组合数学

笔记整理

姓名：刘斯宇
学号：17341110

目录

1 整数的可除性

1.1 整除

定义 1.1 (整除) 设 a,b 是任意两个整数，若存在一个 $q \in Z$, 使得 $a = bq$ 成立，则称 b 整除 a, 或者说 a 被 b 整除，记作 $b|a$，b 叫做 a 的因子，a 叫做 b 的倍数。

整除的性质

(1) 如果 b 是 a 的因子，那么 $-b$ 也是 $\pm a$ 的因子

(2) 整数的传递性:$c|b, b|a \Rightarrow c|a$

(3)$c|a, c|b \Rightarrow c|(a \pm b)$

(4)$a|b, b|a \Rightarrow a = \pm b$

定义 1.2 (素数) 给定非零整数 p, 如果 p 除了平凡因子 $(\pm 1, \pm p)$ 外，没有其他因子，那么这种整数称为素数 (也叫做质数)

Properties: 素数

- (1) 如果对于所有小于等于 $\sqrt{n}$ 的素数 p 来说，p 都不能整除 n，那么 n 必定是素数
- (2) 若 n 为合数，设 $1 < p$ 是所有 n 的正因子中最小的那一个，那么 p 一定是素数。
- (3) 一般情形：不超过 x 的素数个数记为 $\pi(x)$，有切比雪夫不等式

$$\frac{\ln 2}{3}\frac{x}{\ln x} < \pi(x) < 6\ln 2\frac{x}{\ln x}$$

定理 1.1 素数一定有无穷多个。

证明　假设只有有限哥素数, 设为 $p_1, p_2, \ldots, p_n$, 令 $N = p_1 p_2 \ldots p_n + 1$, 则 N 一定是合数, 并且存在 $p_j \in \{p_1, p_2, \ldots, p_n\}$, 使得 $p_j|N$, 但是又因为 $p_j|p_1 p_2 \ldots p_n$, 所以 $p_j|(N - p_1 p_2 \ldots p_n = 1)$，矛盾。 □

（例题 1）．欧几里德除法

对于任意给定的正整数 k，必有 k 个连续正整数是合数。

解答

构造的 k 个正整数为

$$(k+1)!+2,(k+1)!+3,(k+1)!+4,(k+1)!+5,(k+1)!+6,\ldots,(k+1)!+(k+1)$$

1.2 欧几里德除法

定理 1.2 (欧几里得除法) 对于 $a \in Z, b \in Z^{+}$，存在唯一的 (q,r) 使得 $a = bq + r, 0 \leqslant r < b$ 成立

Tip 欧几里德除法的应用：正整数 b 进制表示。

1.3 最大公因数与互素

定义 1.3 (最大公因数与互素) 给定整数 $a_1, a_2, \cdots, a_n$，如果：

$$d|a_1, d|a_2, \cdots, d|a_n$$

则称 d 为 $a_1, a_2, \cdots, a_n$ 的公因数

如果 $a_1, a_2, \cdots, a_n$ 不全为 0，那么它们的公因数中存在最大的一个，这个公因数称为 $a_1, a_2, \cdots, a_n$ 的最大公因数，记作 $(a_1, a_2, \cdots, a_n)$

如果 $a_1, a_2, \cdots, a_n$ 的最大公因数为 1 的话，称 $a_1, a_2, \cdots, a_n$ 互素，互质

Properties: 最大公因数

- (1) 给定一个整数 a 和一个素数 p，若果 a 不是 p 的倍数的话，它一定和 p 互素。

证明　设 $d=(a,p)$, 则有 $d|p$, 则 $d=1$或p，若 $d=p$，$p|a$ 这与条件矛盾，所以 $d=1$ □

- (2) $a=bq+c \Rightarrow (a,b)=(b,c)$

证明　设 $d=(a,b), d'=(b,c)$，由于

$$d|a, d|b \Longrightarrow d|(a-bq) \Longrightarrow d|c \Longrightarrow d \leq d'$$
$$d'\left|b, d'\right| c \Longrightarrow d'|(bq+c) \Longrightarrow d'|a \Longrightarrow d' \leq d$$

所以 $d=d'$ □

Properties: 最大公因数

- (3) 辗转相除法的性质：$\exists s,t \in Z, s.t., (a,b) = s\cdot a + t\cdot b$

证明： 由辗转相除法，我们可以得到：$\exists s,t \in Z, s.t., s\cdot a + t\cdot b = 1$

$$
\begin{gathered}
a = bq_1 + r_2 \Longrightarrow r_2 = a - bq_1 \\
b = r_2q_2 + r_3 \Longrightarrow r_3 = b - r_2q_2 \\
r_2 = r_3q_3 + r_4 \Longrightarrow r_4 = r_2 - r_3q_3 \\
r_3 = r_4q_4 + r_5 \Longrightarrow r_5 = r_3 - r_4q_4 \\
\cdots\cdots \\
r_{n-4} = r_{n-3}q_{n-3} + r_{n-2} \Longrightarrow r_{n-2} = r_{n-4} - r_{n-3}q_{n-3} \\
r_{n-3} = r_{n-2}q_{n-2} + r_{n-1} \Longrightarrow r_{n-1} = r_{n-3} - r_{n-2}q_{n-2} \\
r_{n-2} = r_{n-1}q_{n-1} + r_n \Longrightarrow r_n = r_{n-2} - r_{n-1}q_{n-1} \\
r_{n-1} = r_nq_n
\end{gathered}
$$

所以

$$
\begin{aligned}
r_n &= r_{n-2} - r_{n-1}q_{n-1} \\
&= r_{n-2} - \left[r_{n-3} - r_{n-2}q_{n-2}\right] q_{n-1} \\
&= \left[r_{n-4} - r_{n-3}q_{n-3}\right] - \left[r_{n-3} - \left(r_{n-4} - r_{n-3}q_{n-3}\right) q_{n-2}\right] q_{n-1} \\
&\cdots\cdots
\end{aligned}
$$

一直这样替换下去，我们可以得到 $(a,b) = s\cdot a + t\cdot b$

推论 1.1 *如果 a,b 互素，那么*

- (4) $(2^a-1, 2^b-1) = 2^{(a,b)} - 1$

证明：

给定正整数 a,b, 利用欧几里德除法我们知道：

$$
\begin{gathered}
\exists q \in \mathbb{Z}, r(0 \le r < b), s.t., a = bq + r \Longrightarrow 2^a = 2^r \cdot 2^{bq} \\
\Longrightarrow 2^a - 1 = 2^r(2^{bq} - 1) + (2^r - 1) \\
\Longrightarrow 2^a - 1 = 2^r(2^b - 1)(q_1) + (2^r - 1) \\
\Longrightarrow 2^a - 1 = (2^b - 1)(2^r \cdot q_1) + (2^r - 1) \\
\Longrightarrow 2^a - 1 = (2^b - 1)q' + (2^r - 1) \quad (q' \in \mathbb{Z}, 0 \le 2^r - 1 < 2^b - 1)
\end{gathered}
$$

即

$$a = bq + r_2(0 \le r_2 < b) \Longrightarrow 2^a - 1 = (2^b-1)q' + (2^{r_2}-1)(q' \in \mathbb{Z}, 0 \le 2^{r_2} - 1 < 2^b - 1)$$

类似地，我们有:

$$b = r_2q_2 + r_3(0 \le r_3 < r_2) \Longrightarrow 2^b - 1 = (2^{r_2}-1)q_2' + (2^{r_3}-1)(q_2' \in \mathbb{Z}, 0 \le 2^{r_3} - 1 < 2^{r_2} - 1)$$

$$r_2 = r_3q_3 + r_4(0 \le r_4 < r_3) \Longrightarrow 2^{r_2} - 1 = (2^{r_3}-1)q_3' + (2^{r_4}-1)(q_3' \in \mathbb{Z}, 0 \le 2^{r_4} - 1 < 2^{r_3} - 1$$

$$r_3 = r_4q_4 + r_5(0 \le r_5 < r_4) \Longrightarrow 2^{r_3} - 1 = (2^{r_4}-1)q_4' + (2^{r_5}-1)(q_4' \in \mathbb{Z}, 0 \le 2^{r_5} - 1 < 2^{r_4} - 1$$

这个过程一直持续下去，如果左边的余数$r_i \ne 0$的话，右边的余数$2^{r_i} - 1 \ne 0$; 如果左边的余数$r_i = 0$的话，右边的余数$2^{r_i} - 1 = 0$.

这样最终在我们到达 a 与 b 的最大公因数 $r_n = (a,b)$ 的时候，我们就得到了 2^a-1 与 2^b-1 的最大公因数，也就是 $2^{r_n} - 1$, 即 $2^{(a,b)} - 1$

Properties: 最大公因数

- (5) $\forall m \in Z^{+}, (am, bm) = (a,b)m$

证明：

事实上，设$d=(a,b)$，$d'=(am,bm)$，只需要说明$d'|(dm)$，$(dm)|d'$ 即可，

$$d=(a,b) \Longrightarrow \exists s,t, s.t., sa+tb=d \Longrightarrow s(am)+t(bm)=dm$$

$$\because d'|(am), d'|(bm), \therefore d'|(s(am)+t(bm)), \therefore d'|(dm)$$

另一方面，dm是am与bm的公因数，而d'是am与bm的最大公因子，所以有$(dm)|d'$ $\diamond$

- (6) $(a,c)=1 \Rightarrow (ab,c)=(b,c)$

证明：

事实上，设$d=(ab,c)$，$d'=(b,c)$，只需要说明$d|d'$，$d'|d$

$$\left.\begin{array}{c} d'|b \Longrightarrow d'|ab \\ d'|c \end{array}\right\} \Longrightarrow d'|d$$

$$\left.\begin{array}{c} (a,c)=1 \Longrightarrow \exists s,t, s.t., sa+tc=1 \Longrightarrow sab+tcb=b \Longrightarrow s(ab)+tb\cdot c=b \\ d|(ab), d|c \end{array}\right\} \Longrightarrow d|b$$

（例题 2）．欧几里德除法

设 n 是合数，p 是 n 的素因子，$\begin{pmatrix} n \\ p \end{pmatrix} = \frac{n(n-1)(n-2)\ldots(n-p+1)}{p!}$，且 $p^{\alpha}||n$（即 $p^{\alpha}|n, p^{\alpha+1}\nmid n$）

，证明 $p^{\alpha} \nmid \begin{pmatrix} n \\ p \end{pmatrix}$

解答

证明　事实上，

$$p^\alpha \mid n \Rightarrow n = m \cdot p^\alpha$$

$$p^{\alpha+1} \nmid n \Rightarrow p \nmid m \Rightarrow (m, p) = 1(\because \text{p is prime})$$

另外，如果 $p \mid n-1$，则 $p \mid n-(n-1)$，则 $p \mid 1$，不可能，所以，$p \nmid 1$，又因为 p 是素数，所以 $(p, n-1) = 1$；类似地，

$$(p, n-2) = 1, (p, n-3) = 1, \ldots, (p, n-(p-1)) = 1$$

从而，

$$(p, (n-1)(n-2)(n-3)\ldots(n-(p-1))) = 1$$

从而，

$$(p, m(n-1)(n-2)(n-3)\ldots(n-(p-1))) = 1$$

从而，

$$(p, \frac{m(n-1)(n-2)(n-3)\ldots(n-(p-1))}{(p-1)!}) = 1$$

(这是因为 p 与 $m(n-1)(n-2)(n-3)\ldots(n-(p-1))$ 的最大公因数是 1，所以与 $m(n-1)(n-2)(n-3)\ldots(n-(p-1))$ 的因子)

$$\frac{m(n-1)(n-2)(n-3)\ldots(n-(p-1))}{(p-1)!}$$

的最大公因数肯定也是 1. 如果 $p^\alpha \mid \binom{n}{p}$，则

$$p^\alpha \mid [p^{\alpha-1} \cdot \frac{m(n-1)(n-2)(n-3)\ldots(n-(p-1))}{(p-1)!}]$$

即

$$p \mid [p^{\alpha-1} \cdot \frac{m(n-1)(n-2)(n-3)\ldots(n-(p-1))}{(p-1)!}]$$

矛盾 □

(例题 3). 欧几里德除法

求 $s, t \in Z, s.t. (169, 121) = s \cdot 169 + t \cdot 121$

解答

回忆辗转相除法的过程，我们可以得到:

$$169 = 1 \cdot 121 + 48$$

$$121 = 2 \cdot 48 + 25$$

$$48 = 1 \cdot 25 + 23$$

$$25 = 1 \cdot 23 + 2$$

$$23 = 11 \cdot 2 + 1$$

$$2 = 2 \cdot 1$$

$$\Rightarrow (169, 121) = 1$$

这样我们有:

$$\begin{aligned} 1 &= 23 - 11 \cdot 2 \\ &= 23 - 11 \cdot (25 - 1 \cdot 23) = 12 \cdot 23 - 11 \cdot 25 \\ &= 12 \cdot (48 - 1 \cdot 25) - 11 \cdot 25 = 12 \cdot 48 - 23 \cdot 25 \\ &= 12 \cdot 48 - 23 \cdot (121 - 2 \cdot 48) = -23 \cdot 121 + 58 \cdot 48 \\ &= -23 \cdot 121 + 58 \cdot (169 - 1 \cdot 121) = 58 \cdot 169 - 81 \cdot 121 \end{aligned}$$

1.4 算术基本定理

定理 1.3 (算术基本定理) 任意正整数 *n>1*, 都可以表示成素数的乘积:

$$n = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_s (p_1 \leqslant p_2 \leqslant p_3 \leqslant \ldots \leqslant p_s)$$

任意正整数 $n > 1$ 可以唯一的表示成

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_t^{\alpha_t}, \alpha_1, \alpha_2, \cdots, \alpha_t \in Z^+$$

这里 $p_1, p_2, \cdots, p_t$ 是互不相同的素数，这被称为 n 的标准分解式

证明

证明 可以用归纳法开证明任何整数 $n > 1$ 可以唯一的表示成

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_t^{\alpha_t}, \alpha_1, \alpha_2, \cdots, \alpha_t \in Z^+$$

设 n 存在两种分解

$$n = p_1 p_2 \ldots p_s \quad (p_1 \leq p_2 \leq \ldots \leq p_s)$$
$$n = q_1 q_2 \ldots q_t \quad (q_1 \leq q_2 \leq \ldots \leq q_t)$$

事实上，$p_1 p_2 \ldots p_s = q_1 q_2 \ldots q_t \Rightarrow p_1 | (q_1 q_2 \ldots q_t)$

$$\Rightarrow \exists j, s.t., p_1 | q_j \Rightarrow p_1 = q_j$$

同样的，

$$\exists k, s.t., q_1 | p_k \Rightarrow q_1 = p_k$$

$$\Rightarrow p_1 \leq p_k = q_1 \leq q_j = p_1$$

$$\Rightarrow p_1 = q_1$$

同理可得 $p_2 = q_2 \ldots$ □

Properties: 算术基本定理

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_t^{\alpha_t}, \alpha_1, \alpha_2, \cdots, \alpha_t \in Z^+$$

- (1) n 的因数个数为 $(1+\alpha_1)(1+\alpha_2)\cdots(1+\alpha_t)$ 运用乘法定理
- (2) 假设 a,b 有素数分解式
  $a = p_1^{\alpha_1} \cdot \ldots \cdot p_t^{\alpha_t}, \alpha_1, \alpha_2, \cdots, \alpha_t \geqslant 0, b = p_1^{\beta_1} \cdot \ldots \cdot p_t^{\beta_t}, \beta_1, \beta_2, \cdots, \beta_t \geqslant 0,$
  则 $(a, b) = p_1^{min(\alpha_1, \beta_1)} \cdot \ldots \cdot p_t^{min(\alpha_t, \beta_t)}$

证明

证明

$$d_a = p_1^{a_1} \cdot p_2^{a_2} \cdot \dots \cdot p_t^{a_t}, \quad \alpha_1 \geq a_1 \geq 0, \alpha_2 \geq a_2 \geq 0, \dots, \alpha_t \geq a_t \geq 0$$

$$d_b = p_1^{b_1} \cdot p_2^{b_2} \cdot \dots \cdot p_t^{b_t}, \beta_1 \geq b_1 \geq 0, \beta_2 \geq b_2 \geq 0, \dots, \beta_t \geq b_t \geq 0$$

□

很容易看出 $(a, b) = p_1^{min(\alpha_1, \beta_1)} \cdot \dots \cdot p_t^{min(\alpha_t, \beta_t)}$

1.5 最小公倍数

定义 1.4 (最小公倍数) 如果整数 m 分别为整数 $a_1, a_2, \cdots, a_n$ 的倍数，则称 m 为 $a_1, a_2, \cdots, a_n$ 的公倍数，最小的正公倍数叫做 $a_1, a_2, \cdots, a_n$ 的最小公倍数，记作 $[a_1, a_2, \cdots, a_n]$

Properties: 公倍数

- (1) 若 a 与 b 互素（都是正数），则 $[a,b]=ab$

证明

证明　因为 a，b 互素，所以 $ab|[a,b]$，从而 $ab\le[a,b]$，而 ab 本身又是 a 与 b 的公倍数，从而 $[a,b]\le ab$，所以 $[a,b]=ab$ □

- (2) $[a,b]=\frac{ab}{(a,b)}$

证明

证明　由于 $(\frac{a}{(a,b)},\frac{b}{(a,b)})=1$，两个互素的数的最小公倍数是他们的乘积，那么 $[\frac{a}{(a,b)},\frac{b}{(a,b)}]=\frac{a}{(a,b)}\cdot\frac{b}{(a,b)}$, 令 $d=(a,b)$，这说明 $\frac{ab}{d^2}$ 是 $\frac{a}{d}$ 的倍数，也是 $\frac{b}{d}$ 的倍数，从而 $\frac{ab}{d}$ 是 $\frac{a}{d}$ 的倍数，也是 $\frac{b}{d}$ 的倍数，也就是 a 和 b 的公倍数。设 z 也是 a 和 b 的公倍数，那么 $z\ge\frac{ab}{d}$，否则的话 $z<\frac{ab}{d}$ 那么 $\frac{z}{d}<\frac{ab}{d^2}$, 而且 $\frac{z}{d}$ 是 $\frac{a}{d}$ 的倍数，也是 $\frac{b}{d}$ 的倍数，这样 $\frac{z}{d}$ 就是比 $\frac{ab}{d^2}$ 更小的 $\frac{a}{d},\frac{b}{d}$ 的公倍数，这是不可能的，所以 $[a,b]=\frac{ab}{d}=\frac{ab}{(a,b)}$ □

- (3) m 是 a 和 b 的公倍数，则 $[a,b]|m$

证明

证明　设 $d=(a,b)$, 因为 $a|m,b|m\Rightarrow\frac{a}{d}|\frac{m}{d},\frac{b}{d}|\frac{m}{d}$, 由于 $\frac{a}{d}$ 与 $\frac{b}{d}$ 互素，所以 $(\frac{a}{d}\cdot\frac{b}{d})|\frac{m}{d}$, 所以 $\frac{ab}{d}|m$，所以 $[a,b]|m$ □

推论 1.2 $a_1\,|m,a_2|\,m,\ldots,a_n\,|m\Longrightarrow[a_1,a_2,\ldots,a_n]|\,m$

- (4) 假设 a,b 有素数分解式
$a=p_1^{\alpha_1}\cdot\ldots\cdot p_t^{\alpha_t},\alpha_1,\alpha_2,\cdots,\alpha_t\geqslant0,b=p_1^{\beta_1}\cdot\ldots\cdot p_t^{\beta_t},\beta_1,\beta_2,\cdots,\beta_t\geqslant0,$
则 $[a,b]=p_1^{max(\alpha_1,\beta_1)}\cdot\ldots\cdot p_t^{max(\alpha_t,\beta_t)}$

推论 1.3 $\forall a,b\in\mathbb{Z}^+,\exists a'\,|a,b'|\,b,(a',b')=1,s.t.,a'\cdot b'=[a,b]$

证明

证明　设 a，b 的素数分解为

$$
\begin{aligned}
a &= p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}, \quad \alpha_1, \alpha_2, \ldots, \alpha_s \geq 0 \\
b &= p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_s^{\beta_s}, \quad \beta_1, \beta_2, \ldots, \beta_s \geq 0
\end{aligned}
$$

对其中素数 $p_1, p_2 \ldots p_s$ 重新排列，使得

□

1.6　一次不定方程

定义 1.5 (一次不定方程) 形如

$$a_1x_1 + a_2x_2 + \ldots + a_mx_m = n$$

其中 $a_1, a_2, \cdots, a_m, n \in \mathrm{Z}$ 的方程称为 m 元一次不定方程

定理 1.4 二元一次方程 $a_1x_1 + a_2x_2 = n$ 有整数解 $\Leftrightarrow (a_1, a_2)|n$

且有解时，全部解可以表示为 $x = x_0 + a_2t, y = y_0 - a_1t$，其中 x_0, y_0 为任意一组解，t 为任意整数。

2 同余

2.1 同余

定义 2.1 m 是一个正整数，a、b 是任意两个整数，如果 m 整除 a-b：

$$m|(a-b)$$

则称 a 与 b 模 m 同余，记作 $a \equiv b(\mod m)$

Properties: 同余

- (1)
$$\left.\begin{aligned} ad \equiv bd \mod m \\ (d,m)=1 \end{aligned}\right\} \Rightarrow a \equiv b \mod m$$
- (2)
$$\left.\begin{aligned} a \equiv b \mod m_1 \\ a \equiv b \mod m_2 \\ \cdots \\ a \equiv b \mod m_k \end{aligned}\right\} \Rightarrow a \equiv b \mod [m_1, m_2, \cdots, m_k]$$
- (3)
$$\left. a \equiv b \mod m d|a,b,m \right\} \Rightarrow \frac{a}{d} \equiv \frac{b}{d} \mod \frac{m}{d}$$
- (4)$\forall 0 \leqslant i \in Z, a \equiv b \mod m \Rightarrow a^i \equiv b^i \mod m$
- $a \equiv b \mod m \Rightarrow (a,m) = (b,m)$

2.2 剩余类

定义 2.2 (剩余类) 剩余类：称

$$C_a = \{c | c \equiv a \mod m, c \in Z\}$$

为模 m 的 a 的剩余类。C_a 的任意元素称为这个类的剩余或代表元

定义 2.3 (完全剩余系) 完全剩余系：如果

$$r_0, r_1, \ldots, r_{m-1} \in Z$$

且它们模 m 两两不同余，则称

$$\{r_0, r_1, \ldots, r_{m-1}\}$$

为模 m 的一个完全剩余系

$\{0, 1, 2, 3, \ldots, m-1\}$ 是模 m 的最小非负完全剩余系；$\{1, 2, 3, \ldots, m\}$ 是模 m 的最小正剩余系

定义 2.4 (简化剩余类) 如果一个模 m 的完全剩余类中有元素与 m 互素，则这个剩余类被称为简化剩余类

定义 2.5 (简化剩余) 在模 m 的所有简化剩余类中各取一个元素构成的集合叫做模 m 的简化剩余

1,2,3,...,m-1 中与 m 互素的整数全踢构成的集合称为模 m 的最小简化剩余系

定理 2.1 (wilson 定理) p 是素数，则 $(p-1)! \equiv -1 \mod p$

2.3 欧拉函数

Properties: 欧拉函数的性质

- (1)$(m, n) = 1 \Rightarrow \varphi(mn) = \varphi(m)\varphi(n)$
- (2) 正整数 n 的标准分解式为

$$n = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$$

$$\varphi(n) = n \cdot (1 - \frac{1}{p_1}) \cdot \ldots \cdot (1 - \frac{1}{p_s})$$

- (3) $n \in Z^+, \sum_{d|n} \varphi(d) = n$

定理 2.2 (欧拉定理) $1 < m \in Z, (a, m) = 1 \Rightarrow a^{\varphi(m)} \equiv 1 \mod m$

定理 2.3 (费马定理) p 是素数，$a^p \equiv a \mod p$

2.4 模指数计算

也就是常说的快速幂算法

3 同余方程

3.1 基本概念

定义 3.1 (同余式) $m \in \mathrm{Z}^+$, 称

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \equiv 0 \mod m$$

为模 m 同余式，其中系数均为整数
把所有对模 m 两两不同余的同余式的解得个数称为该同余式的解数

定理 3.1 (一次同余式) $m \in \mathrm{Z}^+, m \not| a, d = (a, m)$, 则 $ax \equiv b \mod m$ 有解 $\Leftrightarrow d|b$. 且当这个一次同余式有解的话, 解数必为 d

定义 3.2 (逆元) $m \in \mathrm{Z}^+$，$a \in \mathrm{Z}$，如果存在 $a' \in \mathrm{Z}$ 使得

$$aa' \equiv 1 \mod m$$

成立，则称 a 为模 m 可逆元，称 a' 为 a 的模 m 可逆元，记作 $a^{-1}(\mod m)$

推论 3.1 a 是模 m 的简化剩余 $\Leftrightarrow a$ 是模 m 的可逆元

3.2 中国剩余定理

定理 3.2 (孙子定理) 两两互素的 $m_1, m_2, \ldots, m_k in Z^+, b_1, b_2, \ldots, b_k \in Z$, 则下面的同余式组有解且解唯一 (在模的意义下)

$$\begin{cases} x \equiv b_1 \mod m_1 \\ x \equiv b_2 \mod m_2 \\ \cdots \\ x \equiv b_k \mod m_k \end{cases}$$

解为

$$x \equiv M_1' M_1 b_1 + \cdots + M_k' M_k b_k \mod M$$

其中 $M = m_1 \cdot \ldots \cdot m_k, M_i = \frac{M}{m_i}, M_i' M_i \equiv 1 \mod m_i$

3.3 同余方程式的恒等变形

3.4 高次同余式

定义 3.3 为了求解方程 $f(x) \equiv 0 \mod p^{\alpha}$ 已知 $f(c) \equiv 0 \mod p^{\alpha-1}, d = p^{\alpha-1}$, 设解为 $kd + c$, 则 $f'(c)p^{\alpha-1} \cdot k \equiv -f(c) \mod p^{\alpha}$ 等价于

$$f'(c) \cdot k \equiv \frac{-f(c)}{p^{\alpha-1}} \mod p$$

定理 3.3 设 $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, 设 $x = a_1 mod p$ 是同余方程 $f(x) \equiv 0 \mod p$ 的解, 则存在 *n-1* 次的首项系数为 a_n 的多项式 $f_1(x)$ 使得对任意的整数 x 都有: $f(x) \equiv (x - a_1)f_1(x) \mod p$

定理 3.4 次数为 n 的同余方程，它的解数最多为 n

定理 3.5 设 $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0, n \leqslant p, x^p - x = f(x)q(x) + r(x)$(*r(x)* 的次数 <*n*，首项系数为 *1* 的 *q(x)* 的次数 =*p-n*)，则 $f(x) \equiv 0 \mod p$ 有 n 个解 ⇔*r(x)* 的系数都是 p 的倍数

Properties

- (1) 任一模 p 的同余方程一定与一个次数不超过 p-1 的模 p 同余方程等价；
- (2) 这个模 p 的次数不超过 p-1(比如记为 n) 的同余方程的解数至多为它的次数 n；
- (3) 这个模 p 的次数为 n(<p) 的同余方程的解数为 n 的充要条件为 $x^p - x$ 被它除后所得余式的系数都是 p 的倍数

4 同余方程

4.1 模为素数的二次同余方程-解得存在性

定理 4.1 考虑二次同余方程 $ay^2 + by + c \equiv 0 \mod p$ 等价于 $(2ay + b)^2 \equiv (b^2 - 4ac) \mod p$ 这样，我们就一般考虑形如：

$$x^2 \equiv a \mod p$$

定义 4.1 (二次剩余) 设素数 p>2，如果 $x^2 \equiv a \mod p$ 有解，则称 a 是一个模 p 的平凡剩余（二次剩余），否则，称 a 是一个模 p 的平方非剩余（二次非剩余）.

定理 4.2 在模 p 的一个简化剩余系中，恰有 $\frac{p-1}{2}$ 个模 p 二次剩余，恰有 $\frac{p-1}{2}$ 个模 p 二次非剩余：如果 a 是模 p 二次剩余的话，$x^2 \equiv a \mod p((a,p)=1)$ 的解数为 2

定理 4.3 (欧拉判别条件) a 是模 p 的平方剩余 $a^{\frac{p-1}{2}} \equiv 1 \mod p$
a 是模 p 的非平方剩余 $a^{\frac{p-1}{2}} \equiv -1 \mod p$

4.2 勒让德符号

定义 4.2 (勒让德符号) 设 p 是素数，定义

$$(\frac{a}{p}) = \begin{cases} 1 \text{ 如果 } a \text{ 是模 } p \text{ 的平方剩余} \\ -1 \text{ 如果 } a \text{ 是模 } p \text{ 的平方非剩余} \\ 0 \text{ 如果} p|a \end{cases}$$

Properties

- $(1)(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$
- $(2)(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$
- $(3)(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$
- 二次互反律：p，q 都是奇素数，$(\frac{q}{p})(\frac{p}{q}) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$

4.3 雅克比符号

定义 4.3 m 是奇素数的乘积，$m = p_1 \dots p_s, \forall a \in Z,$

$$(\frac{a}{m}) \triangleq (\frac{a}{p_1}) \cdot \dots \cdot (\frac{a}{p_s})$$

Properties

- (1)$(\frac{a+m}{m}) = (\frac{a}{m})$
- (2)$(\frac{ab}{m}) = (\frac{a}{m})(\frac{b}{m})$
- (3)$(\frac{-1}{m}) = (-1)^{\frac{m-1}{2}}$
- (4)$(\frac{2}{m}) = (-1)^{\frac{m^2-1}{8}}$
- (5) 雅克比符号的互反律：$(\frac{n}{m})(\frac{m}{n}) = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}$

4.4 模素数的二次同余方程求解

4.5 模为合数的二次同余方程

定理 4.4 *方程* $x^2 \equiv a \mod p^\alpha$（$a$ *与* p *互素，*p *为奇素数*）*的判定与求解：*$x^2 \equiv a \mod p^\alpha$ *有解* $\Leftrightarrow a$ *为模* p *的二次剩余. 且有解的话，解数为 2*

定理 4.5 *方程* $x^2 \equiv a \mod 2^\delta$ *判定：*

(1) 如果 $\delta = 2$

$$x^2 \equiv a \mod 4\text{有解} \Leftrightarrow a \equiv 1 \mod 4$$

如果有解，则解数为 2

(2) 如果 $\delta \geqslant 3$

$$x^2 \equiv a \mod 2^\delta\text{有解} \Leftrightarrow a \equiv 1 \mod 8$$

如果有解，则解数为 4

5 组合数学

定义 5.1 (拉丁方) 若 A 是由 n 个元素构成的 n 阶方阵，其中每个元素在每行每列各出现一次, 则称 A 是拉丁方. 一个简单 3 阶拉丁方如下图所示：

$$\begin{matrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{matrix}$$

定义 5.2 (正交拉丁方) 设 $A = (a_{ij})_{n*n}, B = (b_{ij})_{n*n}$ 是两个 $n*n$ 拉丁方. 令 $C = ((a_{ij}, b_{ij}))_{n*n}$, 若 C 的 n^2 对数偶互不相同, 则称 A 与 B 正交。3 阶正交拉丁方如下图所示

$$A = \begin{bmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{bmatrix} B = \begin{bmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \end{bmatrix} \quad C = \begin{bmatrix} (0,0) & (1,1) & (2,2) \\ (1,2) & (2,0) & (0,1) \\ (2,1) & (0,2) & (1,0) \end{bmatrix}$$

> **Tip** 正交的拉丁方的一个应用: 药物配合试验三种治发烧药和三种治感冒药, 对三位病人试验, 要求三天内每人都服这几种药, 比较配合疗效. 这时就可用上面讨论过的 3 阶正交拉丁方.

6 鸽巢原理

定理 6.1 (鸽巢原理) *若有 n 个鸽巢, n+1 只鸽子, 则至少有一个鸽巢里至少有两只鸽子.*

定理 6.2 (中国剩余定理不互素的情况) *设 m,n 是正整数, $0 \le a < m, 0 \le b < n$, 则方程组, $\begin{cases} x \equiv a \mod m \\ x \equiv b \mod n \end{cases}$ 有解当且仅当 $gcd(m,n)|(b-a)$. 若 $d|(b-a)$, 那么存在唯一解:*

$$x \equiv a + cm[(b-a)/d] \mod M$$

.

定理 6.3 (Erdös-Szekeres 定理) *在由 n^2+1 个实数构成的序列中, 必然含有长为 $n+1$ 的单调 (增或减) 子序列.*

7 排列与组合

定义 7.1 (多重集) 多重集: 可以重复, 没有次序，比如 $\{a,b,b\}=\{b,a,b\}\neq\{a,b\}$. 多重集的记法

$$M=\{a,a,a,b,c,c,d,d,d,d\}:=\{3\cdot a,b,2\cdot c,4\cdot d\}$$

$$N=\{\infty\cdot a,2\cdot b,\infty\cdot c,4\cdot d\}$$

定义 7.2 (排列数与组合数) 用 $P(n,r)$ 表示 n 元素集合的 r-排列的个数, 用 $C(n,r)$ 表示 n 元素集合的 r-组合的个数. 通常记 $C(n,r)$ 为 $\begin{pmatrix}\boldsymbol{n}\\\boldsymbol{r}\end{pmatrix}$

定理 7.1

$$0\leq r\leq n, P(n,r)=n!/(n-r)!$$

$$0rn, C(n,r)=n!/(n-r)!/r!$$

$$C(n,r)=C(n,n-r).$$

$$C(n,0)+C(n,1)+\cdots+C(n,n)=2^n$$

定理 7.2 设 $S=\{\infty\cdot a_1,\infty\cdot a_2,\ldots,\infty\cdot a_k\},r\geq 0$, 则 S 的 r-排列个数是 k^r ,S 的 r-组合个数是 $C(r+k-1,r)$.

定理 7.3 设 $S=\{n_1\cdot a_1,n_2\cdot a_2,\ldots,n_k\cdot a_k\},r\geq 0$, 且 $|S|=n_1+n_2+\cdots+n_k=n$, 则 S 的全排列个数为

$$\frac{n!}{n_1!n_2!\ldots n_k!}$$

8 生成排列和组合

9 容斥原理及其应用

定理 9.1 (容斥原理) $|A \cup B| = |A| + |B| - |A \cap B|$

定理 9.2 (容斥原理) 设 $A_1, A_2, \ldots, A_n$ 是 U 中的有限集合, 则

$$\begin{aligned}
&|\mathbf{A}_1^c \cap \mathbf{A}_2^c \cap \ldots \cap \mathbf{A}_\mathrm{n}^c| \\
=&|\boldsymbol{U}| - \sum_{i=1}^{n} |A_i| + \sum_{\mathrm{ti} \in j \leqslant n} \left|A_i \cap A_j\right| \\
&- \sum_{\mathrm{i} \leq i \leq j < k < n} \left|A_i \cap A_j \cap A_k\right| - \cdots \\
&+ (-1)^\mathrm{n} \, |\boldsymbol{A}_1 \cap \boldsymbol{A}_2 \cap \ldots \cap \boldsymbol{A}_\mathrm{n}|
\end{aligned}$$

定义 9.1 (错位排序) 若 $S = 1, 2, \ldots, n$ 的排列 $i_1 i_2 \ldots i_n$ 满足 $i_1 \neq 1, i_2 \neq 2, \ldots, i_n \neq n$, 则称它为 n 元素的错位排列. 以 D_n 记 n 元素的错位排列数.

定理 9.3 $D_n = n![1 - 1/1! + 1/2! - 1/3! + \cdots + (-1)/n!]$

定理 9.4 $D_n = (n-1)D_{n-1} + (n-1)D_{n-2}$

10 递推关系和生成函数

定义 10.1 对于序列 $h_0, h_1, \ldots$, 若存在 $a_1, a_2, \ldots, a_k, b_n$, (可能依赖于 n, a k 0) 使得对任意 $n \geq k$, $h_n = a_1 h_{n-1} + a_2 h_{n-2} + \cdots + a_k h_{n-k} + b_n$, 则称该序列满足 k 阶线性递推关系. 若其中 b $n = 0$, 则称之为齐次的. 若 $a_1, a_2, \ldots, a_k$ 为常数, 则称为常系数的.