小数部分函数 $\{x\}$

$$\{x\} = x - [x], \quad x = [x] + \{x\}.$$

1. $[x] \leq x < [x] + 1, \quad x - 1 < [x] \leq x, \quad 0 \leq \{x\} < 1.$

高斯取整函数 $[x]$、小数部分函数 $\{x\}$

$$\{x\} = x - [x], \quad x = [x] + \{x\}.$$

1. $[x] \le x < [x] + 1, \quad x - 1 < [x] \le x, \quad 0 \le \{x\} < 1.$
2. 若 $x \le y$，则 $[x] \le [y]$.

高斯取整函数 $[x]$、小数部分函数 $\{x\}$

$$\{x\} = x - [x], \quad x = [x] + \{x\}.$$

1. $[x] \le x < [x] + 1, \quad x - 1 < [x] \le x, \quad 0 \le \{x\} < 1.$
2. 若 $x \le y$，则 $[x] \le [y]$.
3. $[n + x] = n + [x], \quad \{n + x\} = \{x\}$，$n \in \mathbb{Z}$.

高斯取整函数 $[x]$、小数部分函数 $\{x\}$

$$\{x\} = x - [x], \quad x = [x] + \{x\}.$$

1. $[x] \le x < [x] + 1, \quad x - 1 < [x] \le x, \quad 0 \le \{x\} < 1.$
2. 若 $x \le y$，则 $[x] \le [y]$.
3. $[n + x] = n + [x], \quad \{n + x\} = \{x\},\ n \in \mathbb{Z}.$
4. $[x] + [y] \le [x + y], \quad \{x\} + \{y\} \ge \{x + y\}.$

高斯取整函数 $[x]$、小数部分函数 $\{x\}$

$$\{x\} = x - [x], \quad x = [x] + \{x\}.$$

1. $[x] \le x < [x] + 1, \quad x - 1 < [x] \le x, \quad 0 \le \{x\} < 1.$
2. 若 $x \le y$，则 $[x] \le [y]$.
3. $[n + x] = n + [x], \quad \{n + x\} = \{x\}, \ n \in \mathbb{Z}.$
4. $[x] + [y] \le [x + y], \quad \{x\} + \{y\} \ge \{x + y\}.$
5. $[-x] = \begin{cases} -[x] - 1 & x \notin \mathbb{Z}, \\ -[x] & x \in \mathbb{Z}. \end{cases}, \qquad \{-x\} = \begin{cases} 1 - \{x\} & x \notin \mathbb{Z}, \\ -\{x\} = 0 & x \in \mathbb{Z}. \end{cases}$

高斯取整函数 $[x]$、小数部分函数 $\{x\}$

$$\{x\} = x - [x], \quad x = [x] + \{x\}.$$

1. $[x] \le x < [x] + 1, \quad x - 1 < [x] \le x, \quad 0 \le \{x\} < 1.$
2. 若 $x \le y$，则 $[x] \le [y]$.
3. $[n + x] = n + [x], \quad \{n + x\} = \{x\}$，$n \in \mathbb{Z}$.
4. $[x] + [y] \le [x + y], \quad \{x\} + \{y\} \ge \{x + y\}.$
5. $[-x] = \begin{cases} -[x] - 1 & x \notin \mathbb{Z}, \\ -[x] & x \in \mathbb{Z}. \end{cases}, \qquad \{-x\} = \begin{cases} 1 - \{x\} & x \notin \mathbb{Z}, \\ -\{x\} = 0 & x \in \mathbb{Z}. \end{cases}$
6. (带余除法)：若 a, b 是两整数，$b > 0$，则
$$a = b\left[\frac{a}{b}\right] + b\left\{\frac{a}{b}\right\}, \quad 0 \le b\left\{\frac{a}{b}\right\} \le b - 1.$$

高斯取整函数 $[x]$、小数部分函数 $\{x\}$

$$\{x\} = x - [x], \quad x = [x] + \{x\}.$$

1. $[x] \le x < [x] + 1, \quad x - 1 < [x] \le x, \quad 0 \le \{x\} < 1.$
2. 若 $x \le y$，则 $[x] \le [y]$.
3. $[n + x] = n + [x], \quad \{n + x\} = \{x\}$，$n \in \mathbb{Z}$.
4. $[x] + [y] \le [x + y], \quad \{x\} + \{y\} \ge \{x + y\}.$
5. $[-x] = \begin{cases} -[x] - 1 & x \notin \mathbb{Z}, \\ -[x] & x \in \mathbb{Z}. \end{cases}, \qquad \{-x\} = \begin{cases} 1 - \{x\} & x \notin \mathbb{Z}, \\ -\{x\} = 0 & x \in \mathbb{Z}. \end{cases}$
6. (带余除法)：若 a, b 是两整数，$b > 0$，则
$$a = b\left[\frac{a}{b}\right] + b\left\{\frac{a}{b}\right\}, \quad 0 \le b\left\{\frac{a}{b}\right\} \le b - 1.$$
7. 若 $a, b \in \mathbb{N}$，则不大于 a 而为 b 的倍数的正整数的个数是 $\left[\frac{a}{b}\right]$.

$n!$ 的标准分解式

定理 1

在 $n!$ 的标准分解式中素因数 p $(p \le n)$ 的指数

$$h = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \cdots = \sum_{r=1}^{\infty} \left[\frac{n}{p^r}\right]. \tag{1}$$

$n!$ 的标准分解式

定理 1

在 $n!$ 的标准分解式中素因数 p $(p \le n)$ 的指数

$$h = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \cdots = \sum_{r=1}^{\infty} \left[\frac{n}{p^r}\right]. \tag{1}$$

推论 2

1. $n! = \prod\limits_{p \le n} p^{\sum\limits_{r=1}^{\infty}\left[\frac{n}{p^r}\right]}$

$n!$ 的标准分解式

定理 1

在 $n!$ 的标准分解式中素因数 p $(p \le n)$ 的指数

$$h = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \cdots = \sum_{r=1}^{\infty} \left[\frac{n}{p^r}\right]. \tag{1}$$

推论 2

1. $n! = \prod_{p \le n} p^{\sum_{r=1}^{\infty} \left[\frac{n}{p^r}\right]}$
2. $\dfrac{n!}{k!(n-k)!} \in \mathbb{Z} \quad (0 < k < n)$

$n!$ 的标准分解式

定理 1

在 $n!$ 的标准分解式中素因数 p $(p \leq n)$ 的指数

$$h = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \cdots = \sum_{r=1}^{\infty} \left[\frac{n}{p^r}\right]. \tag{1}$$

推论 2

1. $n! = \prod\limits_{p \leq n} p^{\sum_{r=1}^{\infty} \left[\frac{n}{p^r}\right]}$
2. $\dfrac{n!}{k!(n-k)!} \in \mathbb{Z} \quad (0 < k < n)$
3. 设 $f(x) \in \mathbb{Z}[x], \deg f(x) = n$，则 $\dfrac{f^{(k)}(x)}{k!} \in \mathbb{Z}[x]$ 且其次数为 $n - k$.

$n!$ 的标准分解式

定理 1

在 $n!$ 的标准分解式中素因数 p $(p \le n)$ 的指数

$$h = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \cdots = \sum_{r=1}^{\infty}\left[\frac{n}{p^r}\right]. \tag{1}$$

推论 2

1. $n! = \prod\limits_{p \le n} p^{\sum\limits_{r=1}^{\infty}\left[\frac{n}{p^r}\right]}$
2. $\dfrac{n!}{k!(n-k)!} \in \mathbb{Z} \quad (0 < k < n)$
3. 设 $f(x) \in \mathbb{Z}[x], \deg f(x) = n$，则 $\dfrac{f^{(k)}(x)}{k!} \in \mathbb{Z}[x]$ 且其次数为 $n-k$.

例： $20!$ 的十进制表示中末尾有多少个零?

第二章：不定方程

- 二元一次不定方程
- 多元一次不定方程
- 勾股数
- 费马问题：无穷递降法 $\rightsquigarrow$ Fermat Last Theorem

定理 3

设 $a, b \in \mathbb{Z}_{\neq 0}, c \in \mathbb{Z}$ 且 $ax + by = c$ 有一整数解 $(x, y) = (x_0, y_0)$，则

$$x = x_0 - \frac{b}{(a, b)}t, \quad y = y_0 + \frac{a}{(a, b)}t, \quad t \in \mathbb{Z}$$

是其所有整数解.

二元一次不定方程 $ax + by = c$

定理 3

设 $a, b \in \mathbb{Z}_{\neq 0}, c \in \mathbb{Z}$ 且 $ax + by = c$ 有一整数解 $(x, y) = (x_0, y_0)$，则

$$x = x_0 - \frac{b}{(a, b)}t, \quad y = y_0 + \frac{a}{(a, b)}t, \quad t \in \mathbb{Z}$$

是其所有整数解.

定理 4

$ax + by = c$ 有整数解 $\Leftrightarrow (a, b) \mid c.$

二元一次不定方程 $ax+by=c$

定理 3

设 $a,b\in\mathbb{Z}_{\neq 0}, c\in\mathbb{Z}$ 且 $ax+by=c$ 有一整数解 $(x,y)=(x_0,y_0)$，则

$$x=x_0-\frac{b}{(a,b)}t,\quad y=y_0+\frac{a}{(a,b)}t,\quad t\in\mathbb{Z}$$

是其所有整数解.

定理 4

$ax+by=c$ 有整数解 $\Leftrightarrow (a,b)\mid c$.

怎么求解?

定理 3

设 $a, b \in \mathbb{Z}_{\neq 0}, c \in \mathbb{Z}$ 且 $ax + by = c$ 有一整数解 $(x, y) = (x_0, y_0)$，则

$$x = x_0 - \frac{b}{(a, b)}t, \quad y = y_0 + \frac{a}{(a, b)}t, \quad t \in \mathbb{Z}$$

是其所有整数解.

定理 4

$ax + by = c$ 有整数解 $\Leftrightarrow (a, b) \mid c$.

怎么求解?

1. $\rightsquigarrow ax + by = (a, b) \quad \Leftrightarrow \quad a_1 x + b_1 y = 1$

二元一次不定方程 $ax+by=c$

定理 3

设 $a,b\in\mathbb{Z}_{\neq 0}, c\in\mathbb{Z}$ 且 $ax+by=c$ 有一整数解 $(x,y)=(x_0,y_0)$，则

$$x=x_0-\frac{b}{(a,b)}t,\quad y=y_0+\frac{a}{(a,b)}t,\quad t\in\mathbb{Z}$$

是其所有整数解.

定理 4

$ax+by=c$ 有整数解 $\Leftrightarrow (a,b)\mid c$.

怎么求解?

1. $\rightsquigarrow ax+by=(a,b) \quad\Leftrightarrow\quad a_1x+b_1y=1$
2. $\rightsquigarrow ax+by=1,\ (a,b)=1$ 用辗转相除法求出其一个特解

二元一次不定方程 $ax+by=c$

定理 3

设 $a,b\in\mathbb{Z}_{\neq 0}, c\in\mathbb{Z}$ 且 $ax+by=c$ 有一整数解 $(x,y)=(x_0,y_0)$，则

$$x=x_0-\frac{b}{(a,b)}t,\quad y=y_0+\frac{a}{(a,b)}t,\quad t\in\mathbb{Z}$$

是其所有整数解.

定理 4

$ax+by=c$ 有整数解 $\Leftrightarrow (a,b)\mid c$.

怎么求解?

1. $\rightsquigarrow ax+by=(a,b) \quad \Leftrightarrow \quad a_1x+b_1y=1$
2. $\rightsquigarrow ax+by=1,\ (a,b)=1$ 　用辗转相除法求出其一个特解
3. 定理 3 $\Rightarrow$ 所有整数解

定理 3

设 $a, b \in \mathbb{Z}_{\neq 0}, c \in \mathbb{Z}$ 且 $ax + by = c$ 有一整数解 $(x, y) = (x_0, y_0)$，则

$$x = x_0 - \frac{b}{(a, b)}t, \quad y = y_0 + \frac{a}{(a, b)}t, \quad t \in \mathbb{Z}$$

是其所有整数解.

定理 4

$ax + by = c$ 有整数解 $\Leftrightarrow (a, b) \mid c$.

怎么求解?

1. $\rightsquigarrow ax + by = (a, b) \quad \Leftrightarrow \quad a_1 x + b_1 y = 1$
2. $\rightsquigarrow ax + by = 1,\ (a, b) = 1$ 用辗转相除法求出其一个特解
3. 定理 3 $\Rightarrow$ 所有整数解

例： 求 $7x + 4y = 100$ 的一切整数解.

多元一次不定方程

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = N, \quad a_i \neq 0,\ 1 \leq i \leq n. \tag{2}$$

定理 5

(2)式有整数解 $\Leftrightarrow (a_1, a_2, \cdots, a_n) \mid N$.

多元一次不定方程

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = N, \quad a_i \neq 0,\ 1 \leq i \leq n. \tag{2}$$

定理 5

(2)式有整数解 $\Leftrightarrow (a_1, a_2, \cdots, a_n) \mid N.$

怎么求解?

多元一次不定方程

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = N, \quad a_i \neq 0,\ 1 \leq i \leq n. \tag{2}$$

定理 5

(2)式有整数解 $\Leftrightarrow (a_1, a_2, \cdots, a_n) \mid N.$

怎么求解?

$\rightsquigarrow$ 求解二元一次不定方程

多元一次不定方程

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = N, \quad a_i \neq 0,\ 1 \leq i \leq n. \tag{2}$$

定理 5

(2)式有整数解 $\Leftrightarrow (a_1, a_2, \cdots, a_n) \mid N$.

怎么求解?

$\rightsquigarrow$ 求解二元一次不定方程

例 1： 求 $9x + 24y - 5z = 1000$ 的一切整数解.

多元一次不定方程

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = N, \quad a_i \neq 0,\ 1 \leq i \leq n. \tag{2}$$

定理 5

(2)式有整数解 $\Leftrightarrow (a_1, a_2, \cdots, a_n) \mid N.$

怎么求解?

$\rightsquigarrow$ 求解二元一次不定方程

例 1： 求 $9x + 24y - 5z = 1000$ 的一切整数解.

例 2： 将 $\dfrac{19}{30}$ 写成三个分数的和，它们的分母分别是 $2, 3$ 和 5.

多元一次不定方程

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = N, \quad a_i \neq 0,\ 1 \leq i \leq n. \tag{2}$$

定理 5

(2)式有整数解 $\Leftrightarrow (a_1, a_2, \cdots, a_n) \mid N.$

怎么求解?

$\rightsquigarrow$ 求解二元一次不定方程

例 1： 求 $9x + 24y - 5z = 1000$ 的一切整数解.

例 2： 将 $\dfrac{19}{30}$ 写成三个分数的和，它们的分母分别是 $2, 3$ 和 5.

注：用 “同余” 的概念求解更简单.

第三次作业（due: 9 月 23 号）

1. $[x]+[y]\le[x+y], \quad \{x\}+\{y\}\ge\{x+y\}.$
2. 设 n 是任一正整数，α 是实数，证明：
   (i) $\left[\dfrac{[n\alpha]}{n}\right]=[\alpha]$;
   (ii) $[\alpha]+\left[\alpha+\dfrac{1}{n}\right]+\cdots+\left[\alpha+\dfrac{n-1}{n}\right]=[n\alpha].$
3. $2024!$ 的十进制表示中末尾有多少个零?
4. 求 $115x+221y=33$ 的一切整数解.
5. 求 $15x+21y-35z=232$ 的一切整数解.
6. 把 $\dfrac{17}{60}$ 写成分母两两互素的三个既约分数之和.