初等数论
第三章 同余方程

中山大学 数据科学与计算机学院

求解一次同余式$ax \equiv b \bmod m$的基本步骤

- 计算$d = (a, m)$;
- 判断是否$d \mid b$, 如果不是则无解;如果整除的话:
- 计算$\frac{a}{d}, \frac{b}{d}, \frac{m}{d}$, 即$\frac{a}{d}$模$\frac{m}{d}$的乘法逆; 和使得$s \cdot \frac{a}{d} + t \cdot \frac{m}{d} = 1$的$s$;
- 写出全部的解

$$x \equiv s \cdot \frac{b}{d} + k \cdot \frac{m}{d} \bmod m, \quad (k = 0, 1, 2, \cdots, d-1)$$

中国剩余定理

两两互素的$m_1, m_2, \ldots, m_k \in \mathbb{Z}^+, b_1, b_2, \ldots, b_k \in \mathbb{Z}$, 则下面的一次同余方程组有解, 且解在模$m_1 m_2 \cdots m_k$的意义下唯一:

$$\begin{cases} x \equiv b_1 \bmod m_1 \\ x \equiv b_2 \bmod m_2 \\ \ldots\ldots \\ x \equiv b_k \bmod m_k \end{cases}$$

其解可以如下表示: 令

$$M = m_1 \cdot m_2 \cdot \ldots \cdot m_k, \quad M_1 = \frac{M}{m_1}, M_2 = \frac{M}{m_2}, \ldots, M_k = \frac{M}{m_k}$$

$$M_1' M_1 \equiv 1 \bmod m_1, M_2' M_2 \equiv 1 \bmod m_2, \ldots, M_k' M_k \equiv 1 \bmod m_k$$

解为

$$x \equiv M_1' M_1 b_1 + M_2' M_2 b_2 + \ldots + M_k' M_k b_k \bmod M$$

定理

设$m_1, m_2, \ldots, m_k$两两互素, $b_1, b_2, \ldots, b_k$分别遍历模$m_1, m_2, \ldots, m_k$的完全剩余系，则

$$x \equiv M_1' M_1 b_1 + M_2' M_2 b_2 + \ldots + M_k' M_k b_k \bmod M$$

遍历M的完全剩余系, 其中

$$M = m_1 \cdot m_2 \cdot \ldots \cdot m_k, \quad M_1 = \frac{M}{m_1}, M_2 = \frac{M}{m_2}, \ldots, M_k = \frac{M}{m_k},$$

$$M_1' M_1 \equiv 1 \bmod m_1, M_2' M_2 \equiv 1 \bmod m_2, \ldots, M_k' M_k \equiv 1 \bmod m_k.$$

定理

设$m_1, m_2, \ldots, m_k$两两互素, $M = m_1 \cdot m_2 \cdot \ldots \cdot m_k$, $0 \leq b < m$, 则存在唯一的一组整数$b_1, b_2, \ldots, b_k$, $0 \leq b_i < m_i$, $1 \leq i \leq k$, 使得

$$M_1' M_1 b_1 + M_2' M_2 b_2 + \ldots + M_k' M_k b_k \equiv b(\bmod M),$$

其中

$$M_1 = \frac{M}{m_1}, M_2 = \frac{M}{m_2}, \ldots, M_k = \frac{M}{m_k},$$

$$M_1' M_1 \equiv 1 \bmod m_1, M_2' M_2 \equiv 1 \bmod m_2, \ldots, M_k' M_k \equiv 1 \bmod m_k.$$

进一步, $(b, m) = 1$当且仅当$(b_i, m_i) = 1$, $1 \leq i \leq k$.

$$b_i \equiv b(\mathrm{mod} m_i) \Longrightarrow b = qm_i + b_i \Longrightarrow (b_i, m_i) = (b, m_i) = 1, 1 \leq i \leq k$$

中国剩余定理的应用

如果给定的整数x是一个很大的数字, 要求计算它模M后的值, 可以将M分解成两两互素的$m_1, m_2, \ldots, m_k$之后, 计算x模m_1后的值记为b_1, 计算x模m_2后的值记为b_2, $\ldots$, 计算x模m_k后的值记为b_k, 从而建立一个一次同余方程组

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

求解这个一次同余式组的解即可得到x模M后的值.

3. 高次同余方程的求解

高次同余方程求解的基本思路：

1. 同余方程规约：$f(x)(\mathrm{mod}m) \rightharpoonup f(x)(\mathrm{mod}p^{\alpha}) \rightharpoonup f(x)(\mathrm{mod}p)$.
2. 判断解的存在性.
3. 确定解的个数.
4. 进行模运算求解.

为了求解同余方程需要利用同余的性质对同余方程进行变形, 或者说同余方程规约, 即把要求解的同余方程变为解完全相同的另一个同余方程, 并保证两个同余方程是等价的, 而后者更易于求解.

(3-1) 设$s(x)$是任一整系数多项式, 则

$$f(x) \equiv 0 \bmod m \iff f(x)+ms(x) \equiv 0 \bmod m$$

这个结论显然成立:
因为$\forall x_0 \in \mathbb{Z}$:

$$\because ms(x_0) \equiv 0 \bmod m, \quad f(x_0) \equiv f(x_0) \bmod m$$

$$\therefore f(x_0) + ms(x_0) \equiv f(x_0) \bmod m$$

$$\therefore f(x_0) + ms(x_0) \equiv 0 \bmod m \iff f(x_0) \equiv 0 \bmod m$$

这表明: 整数x_0使得$f(x_0) \equiv 0 \bmod m$当且仅当x_0使得$f(x_0) + ms(x_0) \equiv 0 \bmod m$.
整数x是方程$f(x) \equiv 0 \bmod m$的解当且仅当它是方程$f(x) + ms(x) \equiv 0 \bmod m$的解.

例如, $4x^2 - 3x + 3 \equiv 0 \bmod 15 \iff 4x^2 - 3x + 3 + 15(x - 1) \equiv 0 \bmod 15$, 即, 同余方程$4x^2 - 3x + 3 \equiv 0 \bmod 15$和同余方程$4x^2 + 12x - 12 \equiv 0 \bmod 15$等价.

特别地, 一个同余方程中系数为模的倍数的项去掉后, 同余方程的解不变: 比如同余方程$15x^8 + 7x^6 + 45x^3 - 30x + 6 \equiv 0 \bmod 15$可以化简为$7x^6 + 6 \equiv 0 \bmod 15$.

(3-2) 设$s(x)$是整系数多项式.
同余方程$f(x) \equiv 0 \bmod m$与$f(x) + s(x) \equiv s(x) \bmod m$等价, 即解完全相同:

$$f(x) \equiv 0 \bmod m \iff f(x) + s(x) \equiv s(x) \bmod m$$

这个结论显然成立:
因为$\forall x_0 \in \mathbb{Z}$:

$$\because s(x_0) \equiv s(x_0) \bmod m$$

$$f(x_0) \equiv 0 \bmod m \iff f(x_0) + s(x_0) \equiv s(x_0) \bmod m$$

这表明: 整数x_0使得$f(x_0) \equiv 0 \bmod m$当且仅当x_0使得$f(x_0) + s(x_0) \equiv s(x_0) \bmod m$.
也就是说, 整数x是$f(x) \equiv 0 \bmod m$的解当且仅当它是$f(x) + s(x) \equiv s(x) \bmod m$的解.

例如, $4x^2 + 27x - 12 \equiv 0 \bmod 15 \iff 4x^2 + 27x \equiv 12 \bmod 15$.
同余方程$ax - b \equiv 0 \bmod m$和同于方程$ax \equiv b \bmod m$等价.

(3-3) 设$(a,m)=1$.
同余方程$f(x)\equiv 0 \bmod m$与同余方程$af(x)\equiv 0 \bmod m$等价, 即解完全相同:

$$f(x)\equiv 0 \bmod m \iff af(x)\equiv 0 \bmod m$$

因为a与m互素, 所以对$\forall x_0\in\mathbb{Z}$有$m|f(x_0) \iff m|af(x_0)$成立, 即

$$f(x_0)\equiv 0 \bmod m \iff af(x_0)\equiv 0 \bmod m$$

这表明: 整数x_0使得$f(x_0)\equiv 0 \bmod m$当且仅当x_0使得$af(x_0)\equiv 0 \bmod m$.
也就是说, 整数x是$f(x)\equiv 0 \bmod m$的解当且仅当它是$af(x)\equiv 0 \bmod m$的解.
例如, $4x^2+12x-12\equiv 0 \bmod 15 \iff x^2+3x-3\equiv 0 \bmod 15$;

一般地, 如果$(a_n,m)=1$, 则同余方程$a_nx^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0\equiv 0 \bmod m$
与同余方程

$$x^n+a_n^{-1}a_{n-1}x^{n-1}+\ldots+a_n^{-1}a_1x+a_n^{-1}a_0\equiv 0 \bmod m$$

等价.
例如, 同余方程$7x^6+6\equiv 0 \bmod 15$与$x^6+3\equiv 0 \bmod 15$等价.

(3-3) 设$(a,m)=1$.
同余方程$f(x)\equiv 0 \bmod m$与同余方程$af(x)\equiv 0 \bmod m$等价, 即解完全相同:

$$f(x)\equiv 0 \bmod m \iff af(x)\equiv 0 \bmod m$$

因为a与m互素, 所以对$\forall x_0\in\mathbb{Z}$有$m|f(x_0) \iff m|af(x_0)$成立, 即

$$f(x_0)\equiv 0 \bmod m \iff af(x_0)\equiv 0 \bmod m$$

这表明: 整数x_0使得$f(x_0)\equiv 0 \bmod m$当且仅当x_0使得$af(x_0)\equiv 0 \bmod m$.
也就是说, 整数x是$f(x)\equiv 0 \bmod m$的解当且仅当它是$af(x)\equiv 0 \bmod m$的解.
例如, $4x^2+12x-12\equiv 0 \bmod 15 \iff x^2+3x-3\equiv 0 \bmod 15$;

一般地, 如果$(a_n,m)=1$, 则同余方程$a_nx^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0\equiv 0 \bmod m$
与同余方程

$$x^n+a_n^{-1}a_{n-1}x^{n-1}+\ldots+a_n^{-1}a_1x+a_n^{-1}a_0\equiv 0 \bmod m$$

等价.
例如, 同余方程$7x^6+6\equiv 0 \bmod 15$与$x^6+3\equiv 0 \bmod 15$等价.
这是因为7模15的乘法逆是$13(\mathrm{mod}15)$, 而$(13\cdot 6)\equiv 3(\mathrm{mod}15)$.

(3-4) 设同余方程$h(x) \equiv 0 \bmod m$有m个解, 即任意整数带入此同余方程都成立. 这样的同余方程可以称之为模m的同余恒等式, 例如$x^p - x \equiv 0 \bmod p$.

设$h(x) \equiv 0 \bmod m$是同余恒等式. 如果有整系数多项式$q(x)$, $r(x)$使得$f(x) = q(x)h(x) + r(x)$, 则同余方程$f(x) \equiv 0 \bmod m$等价于$r(x) \equiv 0 \bmod m$.
因为对满足$f(x_0) = q(x_0)h(x_0) + r(x_0)$的所有整数$x_0$都有

$$f(x_0) \equiv 0 \bmod m \iff q(x_0)h(x_0) + r(x_0) \equiv 0 \bmod m \iff r(x_0) \equiv 0 \bmod m$$

这个表明: 整数x_0使得$f(x_0) \equiv 0 \bmod m$当且仅当x_0使得$r(x_0) \equiv 0 \bmod m$.
也就是说, 整数x是$f(x) \equiv 0 \bmod m$的解当且仅当它是$r(x) \equiv 0 \bmod m$的解.

例如:

$$2x^7 - x^5 - 3x^3 + 6x + 1 \equiv 0 \bmod 5 \iff x^3 \equiv 1 \bmod 5.$$

(3-4) 设同余方程$h(x) \equiv 0 \bmod m$有m个解, 即任意整数带入此同余方程都成立. 这样的同余方程可以称之为模m的同余恒等式, 例如$x^p - x \equiv 0 \bmod p$.

设$h(x) \equiv 0 \bmod m$是同余恒等式. 如果有整系数多项式$q(x)$, $r(x)$使得$f(x) = q(x)h(x) + r(x)$, 则同余方程$f(x) \equiv 0 \bmod m$等价于$r(x) \equiv 0 \bmod m$.
因为对满足$f(x_0) = q(x_0)h(x_0) + r(x_0)$的所有整数$x_0$都有

$$f(x_0) \equiv 0 \bmod m \iff q(x_0)h(x_0) + r(x_0) \equiv 0 \bmod m \iff r(x_0) \equiv 0 \bmod m$$

这个表明: 整数x_0使得$f(x_0) \equiv 0 \bmod m$当且仅当x_0使得$r(x_0) \equiv 0 \bmod m$.
也就是说, 整数x是$f(x) \equiv 0 \bmod m$的解当且仅当它是$r(x) \equiv 0 \bmod m$的解.

例如:

$$2x^7 - x^5 - 3x^3 + 6x + 1 \equiv 0 \bmod 5 \iff x^3 \equiv 1 \bmod 5.$$

这是因为$f(x) = 2x^7 - x^5 - 3x^3 + 6x + 1 = (2x^2 - 1)(x^5 - x) + (-x^3 + 5x + 1)$,
且$x^5 - x \equiv 0 \bmod 5$对任意整数都成立.
进一步, 同余方程$-x^3 + 5x + 1 \equiv 0 \bmod 5$与同余方程$-x^3 + 1 \equiv 0 \bmod 5$等价.
而同余方程$-x^3 + 1 \equiv 0 \bmod 5$与同余方程$x^3 \equiv 1 \bmod 5$等价.

类似于数的整除中欧几里德除法, 对于多项式也有多项式的欧几里德除法:
整系数多项式

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$$

和

$$g(x) = x^m + b_{m-1} x^{m-1} + \ldots + b_1 x + b_0,$$

存在整系数多项式$q(x)$和$r(x)$使得$f(x) = g(x)q(x) + r(x)$, 且$\deg(r(x)) < \deg(g(x))$.

可以看到, 如果$g(x)$的次数m比$f(x)$的次数n大, 直接取$q(x) = 0$, $r(x) = f(x)$,
则$f(x) = g(x) \cdot 0 + f(x)$即满足要求.

类似于数的整除中欧几里德除法, 对于多项式也有多项式的欧几里德除法.

如果f的次数比g的大:

$$
\begin{array}{r}
x^4 \\
x^3-x^2+3x-3 \;\overline{)\; x^7-x} \\
\underline{-\quad x^7-x^6+3x^5-3x^4} \\
x^6-3x^5+3x^4-x
\end{array}
$$

即$x^7 - x = (x^3 - x^2 + 3x - 3)(x^4) + (x^6 - 3x^5 + 3x^4 - x)$

类似于数的整除中欧几里德除法, 对于多项式也有多项式的欧几里德除法.

如果f的次数比g的大:

$$
\begin{array}{r|l}
 & x^4+x^3 \\
\hline
x^3-x^2+3x-3 & x^7-x \\
 & \underline{-\ x^7-x^6+3x^5-3x^4} \\
 & \quad x^6-3x^5+3x^4-x \\
 & \underline{-\ x^6-x^5+3x^4-3x^3} \\
 & \quad -2x^5+3x^3-x
\end{array}
$$

即$x^7 - x = (x^3 - x^2 + 3x - 3)(x^4 + x^3) + (-2x^5 + 3x^3 - x)$

类似于数的整除中欧几里德除法, 对于多项式也有多项式的欧几里德除法.

如果f的次数比g的大:

$$
\begin{array}{r|l}
 & x^4+x^3-2x^2 \\
\cline{2-2}
x^3-x^2+3x-3 & x^7-x \\
\multicolumn{2}{r}{\underline{-\ x^7-x^6+3x^5-3x^4}} \\
\multicolumn{2}{r}{x^6-3x^5+3x^4-x} \\
\multicolumn{2}{r}{\underline{-\ x^6-x^5+3x^4-3x^3}} \\
\multicolumn{2}{r}{-2x^5+3x^3-x} \\
\multicolumn{2}{r}{\underline{-\ -2x^5+2x^4-6x^3+6x^2}} \\
\multicolumn{2}{r}{-2x^4+9x^3-6x^2-x}
\end{array}
$$

即$x^7 - x = (x^3 - x^2 + 3x - 3)(x^4 + x^3 - 2x^2) + (-2x^4 + 9x^3 - 6x^2 - x)$

类似于数的整除中欧几里德除法, 对于多项式也有多项式的欧几里德除法.

如果f的次数比g的大:

$$
\begin{array}{r|l}
 & x^4+x^3-2x^2-2x+7 \\
\cline{2-2}
x^3-x^2+3x-3 & x^7-x \\
 & \underline{-\ x^7-x^6+3x^5-3x^4} \\
 & x^6-3x^5+3x^4-x \\
 & \underline{-\ x^6-x^5+3x^4-3x^3} \\
 & -2x^5+3x^3-x \\
 & \underline{-\ -2x^5+2x^4-6x^3+6x^2} \\
 & -2x^4+9x^3-6x^2-x \\
 & \underline{-\ -2x^4+2x^3-6x^2+6x} \\
 & 7x^3-6x-x \\
 & \underline{-\ 7x^3-7x^2+21x-21} \\
 & 7x^2-28x+21
\end{array}
$$

即$x^7 - x = (x^3 - x^2 + 3x - 3)(x^4 + x^3 - 2x^2 - 2x + 7) + (7x^2 - 28x + 21)$

(3-5) 设d是m的正因子.
同余方程$f(x) \equiv 0 \bmod m$有解的必要条件是同余方程$f(x) \equiv 0 \bmod d$有解,
即$f(x) \equiv 0 \bmod m$有解$\Longrightarrow f(x) \equiv 0 \bmod d$有解.

如果存在整数x_0使得$f(x_0) \equiv 0 \bmod m$成立, 从而对整数x_0, 有$f(x_0) \equiv 0 \bmod d$ 成立,
同余方程$f(x) \equiv 0 \bmod d$有解.

这个结论可以用来说明方程无解:
如果$f(x) \equiv 0 \bmod d$ 无解, 则同余方程$f(x) \equiv 0 \bmod m$ 无解.

例如, 同余方程$4x^2 + 27x - 9 \equiv 0 \bmod 15$无解.
这是因为同余方程$4x^2 + 27x - 9 \equiv 0 \bmod 5$无解.
这又是因为

$$4x^2 + 27x - 9 \equiv 0 \bmod 5 \iff -x^2 + 2x + 1 \equiv 0 \bmod 5 \iff (x-1)^2 \equiv 2 \bmod 5,$$

可以验算最后的这个同余方程无解.

高次同余方程解的个数

(4.1.) **一般高次同余式**

设$m_1, m_2, \ldots, m_k \in \mathbb{Z}^+$两两互素, $m = m_1 m_2 \ldots m_k$, 则同余式

$$f(x) \equiv 0 \bmod m \qquad (1)$$

与同余式方程组

$$\begin{cases} f(x) \equiv 0 \bmod m_1 \\ f(x) \equiv 0 \bmod m_2 \\ \cdots\cdots \\ f(x) \equiv 0 \bmod m_k \end{cases} \qquad (2)$$

等价. 设$f(x) \equiv 0 \bmod m_i (i = 1, 2, \ldots, k)$的解数为$T_i$, $f(x) \equiv 0 \bmod m$的解数为T, 则

$$T = T_1 T_2 \ldots T_k.$$

如果x_0是同余式$f(x) \equiv 0 \bmod m$的解, 即

$$f(x_0) \equiv 0 \bmod m$$

从而

$$f(x_0) \equiv 0 \bmod m_1$$

(理由: $a \equiv b \bmod m, d \mid m \Longrightarrow a \equiv b \bmod d$), 类似地,

$$f(x_0) \equiv 0 \bmod m_2, \ldots, f(x_0) \equiv 0 \bmod m_k$$

即x_0是同余式组的解.

反之，如果x_0是同余式组的解，则

$$\begin{cases} f(x_0) \equiv 0 \bmod m_1 \\ f(x_0) \equiv 0 \bmod m_2 \\ \cdots\cdots \\ f(x_0) \equiv 0 \bmod m_k \end{cases}$$

所以有

$$f(x_0) \equiv 0 \bmod [m_1, m_2, \ldots, m_k].$$

其中$[m_1, m_2, \ldots, m_k]$是$m_1, m_2, \ldots, m_k$的最小公倍数. 又因为$m_1, m_2, \ldots, m_k$两两互素, 所以$[m_1, m_2, \ldots, m_k] = m_1 \cdot m_2 \cdot \ldots m_k$, 即

$$f(x_0) \equiv 0 \bmod m$$

从而x_0是同余式$f(x) \equiv 0 \bmod m$的解.
所以,

$$f(x) \equiv 0 \bmod m \iff \begin{cases} f(x) \equiv 0 \bmod m_1 \\ f(x) \equiv 0 \bmod m_2 \\ \cdots\cdots \\ f(x) \equiv 0 \bmod m_k \end{cases}$$

在上述等价的同余方程组中:
设第1个同余方程的一个解为$x \equiv b_1 \bmod m_1$
设第2个同余方程的一个解为$x \equiv b_2 \bmod m_2$
.....
设第2个同余方程的一个解为$x \equiv b_k \bmod m_k$
这样可以建立一次同余方程组

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

根据中国剩余定理可以求出该同余方程组唯一的一个解

$$x \equiv M_1' M_1 b_1 + M_2' M_2 b_2 + \ldots + M_k' M_k b_k \bmod M,$$

其中

$$M = m = m_1 \cdot m_2 \cdot \ldots \cdot m_k, \quad M_1 = \frac{M}{m_1}, M_2 = \frac{M}{m_2}, \ldots, M_k = \frac{M}{m_k},$$

$$M_1' M_1 \equiv 1 \bmod m_1, M_2' M_2 \equiv 1 \bmod m_2, \ldots, M_k' M_k \equiv 1 \bmod m_k.$$

这个解也是同余方程$f(x) \equiv 0 \bmod m$的一个解.

当$b_1, b_2, \ldots, b_k$分别遍历下面k个同余方程

$$\begin{cases} f(x) \equiv 0 \bmod m_1 \\ f(x) \equiv 0 \bmod m_2 \\ \cdots\cdots \\ f(x) \equiv 0 \bmod m_k \end{cases}$$

的所有解时,

$$x \equiv M_1' M_1 b_1 + M_2' M_2 b_2 + \ldots + M_k' M_k b_k \bmod M$$

则遍历同余方程$f(x) \equiv 0 \bmod m$的所有解. 所以,

$$T = T_1 T_2 \ldots T_k.$$

上述结论给出了求解$f(x) \equiv 0 \bmod m$的思路:

1. 分解m为两两互素的数之积: $m_1, m_2, \ldots, m_k$;
2. 分别求解下面k个同余方程

$$\begin{cases} f(x) \equiv 0 \bmod m_1 \\ f(x) \equiv 0 \bmod m_2 \\ \cdots\cdots \\ f(x) \equiv 0 \bmod m_k \end{cases}$$

3. 构造一次同余方程组, 并利用中国剩余定理求解.

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

4. 重复进行(2)(3)步, 直到得到全部$T_1T_2 \ldots T_k$个解.

示例:
求解$x^4+2x^3+8x+9\equiv 0 \bmod 35$
事实上:
$x^4+2x^3+8x+9\equiv 0 \bmod 5$: 通过尝试, 可知它的解为$x\equiv 1,4 \bmod 5$
$x^4+2x^3+8x+9\equiv 0 \bmod 7$: 通过尝试, 可知它的解为$x\equiv 3,5,6 \bmod 7$.
而同余式组

$$\begin{cases} x\equiv b_1 \bmod 5 \\ x\equiv b_2 \bmod 7 \end{cases}$$

的解为

$$x\equiv 21b_1+15b_2 \bmod 35$$

将$b_1=1$或4, $b_2=3$或5或6代入, 可得$x^4+2x^3+8x+9\equiv 0 \bmod 35$的6个解.

求解模为素数幂的同余方程

当m的素因数标准分解式

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$$

时, 可以取$m_1 = p_1^{\alpha_1}$, $m_2 = p_2^{\alpha_2}$, $\dots$, $m_k = p_k^{\alpha_k}$

这样, 解一般模m的同余方程$f(x) \equiv 0 \bmod m$归结为求解模为素数幂的同余方程

$$f(x) \equiv 0 \bmod p^{\alpha}.$$

(4.2.) 模素数幂高次同余方程

定理

设$x \equiv a_1 \bmod m$为同余方程$f(x) \equiv 0 \bmod m$的一个解. 设$x \equiv c_1, c_2, \ldots, c_s \bmod d$为同余方程$f(x) \equiv 0 \bmod d$的全部解, 其中$d \mid m$. 在$c_1, c_2, \ldots, c_k$ 中有且仅有一个, 记为c_i, 满足$a \equiv c_i \bmod d$.

设$x \equiv x_0 \bmod m$是$f(x) \equiv 0 \bmod m$的解, 有$m \mid f(x_0)$, 则$d \mid f(x_0)$, 即$f(x_0) \equiv 0 \bmod d$, 即$x \equiv x_0 \bmod m$也是$f(x) \equiv 0 \bmod d$的解, 所以定理第一部分成立.

如果$x \equiv a \bmod m$为$f(x) \equiv 0 \bmod m$的一个解, 它肯定也是$f(x) \equiv 0 \bmod d$的解, 而$x \equiv c_1 \bmod d$, $x \equiv c_2 \bmod d$, $\ldots$, $x \equiv c_s \bmod d$ 为$f(x) \equiv 0 \bmod d$的全部解, 所以a必定处于这模d的s个剩余类中的一个, 例如处于第i个中, 即$a \equiv c_i \bmod d$,

但只能处于一个之中, 因为如果它同时处于第i个和第$j(j \neq i)$之中的话就有$a \equiv c_i \bmod d$, $a \equiv c_j \bmod d$, 从而$c_i \equiv c_j \bmod d$, 但c_i和c_j处于不同的剩余类中, 所以不可能同余. $\diamond$

这个结论表明, 在求解较大模数m的同余方程$f(x) \equiv 0 \bmod m$时, 可以先找一个较小的正因子d, 求出模d的同余方程$f(x) \equiv 0 \bmod d$的全部解:

$$x \equiv c_1 \bmod d, x \equiv c_2 \bmod d, \ldots, x \equiv c_s \bmod d.$$

对于同余方程$f(x) \equiv 0 \bmod m$的每个解$x \equiv a \bmod m$, 有且仅有一个c_i, 例如c_1, 使得$a \equiv c_1 \bmod d$, 即存在整数k使得$a = dk + c_1$, 所以有

$$f(dk + c_1) \equiv 0 \bmod m$$

成立. 对等式左边加以整理, 得到一个关于k的同余方程, 记作

$$g_1(k) \equiv 0 \bmod m.$$

如果这个关于k的同余方程容易求解, 例如，它是一次方程, 就可以得到对应于这个c_1的同余方程$f(x) \equiv 0 \bmod m$的解.

对每个c_i都这么做, 就可以得到同余方程$f(x) \equiv 0 \bmod m$的全部解.

问题是: 怎样的情况下可以使得得到的关于k的方程是一次的, 从而容易求解?

考虑$m = p^\alpha, d = p^{\alpha-1}, \alpha \geq 2$.设$c$是同余方程$f(x) \equiv 0 \bmod p^{\alpha-1}$的解.
为了求出$f(x) \equiv 0 \bmod p^\alpha$的与$c$模$d$同余的解$a$, 即$a = kd + c$, 必须确定$k$的值.
将$a = kd + c$代入方程$f(x) \equiv 0 \bmod p^\alpha$, 即

$$a_n(kd+c)^n + a_{n-1}(kd+c)^{n-1} + \ldots + a_2(kd+c)^2 + a_1(kd+c) + a_0 \equiv 0 \bmod p^\alpha$$

$$(c+kd)^n = c^n + nc^{n-1}(kd) + @ \cdot (kd)^2 + @ \cdot (kd)^3 + \ldots + @ \cdot (kd)^n$$
$$(c+kd)^{n-1} = c^{n-1} + (n-1)c^{n-2}(kd) + @ \cdot (kd)^2 + @ \cdot (kd)^3 + \ldots + @ \cdot (kd)^{n-1}$$
$$(c+kd)^{n-2} = c^{n-2} + (n-2)c^{n-3}(kd) + @ \cdot (kd)^2 + @ \cdot (kd)^3 + \ldots + @ \cdot (kd)^{n-2}$$
$\ldots\ldots$
$$(c+kd)^2 = c^2 + 2c(kd) + (kd)^2$$
$$(c+kd)^1 = c + kd$$
$$a_n(c+kd)^n = a_n c^n + a_n nc^{n-1}(kd) + a_n @ \cdot (kd)^2 + a_n @ \cdot (kd)^3 + \ldots + a_n @ \cdot (kd)^n$$
$$a_{n-1}(c+kd)^{n-1} = a_{n-1}c^{n-1} + a_{n-1}(n-1)c^{n-2}(kd) + a_{n-1}@ \cdot (kd)^2 + \ldots +$$
$$a_{n-2}(c+kd)^{n-2} = a_{n-2}c^{n-2} + a_{n-2}(n-2)c^{n-3}(kd) + a_{n-2}@ \cdot (kd)^2 + \ldots +$$
$\ldots\ldots$
$$a_2(c+kd)^2 = a_2 c^2 + a_2 2c(kd) + a_2(kd)^2$$
$$a_1(c+kd) = a_1 c + a_1(kd)$$
$$a_0 = a_0$$

整理后, 常数项为

$$a_0 + a_1 c + a_2 c^2 + a_3 c^3 + \ldots + a_{n-2} c^{n-2} + a_{n-1} c^{n-1} + a_n c^n = f(c).$$

kd的1次项:

$$\left(a_1 + 2a_2 c + \ldots + (n-1) a_{n-1} c^{n-3} + n a_n c^{n-1}\right) \cdot (kd) = f'(c) \cdot (kd),$$

其中$f'(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \ldots + 3a_3 x^2 + 2a_2 x + a_1$是$f(x)$对$x$求导, 而$f'(c)$是导数在$c$处的值.

(kd)的2次项, 3次项, 4次项, ..., n次项都是p^α的倍数.
这是因为$\alpha \geq 2$, 所以$2\alpha - 2 \geq \alpha$, 从而$p^\alpha | p^{2\alpha-2}$
类似地可以说明(kd)的3次项, 4次项, ..., n次项都是p^α的倍数.

所以, 最终可以得道同余式:

$$f'(c) d \cdot k + f(c) \equiv 0 \bmod m, \quad \text{即} \quad f'(c) p^{\alpha-1} \cdot k \equiv -f(c) \bmod p^\alpha$$

由于c是$f(x) \equiv 0 \bmod p^{\alpha-1}$的解, 所以$p^{\alpha-1} | f(c)$,
从而上述同余方程等价于

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

这是一个关于k的一次同余方程, 根据一次同余方程的求解方法我们知道:

1. 如果$(f'(c), p) = 1$, 它有唯一解, 并可以求出, 假设解为$x \equiv k_1 \bmod p$;
2. 如果$(f'(c), p) \neq 1$, 那么就有$p | f'(c)$, 这时, 如果$p \nmid \frac{-f(c)}{p^{\alpha-1}}$, 则这个关于$k$的一次同余方程无解;
3. 如果$(f'(c), p) \neq 1$, 那么就有$p | f'(c)$, 这时, 如果$p | \frac{-f(c)}{p^{\alpha-1}}$, 则这个关于$k$的一次同余方程有$p$个解. 由于方程本身是一个模$p$的同余方程, 所以全部$p$个解也就是$k \equiv 0 \bmod p$, $k \equiv 1 \bmod p$, $\ldots$, $k \equiv p-1 \bmod p$;

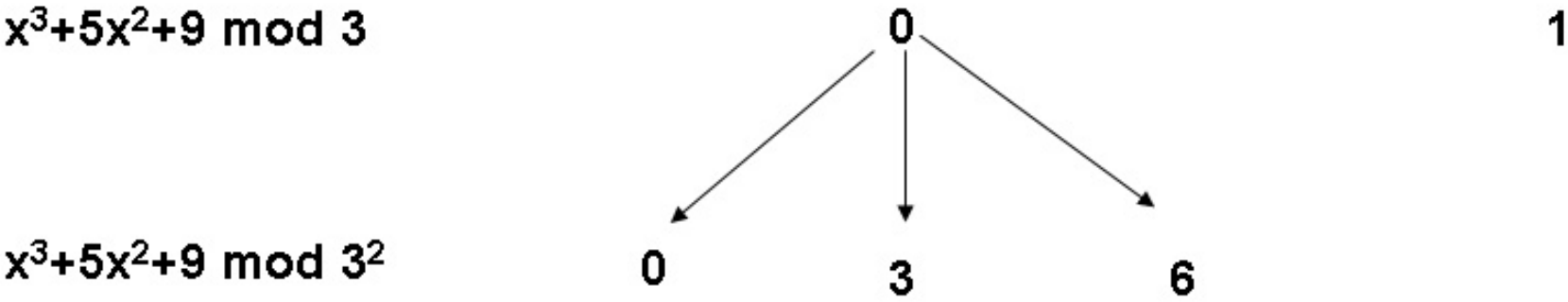
从而可以写出$f(x) \equiv 0 \bmod p^{\alpha}$的对应于$f(c) \equiv 0 \bmod p^{\alpha-1}$的解$c$的解.

$x \equiv c + p^{\alpha-1} k_1 \bmod m$.
或者
$x \equiv c \bmod m$, $x \equiv c + p^{\alpha-1} \bmod m$, $x \equiv c + p^{\alpha-1} \cdot 2 \bmod m$, $\ldots$,
$x \equiv c + p^{\alpha-1} \cdot (p-1) \bmod m$.

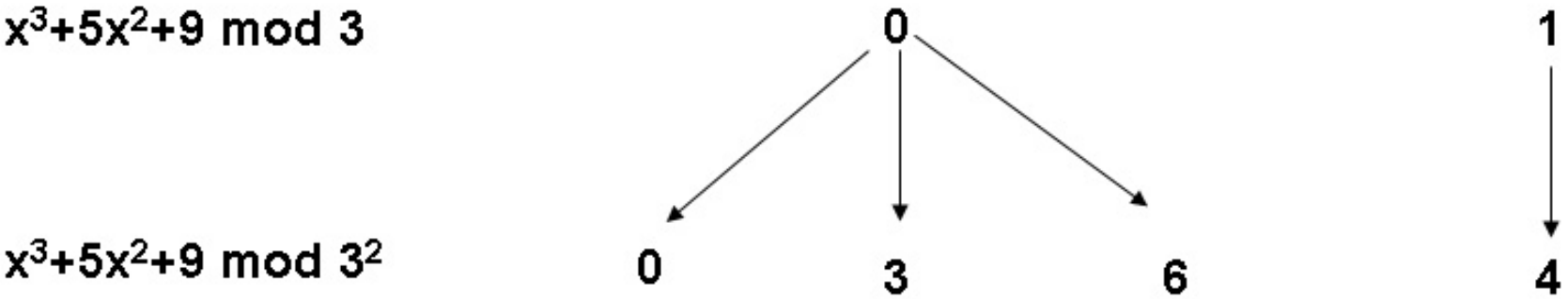
示例: 求解$x^3+5x^2+9\equiv 0 \bmod 3^4$.
这里, $p=3, f(x)=x^3+5x^2+9$, 且$f'(x)=3x^2+10x$.

必须先从$x^3+5x^2+9\equiv 0 \bmod 3$开始求解. 检查$0,1,2$发现$x\equiv 0,1 \bmod 3$是它的解, 利用$x^3+5x^2+9\equiv 0 \bmod 3$的这两个解来求$x^3+5x^2+9\equiv 0 \bmod 3^2$(即$\alpha=2$)的解.

对$x^3+5x^2+9\equiv 0 \bmod 3$的解$x\equiv 0 \bmod 3$即$c=0$时, 所以$f(c)=9$, $f'(c)=0$, $\frac{-f(c)}{p^{\alpha-1}}=3$, 这时有$p|f'(c)$, $p|\frac{-f(c)}{p^{\alpha-1}}$, 所以关于$k$的方程有$p$个解, 即$k\equiv 0,1,2 \bmod 3$.
于是, 得到对应于$x\equiv 0 \bmod 3$的$x^3+5x^2+9\equiv 0 \bmod 3^2$的解$x\equiv 0+3\cdot 0 \bmod 3^2$, $x\equiv 0+3\cdot 1 \bmod 3^2$, $x\equiv 0+3\cdot 2 \bmod 3^2$, 即$x\equiv 0 \bmod 3^2$, $x\equiv 3 \bmod 3^2$, $x\equiv 6 \bmod 3^2$



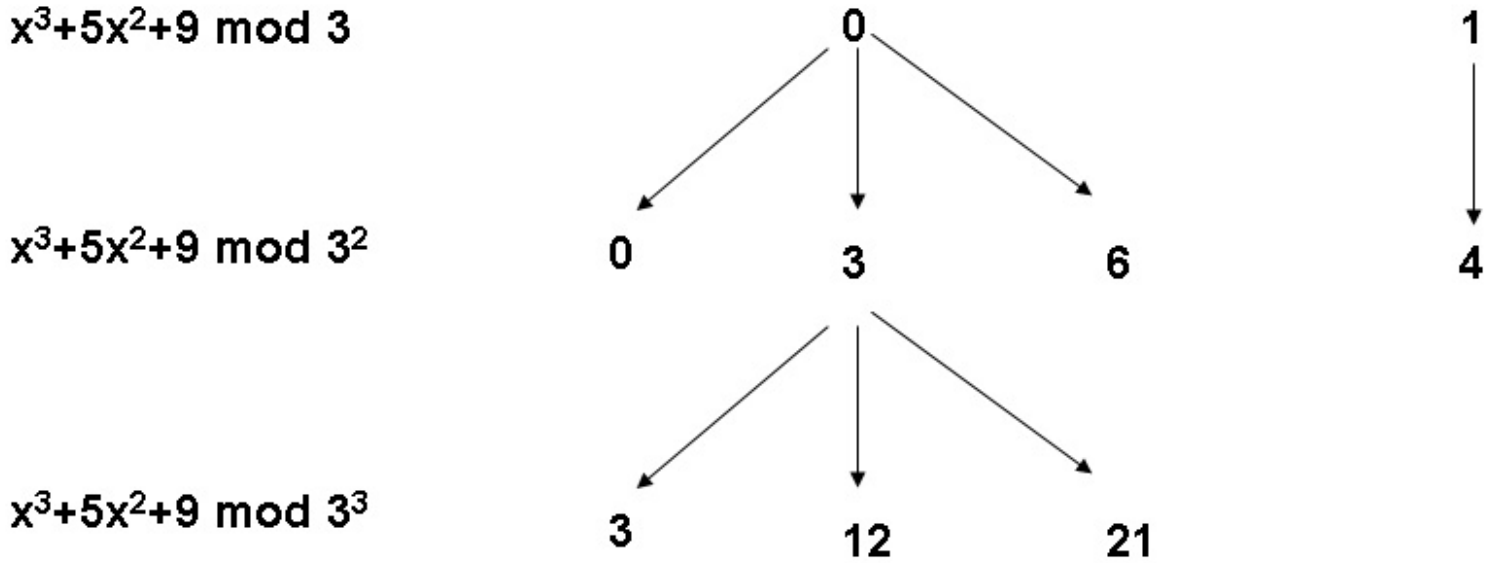
对$x^3+5x^2+9\equiv 0 \bmod 3$的解$x\equiv 1 \bmod 3$即$c=1$时, 所以$f(c)=15$, $f'(c)=13$,
$\frac{-f(c)}{p^{\alpha-1}}=-5$, 这时有$p\nmid f'(c)$, 所以关于$k$的方程$13k\equiv -5 \bmod 3$有一个解,
即$k\equiv 1 \bmod 3$, 从而得到对应于$x^3+5x^2+9\equiv 0 \bmod 3$的解$x\equiv 1 \bmod 3$
的$x^3+5x^2+9\equiv 0 \bmod 3^2$的解$x\equiv 1+3\cdot 1 \bmod 3^2$, 即$x\equiv 4 \bmod 3^2$



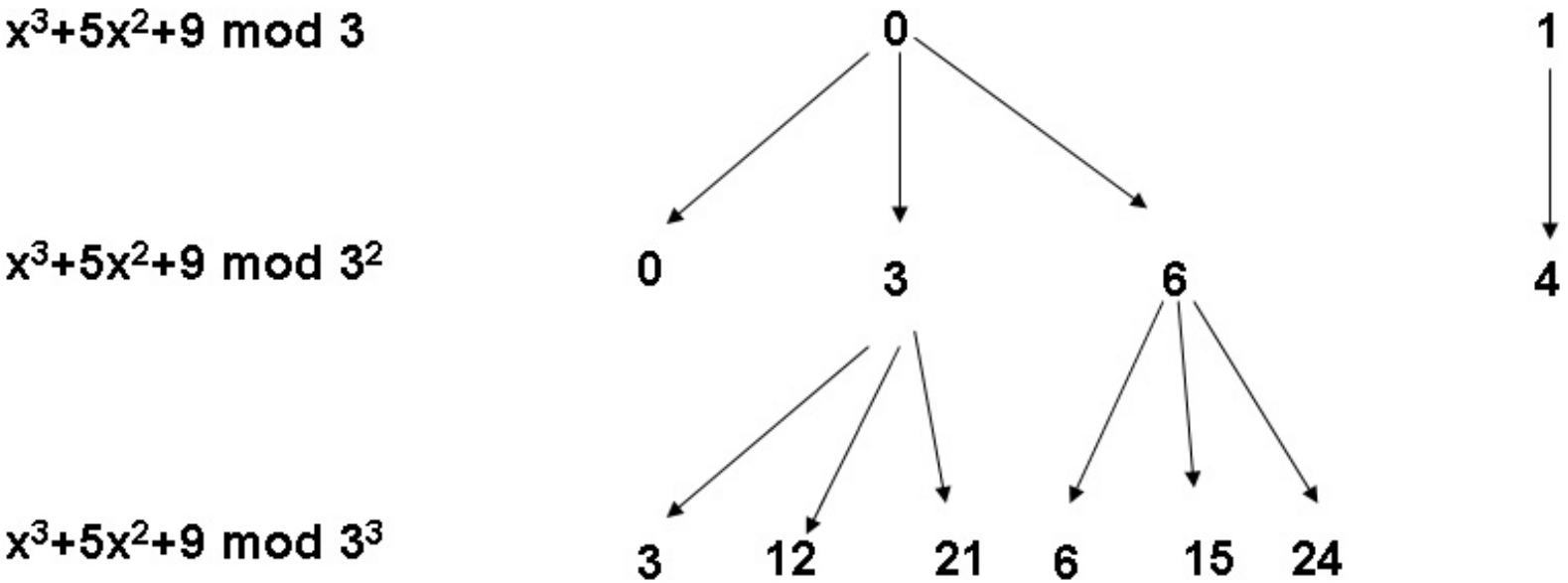
有了$x^3+5x^2+9\equiv 0 \bmod 3^2$的解$x\equiv 0 \bmod 3^2$, $x\equiv 3 \bmod 3^2$, $x\equiv 6 \bmod 3^2$, $x\equiv 4 \bmod 3^2$ 之后要利用他们来求方程$x^3+5x^2+9\equiv 0 \bmod 3^3$(即这是$\alpha=3$)的解:

对$x^3+5x^2+9\equiv 0 \bmod 3^2$的解$x\equiv 0 \bmod 3^2$即$c=0$, 所以$f(c)=9$, $f'(c)=0$, $\frac{-f(c)}{p^{\alpha-1}}=-1$, 这时有$p|f'(c)$, $p\nmid\frac{-f(c)}{p^{\alpha-1}}$, 所以关于$k$的方程无解.

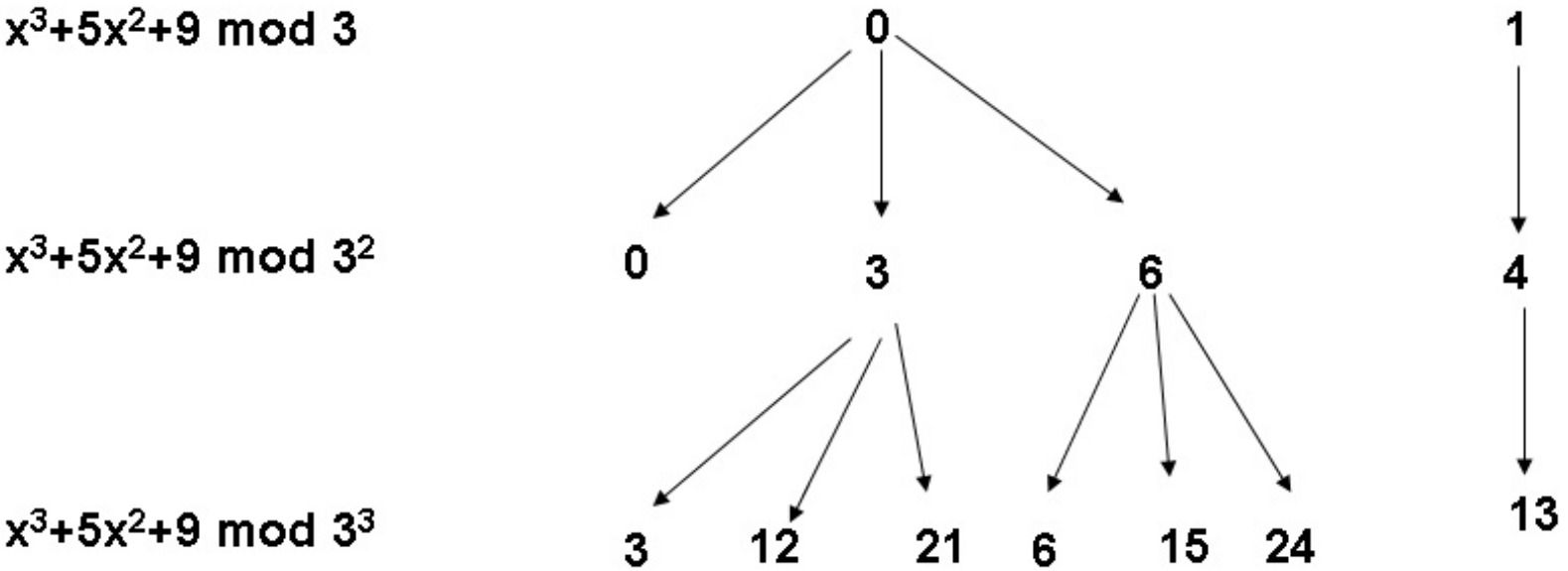
对$x^3+5x^2+9\equiv 0 \bmod 3^2$的解$x\equiv 3 \bmod 3^2$即$c=3$, 所以$f(c)=81$, $f'(c)=57$, $\frac{-f(c)}{p^{\alpha-1}}=-9$, 这时有$p|f'(c)$, $p|\frac{-f(c)}{p^{\alpha-1}}$, 所以关于$k$的方程有$p$个解: 即$k\equiv 0 \bmod 3$, $k\equiv 1 \bmod 3$, $k\equiv 2 \bmod 3$,
从而得到对应于$x^3+5x^2+9\equiv 0 \bmod 3^2$的解$x\equiv 3 \bmod 3^2$
的$x^3+5x^2+9\equiv 0 \bmod 3^3$的解$x\equiv 3+3^2\cdot 0 \bmod 3^3$, $x\equiv 3+3^2\cdot 1 \bmod 3^3$, $x\equiv 3+3^2\cdot 2 \bmod 3^3$, 即$x\equiv 3 \bmod 3^3$, $x\equiv 12 \bmod 3^3$, $x\equiv 21 \bmod 3^3$.



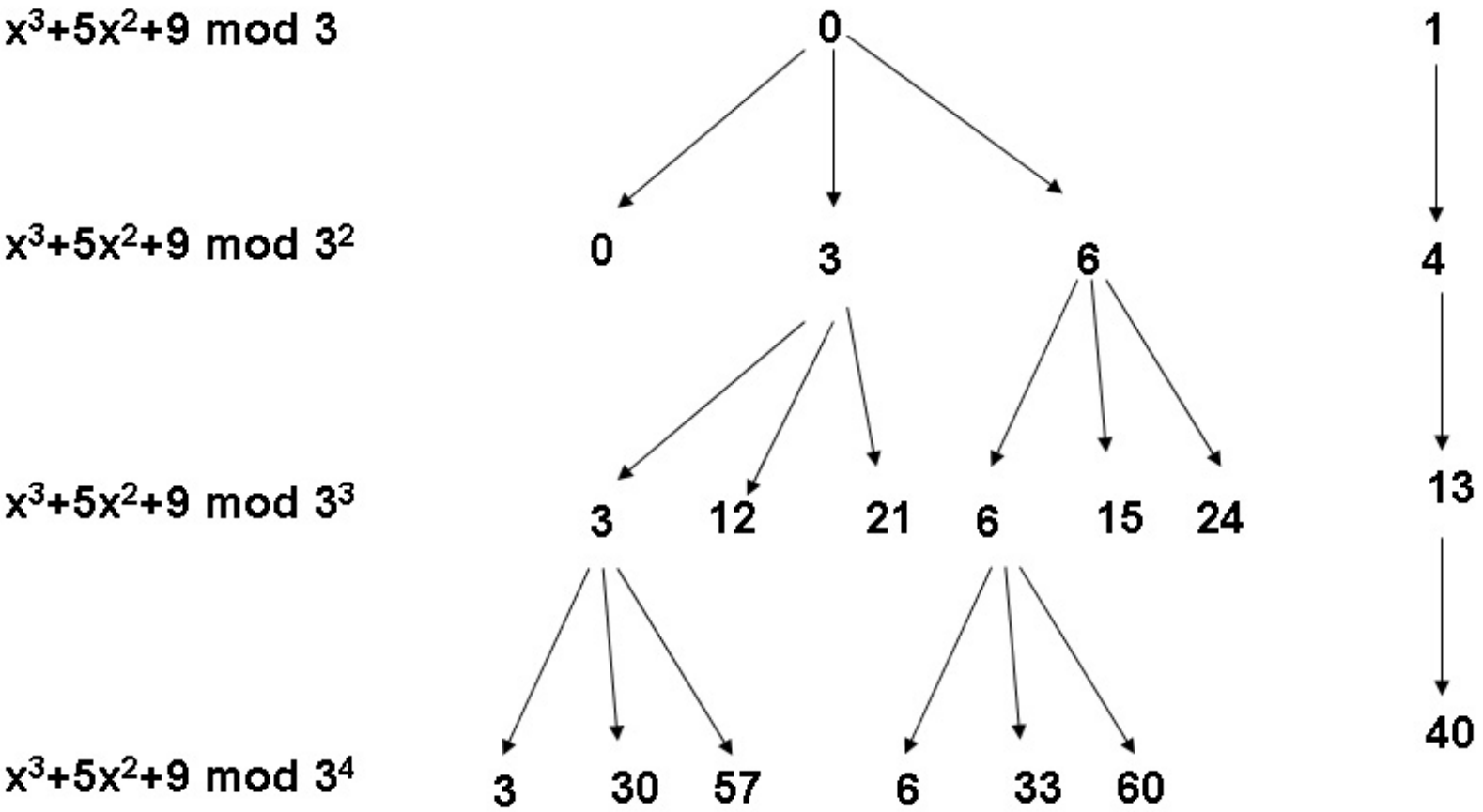
对$x^3+5x^2+9\equiv 0 \bmod 3^2$的解$x\equiv 6 \bmod 3^2$即$c=6$, 所以$f(c)=405$, $f'(c)=168$, $\frac{-f(c)}{p^{\alpha-1}}=-45$, 这时有$p|f'(c)$, $p|\frac{-f(c)}{p^{\alpha-1}}$, 所以关于$k$的方程有$p$个解: 即$k\equiv 0 \bmod 3$, $k\equiv 1 \bmod 3$, $k\equiv 2 \bmod 3$,
从而得到对应于$x^3+5x^2+9\equiv 0 \bmod 3^2$的解$x\equiv 6 \bmod 3^2$
的$x^3+5x^2+9\equiv 0 \bmod 3^3$的解$x\equiv 6+3^2\cdot 0 \bmod 3^3$, $x\equiv 6+3^2\cdot 1 \bmod 3^3$, $x\equiv 6+3^2\cdot 2 \bmod 3^3$, 即$x\equiv 6 \bmod 3^3$, $x\equiv 15 \bmod 3^3$, $x\equiv 24 \bmod 3^3$.



类似可以求出对应于$x^3+5x^2+9\equiv 0 \bmod 3^2$的解$x\equiv 4 \bmod 3^2$的$x^3+5x^2+9\equiv 0 \bmod 3^3$的解$x\equiv 13 \bmod 3^3$.



利用$x^3+5x^2+9\equiv 0 \bmod 3^3$的解$x\equiv 6 \bmod 3^3$, $x\equiv 15 \bmod 3^3$, $x\equiv 24 \bmod 3^3$, $x\equiv 3 \bmod 3^3$, $x\equiv 12 \bmod 3^3$, $x\equiv 21 \bmod 3^3$, $x\equiv 13 \bmod 3^3$,
最终可以求出$x^3+5x^2+9\equiv 0 \bmod 3^4$的解.



示例: 求解同余方程$x^3+5x^2+9\equiv 0 \bmod 7\cdot 3^4$

我们知道这个同余方程等价于同余方程组

$$\begin{cases} x^3+5x^2+9\equiv 0 \bmod 7 \\ x^3+5x^2+9\equiv 0 \bmod 3^4 \end{cases}$$

由直接计算可知第一个方程的解为$x\equiv 5 \bmod 7$, 由前例知第二个方程的解为

$$x\equiv 3,6,30,33,40,57 \bmod 3^4, 60 \bmod 3^4$$

这样, 要求解原同余方程, 等价于求解7个同余方程组:

$$\begin{cases} x\equiv 5 \bmod 7 \\ x\equiv 3 \bmod 3^4 \end{cases} \quad \begin{cases} x\equiv 5 \bmod 7 \\ x\equiv 6 \bmod 3^4 \end{cases} \quad \begin{cases} x\equiv 5 \bmod 7 \\ x\equiv 30 \bmod 3^4 \end{cases} \quad \begin{cases} x\equiv 5 \bmod 7 \\ x\equiv 33 \bmod 3^4 \end{cases}$$

$$\begin{cases} x\equiv 5 \bmod 7 \\ x\equiv 40 \bmod 3^4 \end{cases} \quad \begin{cases} x\equiv 5 \bmod 7 \\ x\equiv 57 \bmod 3^4 \end{cases} \quad \begin{cases} x\equiv 5 \bmod 7 \\ x\equiv 60 \bmod 3^4 \end{cases}$$

根据本节内容, 我们知道, 为了求解一般同余方程有上述的统一方法, 现在的问题是: 对于模素数的同余方程$f(x)\equiv 0 \bmod p$如何求解?

为了求解$f(x) \equiv 0 \bmod p^{\alpha}$, 只需要求解方程$f(x) \equiv 0 \bmod p^{\alpha-1}$即可,

而为了求解方程$f(x) \equiv 0 \bmod p^{\alpha-1}$, 需要求解方程$f(x) \equiv 0 \bmod p^{\alpha-2}$, ... ,

为了求解方程$f(x) \equiv 0 \bmod p^{3}$, 需要求解方程$f(x) \equiv 0 \bmod p^{2}$,

为了求解方程$f(x) \equiv 0 \bmod p^{2}$, 需要求解方程$f(x) \equiv 0 \bmod p$,

这样, 一般模数的同余方程的求解归结为对一个模数为素数的同余方程的求解.

4.3. 模素数高次同余式

考虑$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_2 x^2 + a_1 x + a_0$, 同余方程$f(x) \equiv 0 \bmod p$,

取$g(x) = x^p - x$, 根据多项式的欧几里德除法知道: 存在$q(x), r(x)$, $(\deg(r(x)) < p)$,
使得$f(x) = (x^p - x)q(x) + r(x)$

从而我们知道$f(x) \equiv 0 \bmod p \iff r(x) \equiv 0 \bmod p$,
也就是说, 这个同余方程与一个不超过$p-1$次的同余方程等价.

示例: $f(x) = 3x^{14} + 4x^{13} + 2x^{11} + x^9 + x^6 + x^3 + 12x^2 + x$, $p = 5$,
同余方程$f(x) \equiv 0 \bmod 5$等价于$3x^3 + 16x^2 + 6x \equiv 0 \bmod 5$,
这是因为
$3x^{14} + 4x^{13} + 2x^{11} + x^9 + x^6 + x^3 + 12x^2 + x$
$= (x^5 - x)(3x^9 + 4x^8 + 2x^6 + 3x^5 + 5x^4 + 2x^2 + 4x + 5) + (3x^3 + 16x^2 + 6x)$
因此, 对任意次数模p的同余方程的求解, 可以转换为对一个次数不超过$p-1$的模p同余方程的求解.

定理: 设$f(x)=a_nx^n+a_{n-1}x^{n-1}+\ldots+a_2x^2+a_1x+a_0$, 设$x\equiv a_1 \bmod p$ 是同余方程$f(x)\equiv 0 \bmod p$ 的解, 则存在$n-1$次的首项系数为a_n的多项式$f_1(x)$使得对任意整数x都有: $f(x)\equiv (x-a_1)f_1(x) \bmod p$.

这个结论比较显然, 因为: 取$g(x)=x-a_1$, 根绝多项式的欧几里德除法知道存在$f_1(x)$和$r(x)$使得$f(x)=(x-a_1)f_1(x)+r(x)$, 这里的$r(x)$的次数小于$g(x)$的次数,

所以$r(x)$的次数只能为0, 即$r(x)$是一个整数, 记为r, 这样有$f(x)=(x-a_1)f_1(x)+r$, 同余方程$f(x)\equiv 0 \bmod p$也就是$(x-a_1)f_1(x)+r\equiv 0 \bmod p$.

另外, 由于$f(a_1)\equiv 0 \bmod p$, 所以有$(a_1-a_1)f_1(x)+r\equiv 0 \bmod p$, 即$r\equiv 0 \bmod p$, 即$r=tp$,

从而$f(x)=(x-a_1)f_1(x)+tp$.

从而有$f(x)\equiv (x-a_1)f_1(x) \bmod p$. $\diamond$

如果还有$x \equiv a_2 \bmod p$是同余方程$f(x) \equiv 0 \bmod p$的另外一个解, 即$f(a_2) \equiv 0 \bmod p$, 从而$(a_2 - a_1)f_1(a_2) \equiv 0 \bmod p$, 即$p|(a_2 - a_1)f_1(a_2)$, 从而$p|(a_2 - a_1)$或$p|f_1(a_2)$. 如果$p|(a_2 - a_1)$, 则$a_2 \equiv a_1 \bmod p$, 这就与$x \equiv a_2 \bmod p$是不同余$x \equiv a_1 \bmod p$的同余方程$f(x) \equiv 0 \bmod p$的另一个解矛盾, 所以$p \nmid (a_2 - a_1)$

于是$p|f_1(a_2)$, 即$f_1(a_2) \equiv 0 \bmod p$, 换句话说, $x \equiv a_1 \bmod p$是$f_1(x) \equiv 0 \bmod p$的解, 则存在$n-2$次的首项系数为a_n的多项式$f_2(x)$使得对任意整数x都有

$$f_1(x) \equiv (x - a_2)f_2(x) \bmod p.$$

从而, 存在$n-2$次的首项系数为a_n的多项式$f_2(x)$使得对任意整数x都有

$$f(x) \equiv (x - a_1)(x - a_2)f_2(x) \bmod p.$$

一般地, 如果$x \equiv a_1 \bmod p$, $x \equiv a_2 \bmod p$, $x \equiv a_3 \bmod p$, $\ldots$, $x \equiv a_k \bmod p$是同余方程$f(x) \equiv 0 \bmod p$ 的k个不同解, 则存在$n-k$次的首项系数为a_n的多项式$f_k(x)$使得对任意整数x都有$f(x) \equiv (x - a_1)(x - a_2)(x - a_3)\ldots(x - a_k)f_k(x) \bmod p$.

次数为n的同余方程, 它的解数k至多为n. 另外, 任一模p的同余方程的解数至多为p个, 所以任意模p的同余方程的解数$k \leq \min(p, n)$.

如果$f(x)$中每个系数都是p的倍数的话, 即使$f(x)$的次数$n < p$, 它的解数仍是p.
例如, $11x^2 + 22x + 33 \bmod 11$的解数是11个,但多项式$f(x)$本身最高项是$x^2$.

示例: 对任意整数x, 都有$x^{p-1} - 1 \equiv (x-1)(x-2)(x-3)\dots(x-(p-1)) \bmod p$成立.
根据欧拉定理, 我们有

$$1^{p-1} - 1 \equiv 0 \bmod p$$

$$2^{p-1} - 1 \equiv 0 \bmod p$$

$$3^{p-1} - 1 \equiv 0 \bmod p$$

$$\dots\dots$$

$$(p-1)^{p-1} - 1 \equiv 0 \bmod p$$

即$x \equiv 1 \bmod p, \dots, x \equiv p-1 \bmod p$都是$x^{p-1} - 1 \equiv 0 \bmod p$的解, 所以存在多项式$f_{p-1}(x)$使得$x^{p-1} - 1 \equiv (x-1)(x-2)(x-3)\dots(x-(p-1))f_{p-1}(x) \bmod p$成立.
此处$f_{p-1}(x)$的次数为$(p-1)-(p-1)=0$的首项系数为1的多项式, 即为整数1.

所以$x^{p-1} - 1 \equiv (x-1)(x-2)(x-3)\dots(x-(p-1)) \bmod p$. $\diamond$

注: 这个结论中, 令$x = 0$即得到Wilson定理的结论.

定理: 设$f(x)=x^n+a_{n-1}x^{n-1}+\ldots+a_2x^2+a_1x+a_0$, $n\leq p$,
$x^p-x=f(x)q(x)+r(x)$ ($r(x)$的次数$<n$, 首项系数为1的$q(x)$的次数$=p-n$),
则$f(x)\equiv 0 \bmod p$有n个解 $\Longleftrightarrow$ $r(x)$的系数都是p的倍数.

这个结论是显然的:
"$\Longrightarrow$:" $f(x)$有n个解, 这n个解当然也使得$x^p-x\equiv 0 \bmod p$,
而$r(x)=(x^p-x)-f(x)q(x)$, 那么这n个解也是的$r(x)\equiv 0 \bmod p$, 但因为$r(x)$的次数$<n$, 所以$r(x)$的系数都是p的倍数;

"$\Longleftarrow$:" $\forall x_0\in\mathbb{Z}$, 都有$r(x_0)\equiv 0 \bmod p, x_0^p-x_0\equiv 0 \bmod p$
所以$\forall x_0\in\mathbb{Z}$, 都有$f(x_0)q(x_0)\equiv 0 \bmod p$
从而$\forall x_0\in\mathbb{Z}$, $p|f(x_0)q(x_0)$
即: $\forall x_0\in\mathbb{Z}$, $p\,|\,f(x_0)$和$p\,|\,q(x_0)$至少有一个成立(也可能两个都成立),
即: $\forall x_0\in\mathbb{Z}$, 它要么是$f(x)\equiv 0 \bmod p$的解, 要么是$q(x)\equiv 0 \bmod p$的解.
这样, 它们的解数之和一定等于p.

如果$f(x)\equiv 0 \bmod p$的解数$<n$, 那么$q(x)\equiv 0 \bmod p$的解数必须$>p-n$,
但$q(x)$是一个系数不全为p的倍数(因为首项系数为1), 且次数为$p-n$的多项式, 因此$q(x)\equiv 0 \bmod p$的解数至多为$p-n$, 矛盾出现, 所以$f(x)\equiv 0 \bmod p$的解数等于n.

示例: 同余方程$2x^3+5x^2+6x+1\equiv 0 \bmod 7$有3个解,

由于$(4,7)=1$, 所以同余方程$2x^3+5x^2+6x+1\equiv 0 \bmod 7$等价于$4(2x^3+5x^2+6x+1)\equiv 0 \bmod 7$, 即方程:

$$x^3-x^2+3x-3\equiv 0 \bmod 7$$

这个方程首项系数为1,可以使用前述结论来判定:

$$x^7-x=(x^3-x^2+3x-3)(x^4+x^3-2x^2-2x+7)+(7x^2-28x+21)$$

这里余式$7x^2-28x+21$的系数均为$p=7$的倍数, 所以原方程有3个解.

示例: $d|(p-1)$, 则$x^d - 1 \equiv 0 \bmod p$的解数为d.

令$f(x) = x^d - 1$, 设$p - 1 = dq$, 则有

$$x^p - x = (x^{p-1} - 1)x = (x^{dq} - 1)x$$

$$= (x^d - 1)(x^{d(q-1)} + x^{d(q-2)} + \ldots + x^d + 1)x$$

$$= (x^d - 1)(x^{d(q-1)+1} + x^{d(q-2)+1} + \ldots + x^{d+1} + x)$$

即多项式$x^p - x$被$f(x) = x^d - 1$除后所得余式为0(系数自然都是p的倍数), 所以$f(x) \equiv 0 \bmod p$有d个解.

不像一次同余方程或一次同余方程组那样有完美的公式告知其解的存在性和具体求解方法, 模素数高次同余方程(从而一般高次同余方程)没有那样完美的结论.

本节得到的关于模素数p的高次同余方程的解方面的结论为:

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.