2022-2023学年秋季学期

课程名称: 信息安全数学基础

英文名称: Mathematical Foundations for Information Security

授课团队：胡磊、许军、王丽萍

助　　教：郭一

信息安全数学基础

Mathematical Foundations for Information Security

[第 4 次课] 同余式

授课教师：胡磊

授课时间：2022年9月21日

概 要

- 基本概念及一次同余式
- 中国剩余定理
- 高次同余式的解数及解法
- 素数模的同余式

基本概念及一次同余式

定义 1 设 m 正整数，$f(x)$ 多项式 $f(x)=a_nx^n+\cdots+a_1x+a_0$，其中 a_i 是整数，则 $f(x)\equiv 0\pmod m$ (1)

叫做模 m **同余式**. 若 $a_n\not\equiv 0\pmod m$, 则 n 叫做 $f(x)$ 的 **次数**, 记为 $\deg f$. 此时，(1) 式又叫做模 m 的 n **次同余式**.

如果整数 a 使得 $f(a)\equiv 0\pmod m$ 成立，则 a 叫做该 (1) 的**解**.

(1) 的解 a 常写成 $x\equiv a\pmod m$.

在模 m 的完全剩余系中，使得 (1) 成立的 剩余个数叫做同余式 (1) 的 **解数**.

例 1 $x^5+x+1\equiv 0\pmod 7$ 是首项系数为 1 的模 7 同余式.

$x\equiv 2\pmod 7$ 是该同余式的解.

$$2^5+2+1=35=5\cdot 7\equiv 0\pmod 7.$$

还有解 $x\equiv 4\pmod 7$, 解数为2

定理　设a, m是正整数，(a, m)=1, 则有a′，1≤a′<m，使得

$$aa' \equiv 1 \pmod{m}$$

在模m意义下，a′是唯一的，a′称为a模m的逆元。

记$a' = a^{-1}$

定理 1 设 $a \not| m$. 则一次同余式 $ax \equiv b \pmod{m}$ (2) 有解的充要条件是 $(a,m)|b$. 且当 (2) 有解时，其解数为 $d = (a,m)$.

证 必要性. 设 (2) 有解 $x \equiv x_0 \pmod{m}$

$$ax_0 - my_0 = b.$$

因为 $(a,m)|a$, $(a,m)|m$, 所以 $(a,m)|ax_0 - my_0 = b$.

必要性成立.

充分性.

充分性：

考虑：$\frac{a}{(a,m)}x \equiv \frac{b}{(a,m)} \pmod{\frac{m}{(a,m)}}$　因为$(\frac{a}{(a,m)}, \frac{m}{(a,m)}) = 1$

故　$x \equiv x_1 \equiv (\frac{a}{(a,m)})^{-1} \frac{b}{(a,m)} \pmod{\frac{m}{(a,m)}}$

$x \equiv x_1 \equiv (\frac{a}{(a,m)})^{-1} \frac{b}{(a,m)} \pmod{m}$是$ax \equiv b \bmod m$的一个特解。

$ax \equiv b \bmod m$的全部解：

$$x \equiv x_1 + t\frac{m}{(a,m)} \pmod{m}, \quad t = 0,1,\Lambda\ ,(a,m)-1$$

$ax \equiv b \bmod m$的全部解：

$$x \equiv \frac{b}{(a,m)}\left(\frac{a}{(a,m)}\right)^{-1} \bmod \frac{m}{(a,m)} + t\frac{m}{(a,m)} \pmod{m},$$

$t = 0,1,\Lambda\ ,(a,m)-1$

事实上，如果同时有 $ax \equiv b \pmod{m}$ 和 $ax_1 \equiv b \pmod{m}$

$a(x - x_1) \equiv 0 \pmod{m}$ $x \equiv x_1 \pmod{\frac{m}{(a,m)}}$.

因此, ***ax≡b* mod*m*的全部解可写成上述形式。证毕。**

例 2 求解一次同余式 $33x \equiv 22 \pmod{77}$.

计算 $(33, 77) = 11$, 且有 $(33, 77) = 11|22$, 故原同余式有解.

写出同余式 $3x \equiv 2 \pmod{7}$的一个特解 $x_0 \equiv 2 \cdot x_0' \equiv 2 \cdot 5 \equiv 3 \pmod{7}$.

原同余式的全部解

$$x \equiv 3 + t\frac{77}{(33, 77)} \equiv 3 + 7t \pmod{77}, \qquad t = 0,\ 1, \ldots,\ 10.$$

或者

$$x \equiv 3,\ 10,\ 17,\ 24,\ 31,\ 38,\ 45,\ 52,\ 59,\ 66,\ 73 \pmod{77}.$$

定理 3 设 $(a,m)|b$. 则一次同余式 $ax \equiv b \pmod{m}$ 的全部解为

$$x \equiv \frac{b}{(a,m)} \cdot \left(\left(\frac{a}{(a,m)} \right)^{-1} \pmod{\frac{m}{(a,m)}} \right) + t\frac{m}{(a,m)} \pmod{m},$$

$t = 0,\ 1, \ldots,\ (a,m) - 1.$

中国剩余定理

关于中国剩余定理或孙子定理，其最早见于《孙子算经》的“物不知数”题：
今有物不知其数，三三数之有二，五五数之有三，七七数之有二，问物有多少？
答案：二十三.

将“物不知数”问题用同余式组表示就是：

$$\begin{cases} x \equiv 2 \pmod 3, \\ x \equiv 3 \pmod 5, \\ x \equiv 2 \pmod 7. \end{cases}$$

定理 1 (中国剩余定理) 设 $m_1, \ldots, m_k$ 是 k 个两两互素 的正整数. 则对任意的整数 $b_1, \ldots, b_k$, 同余式组

$$\begin{cases} x \equiv b_1 \pmod{m_1}, \\ \cdots\cdots \\ x \equiv b_k \pmod{m_k}. \end{cases} \tag{1}$$

一定有解，且解是惟一的. 事实上，

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

则同余式组 (1) 的解可表示为

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

其中 $M_i' M_i \equiv 1 \pmod{m_i}, \ i = 1, 2, \ldots, k.$

证 （1）存在性

（2）唯一性

秦九韶：大衍总数术

例 1 求解同余式组
$$\begin{cases} x \equiv b_1 \pmod 5, \\ x \equiv b_2 \pmod 6, \\ x \equiv b_3 \pmod 7, \\ x \equiv b_4 \pmod{11}. \end{cases}$$

解 令 $m = 5 \cdot 6 \cdot 7 \cdot 11 = 2310,$

$$M_1 = 6 \cdot 7 \cdot 11 = 462, \quad M_2 = 5 \cdot 7 \cdot 11 = 385,$$
$$M_3 = 5 \cdot 6 \cdot 11 = 330, \quad M_4 = 5 \cdot 6 \cdot 7 = 210.$$

分别求解同余式 $M_i' M_i \equiv 1 \pmod{m_i}, \quad i = 1, 2, 3, 4.$

得到 $M_1' = 3, \quad M_2' = 1, \quad M_3' = 1, \quad M_4' = 1.$

故同余式组的解为

$$x \equiv 3 \cdot 462 \cdot b_1 + 385 \cdot b_2 + 330 \cdot b_3 + 210 \cdot b_4 \pmod{2310}.$$

例 3 计算 $2^{1000000} \pmod{77}$.

解一 利用 Euler 定理及模重复平方计算法直接计算.

因为 $\varphi(77) = \varphi(7)\varphi(11) = 60$, 所以 $2^{60} \equiv 1 \pmod{77}$. 又 $1000000 = 16666 \cdot 60 + 40$, 所以 $2^{1000000} = (2^{60})^{16666} \cdot 2^{40} \equiv 2^{40} \pmod{77}$. 设 $m = 77,\ b = 2$. 令 $a = 1$. $40 = 2^3 + 2^5$.

1). $n_0 = 0$. 计算 $a_0 = a \equiv 1, \quad b_1 \equiv b^2 \equiv 4 \pmod{77}$.

2). $n_1 = 0$. 计算 $a_1 = a_0 \equiv 1, \quad b_2 \equiv b_1^2 \equiv 16 \pmod{77}$.

3). $n_2 = 0$. 计算 $a_2 = a_1 \equiv 1, \quad b_3 \equiv b_2^2 \equiv 25 \pmod{77}$.

4). $n_3 = 1$. 计算 $a_3 = a_2 \cdot b_3 \equiv 25, \quad b_4 \equiv b_3^2 \equiv 9 \pmod{77}$

5). $n_4 = 0$. 计算 $a_4 = a_3 \equiv 25, \quad b_5 \equiv b_4^2 \equiv 4 \pmod{77}$.

6). $n_5 = 1$. 计算 $a_5 = a_4 \cdot b_5 \equiv 23 \pmod{77}$.

最后，计算出 $2^{1000000} \equiv 23 \pmod{77}$.

解二 令 $x = 2^{1000000}$. 因为 $77 = 7 \cdot 11$, 所以计算 $x \pmod{77}$ 等价于求解同余式组 $\begin{cases} x \equiv b_1 \pmod 7 \\ x \equiv b_2 \pmod{11}. \end{cases}$

因为 Euler 定理给出 $2^{\varphi(7)} \equiv 2^6 \equiv 1 \pmod 7$, 以及 $1000000 = 166666 \cdot 6 + 4$, 所以 $b_1 \equiv 2^{1000000} \equiv (2^6)^{166666} \cdot 2^4 \equiv 2 \pmod 7$.

类似地，因为 $2^{\varphi(11)} \equiv 2^{10} \equiv 1 \pmod{11}$, $\quad 1000000 = 100000 \cdot 10$, 所以 $b_2 \equiv 2^{1000000} \equiv (2^{10})^{100000} \equiv 1 \pmod{11}$.

令 $m_1 = 7,\ m_2 = 11,\ m = m_1 \cdot m_2 = 77$, $M_1 = m_2 = 11, \quad M_2 = m_1 = 7$, 分别求解同余式 $11M_1' \equiv 1 \pmod 7, \quad 7M_2' \equiv 1 \pmod{11}$.

得到 $M_1' = 2, \quad M_2' = 8$. 故

$$x \equiv 2 \cdot 11 \cdot 2 + 8 \cdot 7 \cdot 1 \equiv 100 \equiv 23 \pmod{77}.$$

因此, $\quad 2^{1000000} \equiv 23 \pmod{77}$.

定理 2 在定理 1 的条件下, 若 $b_1, \ldots, b_k$ 分别遍历模 $m_1, \ldots, m_k$ 的完全剩余系, 则 $x \equiv M_1'M_1b_1 + \cdots + M_k'M_kb_k \pmod{m}$ 遍历模 $m = m_1 \cdots m_k$ 的完全剩余系.

证 令 $x_0 = M_1'M_1b_1 + \cdots + M_k'M_kb_k \pmod{m}$, 则当 $b_1, \ldots, b_k$ 分别遍历模 $m_1, \ldots, m_k$ 的完全剩余系时, x_0 遍历 $m_1 \cdots m_k$ 个数. 如果能够证明它们模 m 两两不同余, 则定理成立. 事实上, 若 $M_1'M_1b_1 + \cdots + M_k'M_kb_k \equiv M_1'M_1b_1' + \cdots + M_k'M_kb_k' \pmod{m}$,

则根据 §2.1 定理 11, $M_i'M_ib_i \equiv M_i'M_ib_i' \pmod{m_i}, \quad i = 1, \ldots, k.$ 因为 $M_i'M_i \equiv 1 \pmod{m_i}, \quad i = 1, \ldots, k$, 所以, $b_i \equiv b_i' \pmod{m_i}, \ i = 1, \ldots, k.$ 但 $b_i, \ b_i'$ 是同一个完全剩余系中的两个数, 故

$$b_i = b_i', \quad i = 1, \ldots, k.$$

定理成立.

Pohig-Hellman：计算离散对数的CRT方法

- n阶循环群上的离散对数。若n有素因子分解

$$n = q_1 q_2 \cdots q_r$$

  每个 q_i 为素数方幂
- Know g and $x = g^a$， want to find exponent a
- 利用$x^{n/q_i} = (g^{n/q_i})^a$, 求出$a \bmod q_i$
  （进一步，这个问题先用$X^{n/p_i} = g^{a\ n/p_i}$求出$a \bmod p_i$，再用下面第三节方法解决）
- 利用$a \bmod q_1$、$a \bmod q_2$、…、$a \bmod q_r$，求出$a \bmod n$
- 不能用光滑阶群上的离散对数

RSA解密的CRT方法

- n=pq，解密指数d与n同等规模
- 要计算$m = c^d$ （mod n）　　（*）
- 计算$d_p = d$（mod p-1），d_p 比 d的规模缩小一半
- 计算$m_p = c^{d_p}$（mod p），计算量为（*） 的1/8
- 计算$m_q = c^{d_q}$（mod q）
- 由 $m=m_p$（mod p）和$m=m_q$（mod q）计算m（mod n），计算量为（*） 的1/4

RSA正确解密的条件

- 要计算$m^{ed-1} = 1$（mod n）
- 需要 $m^{ed-1} = 1$（mod p）和 $m^{ed-1} = 1$（mod q）
- 需要 ed-1 = 0（mod p-1）和 ed-1 = 0（mod q-1）
- 充分必要条件：

  需要 ed = 1 （ mod lcm(p-1 q-1) ）
- 充分条件：ed = 1 （ mod (p-1)(q-1) ）

第三节　高次同余式的解数及解法

定理1　设$m_1, \ldots, m_k$是两两互素的正整数,$m=m_1 \ldots m_k$,则

$$f(x)\equiv 0(\mathrm{mod}\ m) \Leftrightarrow \begin{cases} f(x)\equiv 0(\mathrm{mod}\ m_1) & \text{解数为}T_1 \\ \Lambda\ \Lambda\ \Lambda \\ f(x)\equiv 0(\mathrm{mod}\ m_k) & \text{解数为}T_k \end{cases}$$

解数为T

则$T = T_1 \Lambda\ T_k$。

证

$$f(x_0)\equiv 0(\mathrm{mod}\ m) \Rightarrow f(x_0)\equiv 0(\mathrm{mod}\ m_i), \quad i=1,\Lambda\ ,k$$

$$f(x_0)\equiv 0(\mathrm{mod}\ m) \Leftarrow f(x_0)\equiv 0(\mathrm{mod}\ m_i), \quad i=1,\Lambda\ ,k$$

定理1 设$m_1, \ldots, m_k$是两两互素的正整数,$m = m_1 \ldots m_k$,则

$$f(x) \equiv 0 \pmod{m} \Leftrightarrow \begin{cases} f(x) \equiv 0 \pmod{m_1} & \text{解数为} T_1 \\ \cdots\cdots\cdots \\ f(x) \equiv 0 \pmod{m_k} & \text{解数为} T_k \end{cases}$$

解数为T

设 $f(x) \equiv 0 \pmod{m_i}$ 的解是 $b_i,\ i = 1, \ldots, k.$ 则同余式组

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

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

因为 $f(x) \equiv f(b_i) \equiv 0 \pmod{m_i},\quad i = 1, \ldots, k,$ 所以 x 也是 $f(x) \equiv 0 \pmod{m}$ 的解. 故 x 随 b_i 遍历 $f(x) \equiv 0 \pmod{m_i}$ 的所有解 $(i = 1, \ldots, k,)$ 而遍历 $f(x) \equiv 0 \pmod{m}$ 的所有解. 即

$$T = T_1 \cdots T_k.$$

例 1 解同余式 $f(x) \equiv x^4 + 2x^3 + 8x + 9 \equiv 0 \pmod{35}$.

解 原同余式等价于同余式组 $\begin{cases} f(x) \equiv 0 \pmod 5, \\ f(x) \equiv 0 \pmod 7. \end{cases}$

直接验算，$f(x) \equiv 0 \pmod 5$ 的解为 $x \equiv 1,\ 4 \pmod 5$,

$f(x) \equiv 0 \pmod 7$ 的解为 $x \equiv 3,\ 5,\ 6 \pmod 7$.

根据中国剩余定理，可求得同余式组 $\begin{cases} x \equiv b_1 \pmod 5 \\ x \equiv b_2 \pmod 7 \end{cases}$

的解为 $x \equiv 3 \cdot 7 \cdot b_1 + 3 \cdot 5 \cdot b_2 \pmod{35}$.

故原同余式的解为 $x \equiv 31,\ 26,\ 6,\ 24, 19,\ 34 \pmod{35}$

共 $2 \cdot 3 = 6$ 个.

定理1 设$m_1, \ldots, m_k$ 是两两互素的正整数,$m= m_1 \ldots m_k$, 则

$$f(x) \equiv 0 \pmod m \Leftrightarrow \begin{cases} f(x) \equiv 0 \pmod{m_1} & \text{解数为} T_1 \\ \cdots\cdots \\ f(x) \equiv 0 \pmod{m_k} & \text{解数为} T_k \end{cases}$$

则 $T=T_1 T_2 \cdots T_k$

$m=p_1\text{^}\{\alpha_1\}\cdots p_k\text{^}\{\alpha_k\}$

$$f(x) \equiv 0 \pmod m \Leftrightarrow \begin{cases} f(x) \equiv 0 \pmod{p_1^{\alpha_1}} \Leftarrow f(x) \equiv 0 \pmod{p_1} \\ \cdots\cdots \\ f(x) \equiv 0 \pmod{p_k^{\alpha_k}} \Leftarrow f(x) \equiv 0 \pmod{p_k} \end{cases}$$

因为 $m = \pi_p p^\alpha$, 所以要求解同余式 $f(x) \equiv 0 \pmod m$, 只须求解同余式 $f(x) \equiv 0 \pmod{p^\alpha}$.

我们讨论 p 为素数时, $f(x) \equiv 0 \pmod{p^\alpha}$ (3) 的解法.

设 $f(x) = a_n x^n + \cdots + a_2 x^2 + a_1 x + a_0$;

$$f'(x) = n a_n x^{n-1} + \cdots + 2a_2 x + a_1.$$

称 $f'(x)$ 为 $f(x)$ 的 **导式**.

定理 2 设 $x \equiv x_1 \pmod p$ 是 $f(x) \equiv 0 \pmod p$ 的一个解, $(f'(x_1), p) = 1$

则 $f(x) \equiv 0 \pmod{p^\alpha}$ 有解 $x \equiv x_\alpha \pmod{p^\alpha}$,

其中 x_α 由下面关系式递归得到:

$$\begin{cases} x_i \equiv x_{i-1} + p^{i-1} t_{i-1} \pmod{p^i}, \\ \qquad\qquad\qquad\qquad\qquad\qquad i = 2, \ldots, \alpha. \\ t_{i-1} \equiv -\dfrac{f(x_{i-1})}{p^{i-1}} (f'(x_1)^{-1} \pmod p) \pmod p, \end{cases}$$

证 我们对 $\alpha \geq 2$ 作数学归纳法:

(i) $\alpha = 2$. $\quad x = x_1 + pt_1, \qquad t_1 = 0,\ \pm 1,\ \pm 2,\ \ldots,$

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

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

因为 $f(x_1) \equiv 0 \pmod{p}$, 所以 $\quad t_1 f'(x_1) \equiv -\dfrac{f(x_1)}{p} \pmod{p}.$

因为 $(f'(x_1), p) = 1, \quad t_1 \equiv -\dfrac{f(x_1)}{p}(f'(x_1)^{-1} \pmod{p}) \pmod{p}.$

即 $x \equiv x_2 \equiv x_1 + pt_1 \pmod{p^2}$ 是同余式 $f(x) \equiv 0 \pmod{p^2}$ 的解.

(ii) 设 $3 \le i \le \alpha$. 假设定理对 $i-1$ 成立, 即同余式 $f(x) \equiv 0 \pmod{p^{i-1}}$ 有解 $x = x_{i-1} + p^{i-1}t_{i-1}$, $\quad t_{i-1} = 0,\ \pm 1,\ \pm 2,\ \ldots.$

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

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

因为 $f(x_{i-1}) \equiv 0 \pmod{p^{i-1}}$, 所以 $t_{i-1}f'(x_{i-1}) \equiv -\frac{f(x_{i-1})}{p^{i-1}} \pmod{p}$.

又因为 $f'(x_{i-1}) \equiv f'(x_{i-2}) \equiv \cdots \equiv f'(x_1) \pmod{p}$

$$(f'(x_{i-1}), p) = \cdots = (f'(x_1), p) = 1$$

$$t_{i-1} \equiv -\frac{f(x_{i-1})}{p^{i-1}}(f'(x_{i-1})^{-1} \pmod{p}) \equiv -\frac{f(x_{i-1})}{p^{i-1}}(f'(x_1)^{-1} \pmod{p}) \pmod{p}$$

即 $x \equiv x_i \equiv x_{i-1} + p^{i-1}t_{i-1} \pmod{p^i}$ 是 $f(x) \equiv 0 \pmod{p^i}$ 的解.

定理对所有 $2 \le i \le \alpha$ 成立. 特别, 定理对 $i = \alpha$ 成立. 证毕.

定理 2 设 $x \equiv x_1 \pmod{p}$ 是 $f(x) \equiv 0 \pmod{p}$ 的一个解, $(f'(x_1), p) = 1$

则 $f(x) \equiv 0 \pmod{p^\alpha}$ 有解 $x \equiv x_\alpha \pmod{p^\alpha}$,

其中 x_α 由下面关系式递归得到:

$$\begin{cases} x_i \equiv x_{i-1} + p^{i-1} t_{i-1} \pmod{p^i}, \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad i = 2, \ldots, \alpha. \\ t_{i-1} \equiv -\dfrac{f(x_{i-1})}{p^{i-1}} (f'(x_1)^{-1} \pmod{p}) \pmod{p}, \end{cases}$$

性质

设$f(x)$是n次多项式。

- $f(x+yp^i) \equiv f(x)(\mod p^i)$.
- 设$x_0(\mod p)$是$f(x) \equiv 0(\mod p)$的一个根。则$f'(x_0) \not\equiv 0(\mod p) \Leftrightarrow x_0(\mod p)$是$f(x) \equiv 0(\mod p)$的一个单根。

p-adic 求解法：$x = x_0 + x_1 p + x_2 p^2 + \cdots$。依次求出$x_0, x_1, x_2, \cdots$。

记$x_i' = x_0 + x_1 p + x_2 p^2 + \cdots + x_{i-1} p^{i-1}$。

方法

- 若$x_0(\mod p)$是$f(x)\equiv 0(\mod p)$的一个单根，则$f(x)\equiv 0(\mod p^i)$有唯一的模p同余于x_0的一个模p^i根，这个根可迭代计算。

- 若$x_0(\mod p)$是$f(x)\equiv 0(\mod p)$的一个重根，$f(x_i')\equiv 0(\mod p^i)$且$x_i'\equiv x_0(\mod p)$，则$f(x)\equiv 0(\mod p^{i+1})$存在模$p^i$同余于$x_i'$的一个模$p^{i+1}$根$\Leftrightarrow f(x_i')\equiv 0(\mod p^{i+1})$。当这个条件成立时，这些解为$x_{i+1}'=x_i'+x_ip^i$，$x_i$为任意整数。

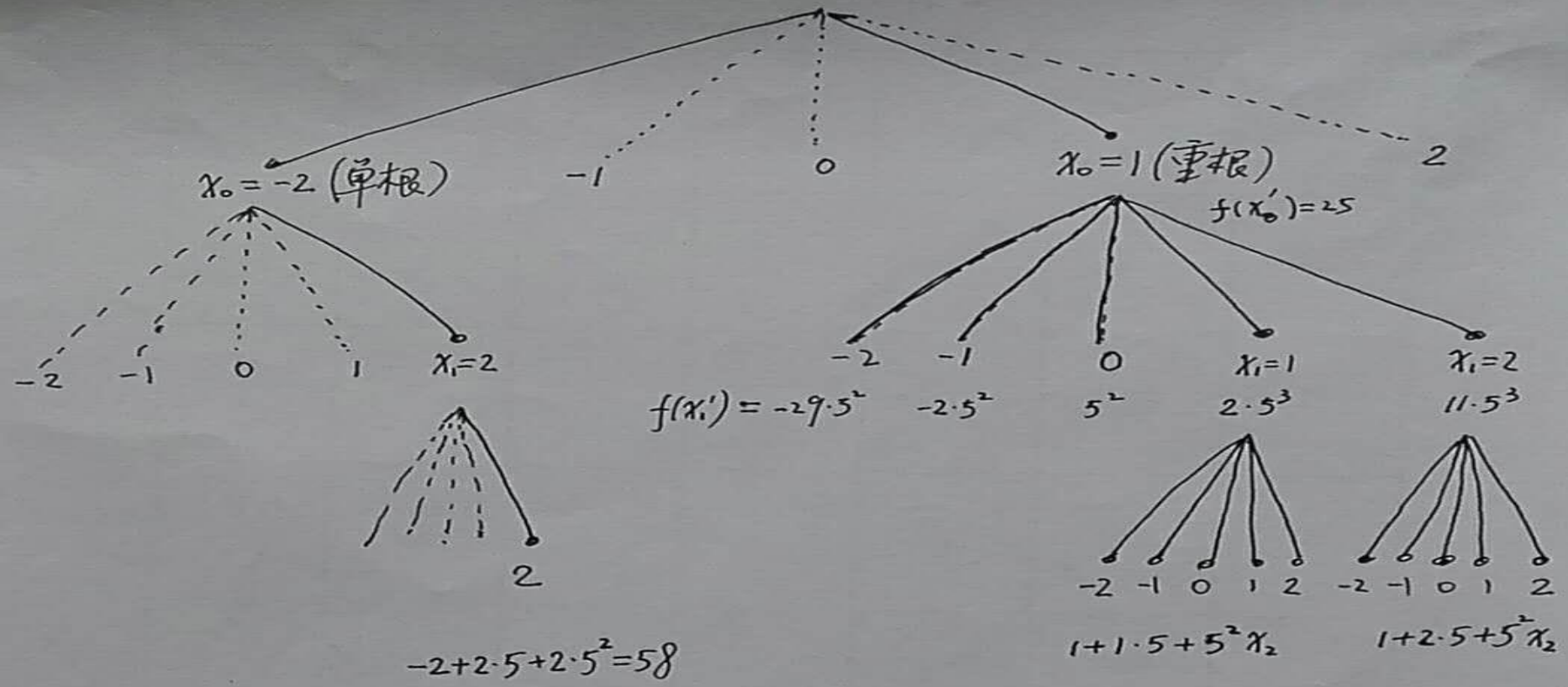
证明：$f(x_i'+x_ip^i)\equiv f(x_i')+f'(x_i')x_ip^i(\mod p^{i+1})$

p叉树

*p*叉树

例：$f(x)=x^3+2x+22\equiv 0(\mod 5^3).$

$f(x)\equiv x^3+2x+2\equiv (x-1)^2(x+2)(\mod 5).$


$x_0=-2$ (単根)
-1
0
$x_0=1$ (重根)
2
$f(x_0')=25$
-2
-1
0
1
$x_1=2$
-2
-1
0
$x_1=1$
$x_1=2$
$f(x_1')=-29\cdot5^2$
$-2\cdot5^2$
5^2
$2\cdot5^3$
$11\cdot5^3$
2
-2 -1 0 1 2
-2 -1 0 1 2
$-2+2\cdot5+2\cdot5^2=58$
$1+1\cdot5+5^2x_2$
$1+2\cdot5+5^2x_2$

Pohig-Hellman：计算离散对数的CRT方法

- n阶循环群上的离散对数。若

$$n = p^s$$

- Know g and $x = g^a$， want to find exponent a
- Write the p-adic expression of a
- 利用$x^{n/p} = (g^{n/p})^a$， 求出a mod p

- 不能用光滑阶群上的离散对数

模p同余式的解数不超过p和其次数

考虑 $f(x) = a_n x^n + \cdots + a_1 x + a_0 \equiv 0 \pmod{p}$ 其中 $p \nmid a_n$.

引理 (多项式欧几里得除法) 设 $f(x) = a_n x^n + \cdots + a_1 x + a_0$ 为 n 次整系数多项式， $g(x) = x^m + \cdots + b_1 x + b_0$ 为 $m \geq 1$ 次首一整系数多项式，则存在整系数多项式 $q(x)$ 和 $r(x)$ 使得

$$f(x) = g(x)q(x) + r(x), \quad \deg r(x) < \deg g(x).$$

定理 1 同余式 $f(x) = a_n x^n + \cdots + a_1 x + a_0 \equiv 0 \pmod{p}$

与一个次数不超过 $p-1$ 模 p 同余式等价.

证 由欧几里得除法，存在 $q(x)$, $r(x)$ 使得 $f(x) = (x^p - x)q(x) + r(x)$, 其中 $\deg r(x) \leq p-1$. 又对任何整数 x, 都有 $x^p - x \equiv 0 \pmod{p}$.

故同余式 $f(x) \equiv 0 \pmod{p}$ 等价于同余式 $r(x) \equiv 0 \pmod{p}$.

- **r(x) 模p是零多项式，p个模p解**
- **r(x) 模p是非零多项式，下证不超过deg r(x)个模p解**

例 1 求与同余式 $3x^{14} + 4x^{13} + 2x^{11} + x^9 + x^6 + x^3 + 12x^2 + x \equiv 0 \pmod{5}$ 等价的次数 < 5 的同余式.

解 作多项式的欧几里得除法，我们有

$$\begin{aligned} & 3x^{14} + 4x^{13} + 2x^{11} + x^9 + x^6 + x^3 + 12x^2 + x \\ = & (x^5 - x)(3x^9 + 4x^8 + 2x^6 + 3x^5 + 5x^4 + 2x^2 + 4x + 5) \\ & + 3x^3 + 16x^2 + 6x. \end{aligned}$$

所以原同余式等价于 $3x^3 + 16x^2 + 6x \equiv 0 \pmod{5}$.

定理 2 设 $1 \le k \le n$. 如果 $x \equiv a_i \pmod p$ 是 $f(x) = a_n x^n + \cdots + a_1 x + a_0 \equiv 0 \pmod p$ 的 k 个不同解，则对任何整数 x, 都有

$$f(x) \equiv (x-a_1)\cdots(x-a_k) f_k(x) \pmod p, \qquad (2)$$

其中 $f_k(x)$ 是 $n-k$ 次多项式，首项系数是 a_n.

证 由多项式的欧几里得除法，存在多项式 $f_1(x)$ 和 $r(x)$ 使得

$$f(x) = (x-a_1) f_1(x) + r(x), \qquad \deg r(x) < \deg(x-a_1).$$

易知, $\deg f_1(x) = n-1$, 首项系数是 a_n, $r(x) = r$ 为整数. 因为 $f(a_1) \equiv 0 \pmod p$, 所以 $r \equiv 0 \pmod p$. 即有 $f(x) \equiv (x-a_1) f_1(x) \pmod p$.

再由 $f(a_i) \equiv 0 \pmod p$ 及 $a_i \not\equiv a_1 \pmod p$, 得到 $f_1(a_i) \equiv 0 \pmod p$, $i = 2, \ldots, k$.

类似地

$$\begin{cases} f_1(x) \equiv (x-a_2) f_2(x) \pmod p, \\ f_2(a_i) \equiv 0 \pmod p, \quad i = 3, \ldots, k. \end{cases}$$

$$\cdots\cdots\cdots\cdots$$

$$f_{k-1}(x) \equiv (x-a_k) f_k(x) \pmod p$$

故 $f(x) \equiv (x-a_1)\cdots(x-a_k) f_k(x) \pmod p$.

定理 4 同余式 $f(x)=a_nx^n+\cdots+a_1x+a_0\equiv 0\ (\mathrm{mod}\ p)\qquad p\not| a_n.$

的解数不超过它的次数.

证 反证法. 设 (1) 式的解数超过 n 个，则 (1) 式至少有 $n+1$ 个解. 设它们为 $x\equiv a_i\ (\mathrm{mod}\ p),\quad i=1,\ldots,n,n+1.$

对于 n 个解 $a_1,\ \ldots,\ a_n$, 可得到 $f(x)\equiv(x-a_1)\cdots(x-a_n)f_n(x)\ (\mathrm{mod}\ p).$

$$f(a_{n+1})\ \equiv\ 0\ (\mathrm{mod}\ p),\ (a_{n+1}-a_1)\cdots(a_{n+1}-a_n)f_n(a_{n+1})\ \equiv 0\ (\mathrm{mod}\ p).$$

$$f_n(a_{n+1})\equiv 0\ (\mathrm{mod}\ p).$$

但 $f_n(x)$ 是首项系数为 a_n, 次数为 $n-n=0$ 的多项式.

故 $p|a_n$. 矛盾.

推论 次数 $<p$ 的整系数多项式对所有整数取值模 p 为零的充要条件是其系数被 p 整除.

Q&A