标题

作者： Autin

目录

第 1 章 同余式

1.1 一次同余式

定理 1.1

$$ax \equiv b \pmod{m}, \quad a \not\equiv 0 \pmod{m}$$

当且仅当 $(a,m) \mid b$，此时解数为 $d=(a,m)$ ♡

解一次同余式的算法：

1. 找最大公因子 $d=(a,m)$；
2. a,b,m 除以 d，化作系数和模数互素的情况。

$$a_1 x \equiv b_1 \pmod{m_1}, \quad (a_1,m_1)=1$$

3. 找到同余式

$$a_1 x \equiv 1 \pmod{m_1}$$

的解 c。

(a). 矩阵行变换形式的辗转相除法；

(b). 欧拉定理

$$c = a_1^{\varphi(m_1)-1}$$

4. 两边乘以 c，得到解

$$x \equiv b_1 c \pmod{m_1}$$

为模 m_1 意义下的唯一解。

5. 所有解为

$$b_1 c + k \cdot m_1 \pmod{m}, \quad k=0,1,\cdots,d-1$$

1.2 孙子定理

定理 1.2 (CRT)

设 $m_1,\cdots,m_k$ 是 k 个两两互素的正整数，令

$$m = m_1 \cdots m_k, \quad m = m_i M_i, \quad i=1,\cdots,k,$$

则同余式组

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ \vdots \\ x \equiv b_k \pmod{m_k} \end{cases}$$

在 $\bmod m$ 意义下的唯一解是

$$x \equiv M_1' M_1 b_1 + \cdots + M_k' M_k b_k \pmod{m}$$

其中

$$M_i' M_i \equiv 1 \pmod{m_i}, i = 1, \cdots, k$$

♡

定理 1.3

若 $b_1, \cdots, b_k$ 过模 $m_1, \cdots, m_k$ 的完全剩余系，则

$$M_1' M_1 b_1 + \cdots + M_k' M_k b_k$$

过模 m 的完全剩余系。

♡

Remark 给出寻找合数模的完全剩余系的方法，只需要做素因子分解，给出每个准素数的完全剩余系，并找出系数 $M_i' M_i$，拼成模 m 的完全剩余系。

1.3 高次同余式

定理 1.4 (合数模变为准素模)

若 $m_1, \cdots, m_k$ 是 k 个两两互素的正整数，令 $m = m_1 m_2 \cdots m_k$，则

$$f(x) \equiv 0 \pmod{m} \iff f(x) \equiv 0 \pmod{m_i}, i = 1, \cdots, k$$

模 m 解的个数为模 m_i 解的个数的乘积。

♡

定理 1.5 (准素模变为素数模)

设 p 是素数。若 $x \equiv x_1 \pmod{p}$ 是 $f(x) \equiv 0 \pmod{p}$ 的一个解，并且 $p \nmid f'(x_1)$，则存在 $\bmod p^\alpha$ 下唯一的 x_α，使得 $x_\alpha \equiv x_1 \pmod{p}$，且 $x \equiv x_\alpha \pmod{p^\alpha}$ 成为 $f(x) \equiv 0 \pmod{p^\alpha}$ 的一个解。

♡

准素数模同余式的算法：对于同余式 $f(x) \equiv 0 \pmod{p^\alpha}$

1. 求同余式

$$f(x) \equiv 0 \pmod{p}$$

的一个解 x_1，使得 $p \nmid f'(x_1)$

2. 寻找 t_1，使得

$$f(x_1 + pt_1) \equiv 0 \pmod{p^2}$$

为此，将左式泰勒展开，得到

$$f(x_1) + pt_1 f'(x_1) \equiv 0 \pmod{p^2}$$

解一次同余式，得到唯一解 $t_1 \equiv t_1' \pmod{p^2}$。
令 $x_2 := x_1 + pt_1'$，则 $x \equiv x_2 \pmod{p^2}$ 是 $f(x) \equiv 0 \pmod{p^2}$ 的一个解。

3. 重复上述操作，对于以上过程中得到的 $f(x) \equiv 0 \pmod{p^{\alpha-1}}$ 的解 $x \equiv x_{\alpha-1} \pmod{p^{\alpha-1}}$ 。
寻找 $t_{\alpha-1}$，使得

$$f\left(x_{\alpha-1} + p^{\alpha-1} t_{\alpha-1}\right) \equiv 0 \pmod{p^{\alpha}}$$

为此，Taylor 展开得到

$$f(x_{\alpha-1}) + p^{\alpha-1} t_{\alpha-1} f'(x_{\alpha-1}) \equiv 0 \pmod{p^{\alpha}}$$

解一次同余式，得到唯一解 $t_{\alpha-1} \equiv t_{\alpha-1}' \pmod{p^{\alpha}}$。
令 $x_{\alpha} := x_{\alpha-1} + t_{\alpha-1}' p^{\alpha-1}$ ，则 $x \equiv x_{\alpha} \pmod{p^{\alpha}}$ 为同余式 $f(x) \equiv 0 \pmod{p^{\alpha}}$ 的一个解。

1.4 素数模的同余式

考虑素数模 p 的同余式

$$f(x) \equiv 0 \pmod{p}, \quad f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$$

其中 p 是素数，$a_n \not\equiv 0 \pmod{p}$

定理 1.6

上述同余式与一个次数不超过 $p-1$ 的模 p 的同余式等价。 ♡

定理 1.7

设 $k \leq n$，$x \equiv \alpha_i \pmod{p}$ $(1, \cdots, k)$ 是素数模同余式的 k 个不同的解，则对于任意的整数 x，我们有

$$f(x) \equiv (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_k) f_k(x) \pmod{p}$$

其中 f_k 是首项系数为 a_n 的 $n-k$ 次多项式。 ♡

定理 1.8

1.

$$x^{p-1}-1\equiv(x-1)(x-2)\cdots(x-(p-1))\pmod{p}$$

2.

$$(p-1)!+1\equiv 0\pmod{p}$$

♡

定理 1.9

若 $n\leq p$，同余式

$$f(x)\equiv 0\pmod{p},\quad f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_0$$

有 n 个解当且仅当 $f(x)$ 除 x^p-x 所得余式的一切系数都是 p 的倍数。

♡

第 2 章 二次同余式

2.1 一般二次同余式的化简

定义 2.1

二次同余式是指

$$ax^2+bx+c\equiv 0\,(\mathrm{mod}\ m)\,,\quad a\not\equiv 0\,(\mathrm{mod}\ m)$$

♣

需要讨论二次同余式什么时候有解。

第一步，将 m 标准分解，化简为每个准素数模的同余式是否有解的问题

定理 2.1

设 m 的标准分解是 $m=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$，则上述二次同余式有解，当且仅当下列每个同余式都有解

$$ax^2+bx+c\equiv 0\,(\mathrm{mod}\ p_i^{\alpha_i})\,,\quad i=1,\cdots,k$$

♡

接下来讨论准素数模同余式何时有解，

定理 2.2

对于二次同余式

$$f(x)\equiv 0\,(\mathrm{mod}\ p^{\alpha})\,,\quad f(x)=ax^2+bx+c$$

1. 当 $p^{\alpha}\mid (a,b,c)$ 时，任意整数满足同余式，进而有解；
2. 若 p^{α} 不整除 (a,b,c)，不妨只考虑 $p\nmid (a,b,c)$ 的情况[a]
   (a). 若 $p\mid a, p\mid b, p\nmid c$，无解。
   (b). 若 $p\mid a, p\nmid b$，

[a]可以让 (a,b,c) 除尽 p，直到 $p\nmid (a,b,c)$，化简为新的形如上的二次同余式。

♡

2.2 奇素数的平方剩余与非剩余

只讨论奇素数 p 的平方剩余与非剩余，即讨论

$$x^2\equiv a\,(\mathrm{mod}\ p)\,,\quad (a,p)=1$$

的同余式的解。

定理 2.3 (欧拉判别)

若 $(a,p)=1$，p 是奇素数，则 a 是模 p 的平方剩余，当且仅当

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

非剩余当且仅当

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

若为平方剩余，则 $x^2 \equiv a \pmod{p}$ 恰有二解。 ♡

定理 2.4

模 p 的既约剩余系有 $p-1$（偶数）个，其中平方剩余与非剩余各占一半，有 $\frac{p-1}{2}$ 个。

其中的平方剩余在同余的意义下与

$$1^2, 2^2, \cdots, \left(\frac{p-1}{2}\right)^2$$

一一对应。 ♡

2.3 利用勒让德符号判定

定理 2.5 (勒让德符号)

设 p 是奇素数，定义勒让德符号 $\left(\frac{a}{p}\right)$ 按

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

♡

命题 2.1 (勒让德符号的运算性质)

1. 若 $a \equiv a_1 \pmod{p}$，则

$$\left(\frac{a}{p}\right) = \left(\frac{a_1}{p}\right)$$

2.

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$$

3.
$$\left(\frac{a_1a_2\cdots a_n}{p}\right)=\left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right)\cdots\left(\frac{a_n}{p}\right)$$

4.
$$\left(\frac{ab^2}{p}\right)=\left(\frac{a}{p}\right),\quad p\nmid b$$

5.
$$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$$

6. 若 $(a,p)=1$ 且 $2\nmid a$，则
$$\left(\frac{a}{p}\right)=(-1)^{\sum_{k=1}^{p_1}[\frac{ak}{p}]},\quad p_1=\frac{p-1}{2}$$

7. 若 p,q 是奇素数，$(p,q)=1$，则
$$\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{p}{q}\right)$$

♠

2.4 雅可比符号

引入以下雅可比符号，可以更方便地计算勒让德符号

定义 2.2

对于奇数 m，定义雅可比符号 $\left(\frac{a}{m}\right)$，按
$$\left(\frac{a}{m}\right):=\left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_r}\right)$$
其中 $m=p_1p_2\cdots p_r$，p_i 是素数，$\left(\frac{a}{p_i}\right)$ 是勒让德符号。

♣

命题 2.2

1. 若 $a\equiv a_1\pmod m$，则
$$\left(\frac{a}{m}\right)=\left(\frac{a_1}{m}\right)$$

2.
$$\left(\frac{-1}{m}\right)\equiv -1^{\frac{m-1}{2}}\pmod m$$

3.

$$\left(\frac{a_1 a_2 \cdots a_n}{m}\right) = \left(\frac{a_1}{m}\right)\left(\frac{a_2}{m}\right)\cdots\left(\frac{a_n}{m}\right)$$

4.

$$\left(\frac{ab^2}{m}\right) = \left(\frac{a}{m}\right), \quad (b, m) = 1$$

5.

$$\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}}$$

6. 若 m, n 是大于 1 的奇数，则

$$\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}\left(\frac{m}{n}\right)$$

♠

✍ **练习 2.1** 判断同余式

$$x^2 \equiv 286 \pmod{563}$$

是否有解。

Solution

$$\begin{aligned}\left(\frac{286}{563}\right) &= \left(\frac{2}{563}\right)\left(\frac{143}{563}\right)\\ &= (-1)(-1)^{\frac{143-1}{2}\cdot\frac{563-1}{2}}\left(\frac{563}{143}\right)\\ &= \left(\frac{-9}{143}\right) = \left(\frac{-1}{143}\right) =\end{aligned}$$

第 3 章 同余

3.1 欧拉定理与费马小定理

定理 3.1 (欧拉)

设 m 是大于 1 的整数，$(a, m) = 1$，则

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

♡

定理 3.2 (费马小定理)

若 p 是素数，则

$$a^p \equiv a \pmod{p}$$

♡

第 4 章 原根和指标

4.1 指数及其基本性质

定义 4.1

若 $m>1,(a,m)=1$，则使得同余式

$$a^{\gamma}\equiv 1\,(\mathrm{mod}\ m)$$

成立的最小正整数 γ 叫做 a 对模 m 的指数。

若 a 对模 m 的指数是 $\varphi(m)$，则 a 叫做模 m 的一个原根。 ♣

定理 4.1

若 a 对模 m 的指数为 δ，则 $1=a^0,a^1,\cdots,a^{\delta-1}$ 对模 m 两两不同余。 ♡

定理 4.2

若 a 对模 m 的指数是 δ，则 $a^{\gamma}=a^{\gamma'}\,(\mathrm{mod}\ m)$ 当且仅当 $\gamma=\gamma'\,(\mathrm{mod}\ \delta)$。

特别地，$a^{\gamma}\equiv 1\,(\mathrm{mod}\ \delta)$ 当且仅当 $\delta\mid\gamma$ 。 ♡

定理 4.3

1. 若 x 对模 m 的指数是 $ab,a>0,b>0$，则 x^a 对模 m 的指数是 b。
2. 若 x 对模 m 的指数是 a，y 对模 m 的指数是 b，且 $(a,b)=1$ ，则 xy 对模 m 的指数是 ab。 ♡

4.2 原根存在条件

定理 4.4

模m的原根存在 $\Longleftrightarrow$ $m=2,4,p^{\alpha},2p^{\alpha},\quad p$是奇素数 ♡

4.3 指标和 n 次剩余

考察同余式

$$x^n\equiv a\,(\mathrm{mod}\ m),\quad (a,m)=1$$

解的存在条件，解的个数，模 m 的原根的个数。

若无特别声明，以下皆设 m 是 p^α 或 $2p^\alpha$，$c=\varphi(m)$，g 是模 m 的一个原根。

定理 4.5

若 γ 过模 c 的最小非负完全剩余系，则 g^γ 过模 m 的一个既约剩余系。 ♡

定义 4.2

设 a 是整数，若对于模 m 的一个原根 g，存在整数 γ，使得

$$a\equiv g^\gamma \pmod m,\quad \gamma\geq 0$$

则称 γ 为以 g 为底的 a 对模 m 的一个指标。 ♣

Remark 可以将指标 γ 看成是 a 以 g 为底的对数，只不过这里 γ 只在模 m 的意义下唯一。

定理 4.6

设 a 是整数使得 $(a,m)=1$，g 是模 m 的一个原根。则存在 γ' 满足 $0\leq\gamma'<c$，是一个 a 的以 g 为底的模 m 的指标。

此外，整数 γ 是 g 为底的 a 的模 m 的指标，当且仅当它满足

$$\gamma\equiv\gamma' \pmod c,\quad \gamma\geq 0$$

此 γ' 记作 $\operatorname{ind}_g a$ 或 $(\operatorname{ind} a)$ ♡

定理 4.7

设 g 是模 m 的一个原根，γ 是一个非负整数。则以 g 为底，对模 m 有同一指标的 γ 的一切指标构成模 m 的一个与模互素的剩余类。 ♡

定理 4.8

设 $a_1,\cdots,a_n$ 是与 m 互素的 n 个整数，则

$$\operatorname{ind}(a_1a_2\cdots a_n)\equiv \operatorname{ind} a_1+\operatorname{ind} a_2+\cdots+\operatorname{ind} a_n \pmod c$$ ♡