第三章 同余式
2015年04月16日

信息安全数学基础

陈恭亮 教授 博士生导师

上海交通大学信息安全工程学院

chengl@sjtu.edu.cn

访问主页
标题页
目录页
第 1 页 共 44 页
返回
全屏显示
关闭
退出

3.3 高次同余式的解数及解法

现在我们考虑高次同余式的求解.

定理3.3.1 设$m_1, \ldots, m_k$ 两两互素, $m = m_1 \cdots m_k$. 则

$$f(x) \equiv 0 \pmod{m} \quad (1) \quad \Leftrightarrow \quad \begin{cases} f(x) \equiv 0 \pmod{m_1}, \\ \quad \cdots\cdots \\ f(x) \equiv 0 \pmod{m_k} \end{cases} \qquad (2)$$

若T_i 为$f(x) \equiv 0 \pmod{m_i}$ 的解数, T 为(1)的解数, 则$T = T_1 \cdots T_k$.

证 设x_0 是同余式(1)的解, 则$f(x_0) \equiv 0 \pmod{m}$. 从而

$f(x_0) \equiv 0 \pmod{m_i}, \quad i = 1, \ldots, k$. 即$x_0$是同余式组(2) 的解.

反过来, 设$f(x_0) \equiv 0 \pmod{m_i}, \quad i = 1, \ldots, k$, 则有$f(x_0) \equiv 0 \pmod{m}$. 即同余式组(2)的解$x_0$也是同余式(1)的解.

设$f(x) \equiv 0 \pmod{m_i}$ 的解是b_i, $i = 1, \dots, k$. 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$x \equiv b_1 \cdot M_1' \cdot M_1 + \cdots + b_k \cdot M_k' \cdot M_k \pmod{m}$.

因为$f(x) \equiv f(b_i) \equiv 0 \pmod{m_i}, \quad i = 1, \dots, k,$

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($i = 1, \dots, k$,) 而遍历$f(x) \equiv 0 \pmod{m}$的所有解.即$\begin{cases} f(x) \equiv 0 \pmod{m_1}, \\ \cdots\cdots \\ f(x) \equiv 0 \pmod{m_k} \end{cases}$的解数为$T = T_1 \cdots T_k$.

例3.3.1 解同余式$f(x) \equiv x^4 + 2x^3 + 8x + 9 \equiv 0 \pmod{35}$.

解 由定理1知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. 事实上,

$$\begin{array}{lll} 1\cdot 21+3\cdot 15=66 \equiv 31, & \quad & 4\cdot 21+3\cdot 15=129 \equiv 24, \\ 1\cdot 21+5\cdot 15=96 \equiv 26, & & 4\cdot 21+5\cdot 15=159 \equiv 19, \\ 1\cdot 21+6\cdot 15=111 \equiv 6, & & 4\cdot 21+6\cdot 15=174 \equiv 34. \end{array}$$

3.3.2 高次同余式的提升

因为

$$m = \prod_p p^\alpha,$$

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,

$$f(x) \equiv 0 \pmod{p^\alpha} \tag{1}$$

的解法.

设$f(x) = a_n x^n + \cdots + a_2 x^2 + a_1 x + a_0$ 为整系数多项式, 我们记

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

称$f'(x)$ 为$f(x)$ 的导式.

提升路线图:

$$
\begin{array}{cc}
f(x) \equiv 0 \ (\mathrm{mod} p^{\alpha}) & x \equiv x_{\alpha} = x_{\alpha-1} + t_{\alpha-1} \cdot p^{\alpha-1} \ (\mathrm{mod} p^{\alpha}) \\
\vdots & \\
f(x) \equiv 0 \ (\mathrm{mod} p^{2}) & x \equiv x_{i} = x_{i-1} + t_{i-1} \cdot p^{i-1} \ (\mathrm{mod} p^{i}) \\
\Uparrow & \\
f(x) \equiv 0 \ (\mathrm{mod} p^{i-1}) & x \equiv x_{i-1} \ (\mathrm{mod} p^{i-1}) \\
\vdots & \\
f(x) \equiv 0 \ (\mathrm{mod} p^{2}) & x \equiv x_{2} = x_{1} + t_{1} \cdot p \ (\mathrm{mod} p^{2}) \\
\Uparrow & \\
f(x) \equiv 0 \ (\mathrm{mod} p) & x \equiv x_{1} \ (\mathrm{mod} p)
\end{array}
$$

定理3.3.2 设$x \equiv x_1 \pmod{p}$ 是同余式

$$f(x) \equiv 0 \pmod{p} \tag{2}$$

的一个解, 且

$$(f'(x_1), p) = 1,$$

则同余式(1)有解

$$x \equiv x_\alpha \pmod{p^\alpha}, \tag{3}$$

其中x_α 由下面关系式递归得到:

$$x_i \equiv x_{i-1} + t_{i-1} \cdot p^{i-1} \pmod{p^i}, \qquad i = 2, \ldots, \alpha, \tag{4}$$

这里

$$t_{i-1} \equiv \frac{-f(x_{i-1})}{p^{i-1}} \cdot (f'(x_1)^{-1} \pmod{p}) \pmod{p}, \qquad i = 2, \ldots, \alpha. \tag{5}$$

证 设$f(x)=a_nx^n+\cdots+a_1x+a_0$. 对$\alpha\ge 2$ 作数学归纳法:

(i) $\alpha=2$. 根据假设条件, 同余式(2) 有解:

$$x=x_1+t_1\cdot p,\qquad t_1=0,\ \pm1,\ \pm2,\ \ldots,$$

所以, 考虑关于t_1 的同余式 $\quad f(x_1+t_1\cdot p)\equiv 0 \pmod{p^2}$

的求解. 因为

$$\begin{aligned}
f(x_1+t_1\cdot p) &= a_n(x_1+t_1\cdot p)^n+\cdots+a_1(x_1+t_1\cdot p)+a_0\\
&= a_n(x_1^n+nx_1^{n-1}(t_1\cdot p)+C_n^2x_1^{n-2}(t_1\cdot p)^2+\cdots+(t_1\cdot p)^n)\\
&\quad +\cdots+a_1(x_1+(t_1\cdot p))+a_0\\
&= f(x_1)+f'(x_1)(t_1\cdot p)+A\cdot(t_1\cdot p)^2
\end{aligned}$$

其中A 为整数, 所以我们有

$$f(x_1)+f'(x_1)(t_1\cdot p)\equiv 0 \pmod{p^2}.$$

$$
\begin{aligned}
& f(x_1 + t_1 \cdot p) \\
= \; & a_n(x_1 + t_1 \cdot p)^n + a_{n-1}(x_1 + t_1 \cdot p)^{n-1} + \cdots + a_2(x_1 + t_1 \cdot p)^2 \\
& + a_1(x_1 + t_1 \cdot p) + a_0 \\
= \; & a_n(\underline{x_1^n} + \underline{\underline{n x_1^{n-1}}}(t_1 \cdot p) + C_n^2 x_1^{n-2}(t_1 \cdot p)^2 + \cdots + (t_1 \cdot p)^n) \\
& + a_{n-1}(\underline{x_1^{n-1}} + \underline{\underline{(n-1)x_1^{n-2}}}(t_1 \cdot p) + C_{n-1}^2 x_1^{n-3}(t_1 \cdot p)^2 + \cdots + (t_1 \cdot p)^{n-1}) \\
& + \cdots + a_2(\underline{x_1^2} + \underline{\underline{2x_1}}(t_1 \cdot p) + (t_1 \cdot p)^2) + a_1(\underline{x_1} + \underline{\underline{1}} \cdot (t_1 \cdot p)) + a_0 \cdot \underline{1} \\
= \; & f(x_1) + f'(x_1)(t_1 \cdot p) + A \cdot (t_1 \cdot p)^2
\end{aligned}
$$

$$\underline{f(x_1) + f'(x_1)(t_1 \cdot p) \equiv 0 \pmod{p^2}}$$

因为$f(x_1) \equiv 0 \pmod p$, 所以上述同余式可写成

$$f'(x_1) \cdot t_1 \equiv \frac{-f(x_1)}{p} \pmod p.$$

又因为$(f'(x_1), p) = 1$, 所以此同余式对模p 有且仅有一解

$$t_1 \equiv \frac{-f(x_1)}{p}(f'(x_1)^{-1} \pmod p) \pmod p.$$

即

$$x \equiv x_2 \equiv x_1 + t_1 \cdot p \pmod{p^2}$$

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 $f(x) \equiv 0 \pmod{p^{i-1}}$

有解 $\quad x = x_{i-1} + t_{i-1} \cdot p^{i-1}, \qquad t_{i-1} = 0,\ \pm 1,\ \pm 2,\ \ldots.$

考虑关于t_{i-1} 的同余式 $\quad f(x_{i-1} + t_{i-1} \cdot p^{i-1}) \equiv 0 \pmod{p^i}$

的求解. 因为

$$
\begin{aligned}
& f(x_{i-1} + t_{i-1} \cdot p^{i-1}) \\
= \ & a_n(x_{i-1} + t_{i-1} \cdot p^{i-1})^n + \cdots + a_1(x_{i-1} + t_{i-1} \cdot p^{i-1}) + a_0 \\
= \ & a_n(x_{i-1}^n + n x_{i-1}^{n-1}(t_{i-1} \cdot p^{i-1}) + C_n^2 x_{i-1}^{n-2}(t_{i-1} \cdot p^{i-1})^2 + \cdots + (t_{i-1} \cdot p^{i-1})^n) \\
& + \cdots + a_1(x_{i-1} + (t_{i-1} \cdot p^{i-1}) + a_0 \\
= \ & f(x_{i-1}) + f'(x_{i-1})(t_{i-1} \cdot p^{i-1}) + A \cdot (t_{i-1} \cdot p^{i-1})^2
\end{aligned}
$$

其中A 为整数. 又$p^{2(i-1)} \ge p^i$, 我们有

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

访问主页

标题页

目录页

返回

全屏显示

关闭

退出

$$
\begin{aligned}
& f(x_{i-1} + t_{i-1} \cdot p^{i-1}) \\
= \; & a_n(x_{i-1} + t_{i-1} \cdot p^{i-1})^n + a_{n-1}(x_{i-1} + t_{i-1} \cdot p^{i-1})^{n-1} + \cdots \\
& + a_2(x_{i-1} + t_{i-1} \cdot p^{i-1})^2 + a_1(x_{i-1} + t_{i-1} \cdot p^{i-1}) + a_0 \\
= \; & a_n(\underline{x_{i-1}^n} + \underline{\underline{n x_{i-1}^{n-1}}}(t_{i-1} \cdot p^{i-1}) + C_n^2 x_{i-1}^{n-2}(t_{i-1} \cdot p^{i-1})^2 + \cdots + (t_{i-1} \cdot p^{i-1})^n) \\
& + a_{n-1}(\underline{x_{i-1}^{n-1}} + \underline{\underline{(n-1) x_{i-1}^{n-2}}}(t_{i-1} \cdot p^{i-1}) \\
& + C_{n-1}^2 x_{i-1}^{n-3}(t_{i-1} \cdot p^{i-1})^2 + \cdots + (t_{i-1} \cdot p^{i-1})^{n-1}) \\
& + \cdots + a_2(\underline{x_{i-1}^2} + \underline{\underline{2 x_{i-1}}}(t_{i-1} \cdot p^{i-1}) + (t_{i-1} \cdot p^{i-1})^2) \\
& + a_1(\underline{x_{i-1}} + \underline{\underline{1}} \cdot (t_{i-1} \cdot p^{i-1}) + a_0 \cdot \underline{1} \\
= \; & f(x_{i-1}) + f'(x_{i-1})(t_{i-1} \cdot p^{i-1}) + A \cdot (t_{i-1} \cdot p^{i-1})^2
\end{aligned}
$$

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

因为$f(x_{i-1}) \equiv 0 \pmod{p^{i-1}}$, 所以上述同余式可写成

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

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

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

所以此同余式对模p有且仅有一解

$$\begin{aligned} t_{i-1} &\equiv \frac{-f(x_{i-1})}{p^{i-1}}(f'(x_{i-1})^{-1} \pmod{p}) \\ &\equiv \frac{-f(x_{i-1})}{p^{i-1}}(f'(x_1)^{-1} \pmod{p}) \quad \pmod{p}, \end{aligned}$$

即 $x \equiv x_i \equiv x_{i-1} + t_{i-1} \cdot p^{i-1} \pmod{p^i}$

是同余式 $f(x) \equiv 0 \pmod{p^i}$ 的解.

故由数学归纳法原理, 定理对所有$2 \le i \le \alpha$ 成立. 特别, 定理对$i = \alpha$ 成立. 证毕

3.3.3 高次同余式的提升-具体应用

例3.3.2 求解同余式$f(x) \equiv x^4 + 7x + 4 \equiv 0 \pmod{27}$.

解一 对于$f(x)$, 有$f'(x) \equiv 4x^3 + 7 \pmod{27}$.

直接验算, 知同余式$f(x) \equiv 0 \pmod 3$ 有一解$x_1 \equiv 1 \pmod 3$.

$$\begin{aligned} f(0) &= 0^4 + 7 \cdot 0 + 4 = 4 \equiv 1 \pmod 3, \\ f(1) &= 1^4 + 7 \cdot 1 + 4 = 12 \equiv 0 \pmod 3, \\ f(2) &= 2^4 + 7 \cdot 2 + 4 = 34 \equiv 1 \pmod 3. \end{aligned}$$

以$x = 1 + 3t_1$代入$f(x) \equiv 0 \pmod 9$, 可得

$$f(1) + 3t_1 f'(1) \equiv 0 \pmod 9.$$

因为$f(1) \equiv 3 \pmod 9$, $\quad f'(1) \equiv 2 \pmod 9$,所以上述同余式可写成

$$3 + 3t_1 \cdot 2 \equiv 0 \pmod 9 \quad \text{或} \quad 2t_1 \equiv -1 \pmod 3.$$

解得$t_1 \equiv 1 \pmod 3$,

故$f(x) \equiv 0 \pmod 9$ 的解为$x_2 \equiv 1 + 3t_1 \equiv 4 \pmod 9$.

再以$x = 4 + 9t_2$代入$f(x) \equiv 0 \pmod{27}$, 得

$$f(4) + 9t_2 f'(4) \equiv 0 \pmod{27}.$$

因为$f(4) \equiv 18 \pmod{27}$, $\quad f'(4) \equiv 20 \pmod{27}$, 所以上述同余式可写成

$$18 + 9t_2 \cdot 20 \equiv 0 \pmod{27} \quad \text{或} \quad 2t_2 \equiv -2 \pmod{3}.$$

解得$t_2 \equiv 2 \pmod{3}$, 因此, 同余式$f(x) \equiv 0 \pmod{27}$ 的解为

$$x_3 \equiv 4 + 9t_2 \equiv 22 \pmod{27}.$$

解二 (应用定理3.3.2的结论)

对于$f(x) \equiv x^4 + 7x + 4 \pmod{27}$, 有$f'(x) \equiv 4x^3 + 7 \pmod{27}$.

直接验算, 知同余式$f(x) \equiv 0 \pmod 3$ 有一解$x_1 \equiv 1 \pmod 3$.

首先, 计算

$$f'(x_1) = 4 \cdot 1^3 + 7 \equiv -1 \pmod 3, \quad f'(x_1)^{-1} \equiv -1 \pmod 3;$$

其次, 计算$\begin{cases} t_1 \equiv -\dfrac{f(x_1)}{3^1}(f'(x_1)^{-1} \pmod 3) \equiv 1 & \pmod 3, \\ x_2 \equiv x_1 + 3t_1 \equiv 4 & \pmod 9; \end{cases}$

最后, 计算$\begin{cases} t_2 \equiv -\dfrac{f(x_2)}{3^2}(f'(x_1)^{-1} \pmod 3) \equiv 2 & \pmod 3, \\ x_3 \equiv x_2 + 3^2 t_2 \equiv 22 & \pmod{27}. \end{cases}$

因此, 同余式$f(x) \equiv 0 \pmod{27}$ 的解为

$$x_3 \equiv 22 \pmod{27}.$$

3.4.1 素数模上的多项式欧几里得除法

现在我们考虑如何求解模素数p 的同余式

$$f(x) = a_n x^n + \cdots + a_1 x + a_0 \equiv 0 \pmod p, \qquad a_n \not\equiv 0 \pmod p \quad (6)$$

引理3.4.1 (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

$$f(x) = q(x) \cdot g(x) + r(x), \quad \deg\ r(x) < \deg\ g(x). \quad (7)$$

证 我们分两种情形讨论:

(I) $n < m$. 我们取$q(x) = 0,\ r(x) = f(x)$, 结论成立.

(II) $n \geq m$. 对$f(x)$ 的次数n 作数学归纳法. $n = m$. 我们有

$$f(x) - a_n \cdot g(x) = (a_{n-1} - a_n b_{m-1}) x^{n-1} + \cdots + (a_1 - a_n b_0) x + a_0.$$

因此, $q(x) = a_n,\ r(x) = f(x) - a_n \cdot g(x)$ 为所求.

假设$n - 1 \geq m$时, 结论成立.

对于$n > m$, 我们有

$$\begin{aligned} f(x) - a_n x^{n-m} \cdot g(x) &= (a_{n-1} - a_n b_{m-1})x^{n-1} + \cdots + (a_{n-m} - a_n b_0)x^{n-m} \\ &\quad + a_{n-m-1}x^{n-m-1} + \cdots + a_0. \end{aligned}$$

这说明$f(x) - a_n x^{n-m} \cdot g(x)$ 是次数$\leq n-1$ 的多项式. 对其运用归纳假设或情形(I), 存在整系数多项式$q_1(x)$ 和$r_1(x)$ 使得

$$f(x) - a_n x^{n-m} \cdot g(x) = q_1(x) \cdot g(x) + r_1(x), \quad \deg\ r_1(x) < \deg\ g(x).$$

因此, $q(x) = a_n x^{n-m} + q_1(x),\ r(x) = r_1(x)$ 为所求.

根据数学归纳法原理, 结论是成立的. 证毕

注 引理中$g(x)$ 须为首一多项式, 因为对于

$$f(x) = x^2,\ g(x) = 2x + 1 \in \mathbf{Z}[x],$$

找不到$q(x), r(x) \in \mathbf{Z}[x]$ 满足(7).

3.4.2 素数模的同余式的简化

其次, 借助于多项式$x^p - x \pmod p$ 对任何整数取值为零(Fermat 小定理), 以及多项式欧几里得除法, 可以将高次多项式的求解转化为次数不超过$p-1$ 的多项式的求解, 即有

定理3.4.1 同余式(6)与一个次数不超过$p-1$ 模p 同余式等价.

证 由多项式的欧几里得除法, 存在整系数多项式$q(x)$, $r(x)$ 使得

$$f(x) = q(x)(x^p - x) + r(x),$$

其中$r(x)$ 的次数$\le p-1$. 由§2.4 定理2.4.2 (费马小定理), 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

$$r(x) \equiv 0 \pmod p.$$

访问主页
标题页
目录页
第 19 页 共 44 页
返回
全屏显示
关闭
退出

例3.4.1 求与如下同余式等价的次数< 5 的同余式$r(x)$.

$$f(x) = 3\,x^{14} + 4\,x^{13} + 2\,x^{11} + x^9 + x^6 + x^3 + 12\,x^2 + x \equiv 0 \pmod 5$$

解 令$g(x) = x^5 - x$, 作多项式的欧几里得除法, 我们有

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

事实上,

$$\begin{aligned} r_0(x) = f(x) - 3\,x^9 \cdot g(x) &= 4\,x^{13} + 2\,x^{11} + 3\,x^{10} + x^9 + x^6 + x^3 + 12\,x^2 + x \\ r_1(x) = r_0(x) - 4\,x^8 \cdot g(x) &= 2\,x^{11} + 3\,x^{10} + 5\,x^9 + x^6 + x^3 + 12\,x^2 + x \\ r_2(x) = r_1(x) - 2\,x^6 \cdot g(x) &= 3\,x^{10} + 5\,x^9 + 2\,x^7 + x^6 + x^3 + 12\,x^2 + x \\ r_3(x) = r_2(x) - 3\,x^5 \cdot g(x) &= 5\,x^9 + 2\,x^7 + 4\,x^6 + x^3 + 12\,x^2 + x \\ r_4(x) = r_3(x) - 5\,x^4 \cdot g(x) &= 2\,x^7 + 4\,x^6 + 5\,x^5 + x^3 + 12\,x^2 + x \\ r_5(x) = r_4(x) - 2\,x^2 \cdot g(x) &= 4\,x^6 + 5\,x^5 + 3\,x^3 + 12\,x^2 + x \\ r_6(x) = r_5(x) - 4\,x \cdot g(x) &= 5\,x^5 + 3\,x^3 + 16\,x^2 + x \\ r_7(x) = r_6(x) - 5 \cdot g(x) &= 3\,x^3 + 16\,x^2 + 6\,x \end{aligned}$$

所以原同余式等价于

$$r(x) = r_7(x) = 3x^3 + 16x^2 + 6x \equiv 0 \pmod 5).$$

所以原同余式等价于

$$r(x) = r_7(x) = 3x^3 + 16x^2 + 6x \equiv 0 \pmod 5.$$

直接验算:

$$\begin{aligned}
r(0) &= 3\cdot 0^3 + 16\cdot 0^2 + 6\cdot 0 = 0 \equiv 0\\
r(1) &= 3\cdot 1^3 + 16\cdot 1^2 + 6\cdot 1 = 25 \equiv 0\\
r(2) &= 3\cdot 2^3 + 16\cdot 2^2 + 6\cdot 2 = 100 \equiv 0\\
r(3) &= 3\cdot 3^3 + 16\cdot 3^2 + 6\cdot 3 = 243 \equiv 3\\
r(4) &= 3\cdot 4^3 + 16\cdot 4^2 + 6\cdot 4 = 472 \equiv 2 \pmod 5.
\end{aligned}$$

故同余式的解为$x \equiv 0,\ 1,\ 2 \pmod 5$.

3.4.3 素数模的同余式的因式分解

定理3.4.2 设$1 \le k \le n$. 如果

$$x \equiv a_i \pmod p, \quad i = 1, \dots, k,$$

是同余式(6)的k个不同解, 则对任何整数x, 都有

$$f(x) \equiv f_k(x) \cdot (x - a_1) \cdots (x - a_k) \pmod p, \tag{8}$$

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

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

易知, $f_1(x)$ 的次数是$n-1$, 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

$$f(x) \equiv f_1(x) \cdot (x - a_1) \pmod p.$$

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

$$f_1(a_i)\equiv 0 \pmod p,\quad i=2,\dots,k.$$

类似地, 对于多项式$f_1(x)$可找到多项式$f_2(x)$使得

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

$$\cdots\cdots\cdots\cdots\cdot$$

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

故

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

证毕

例3.4.2 我们有同余式

$$\begin{aligned}
&3x^{14}+4x^{13}+2x^{11}+x^9+x^6+x^3+12x^2+x \\
\equiv\ &(3x^{11}+3x^{10}+3x^9+4x^7+3x^6+x^5+2x^4+x^2+3x+3) \\
&\cdot x(x-1)(x-2) \pmod 5.
\end{aligned}$$

注 解$a_1=0,\ a_2=1, a_3=2$ 可由例3.4.1 中的$r(x)=3x^3+16x^2+6x$ 得到(例3.4.5):

$$r(x)\equiv 3x(x^2-3x+2)\equiv 3x(x-1)(x-2) \pmod 5.$$

根据定理3.4.2 及定理2.4.2 (费马小定理), 我们立即得到:

定理3.4.3 设p 是一个素数. 则

i) 对任何整数x, 我们有

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

ii) (Wilson定理) $(p-1)! + 1 \equiv 0 \pmod{p}$.

由Wilson定理, 可得到整数是否为素数的判别条件.

整数n 为素数的充分必要条件是

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

3.4.4 素数模的同余式的解数估计

最后, 讨论模p 同余式的解数. 先给出同余式解数的上界估计.

定理3.4.4 同余式(6)的解数不超过它的次数.

证 反证法. 设n 次同余式(6)的解数超过n 个, 则(6)式至少有$n+1$个解. 设它们为 $x \equiv a_i \pmod p, \quad i = 1, \dots, n, n+1.$

根据定理3.4.2, 对于n个解$a_1, \ \dots, \ a_n$, 可得到

$$f(x) \equiv f_n(x)(x-a_1)\cdots(x-a_n) \pmod p.$$

因为$f(a_{n+1}) \equiv 0 \pmod p$,所以

$$f_n(a_{n+1})(a_{n+1}-a_1)\cdots(a_{n+1}-a_n) \equiv 0 \pmod p.$$

因为$a_i \not\equiv a_1 \pmod p, \ i = 2, \dots, n$, 且$p$ 是素数, 所以$f_n(a_{n+1}) \equiv 0 \pmod p$. 但$f_n(x)$ 是首项系数为a_n, 次数为$n - n = 0$ 的多项式. 故$p \mid a_n$. 矛盾. 证毕

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.

证 充分性显然. 我们证必要性. 若不然, 多项式$f(x)$ 有系数不被p 整除, 这说明模p 多项式$f(x) \pmod p$ 次数$< p$. 根据定理3.4.4, 多项式的解数$< p$, 与假设条件矛盾. 故推论成立. 证毕

再给出同余式解数的判断.

定理3.4.5 设p 是一个素数, n 是一个正整数, $n \le p$. 那么同余式

$$f(x) = x^n + \cdots + a_1 x + a_0 \equiv 0 \pmod p, \tag{9}$$

有n 个解的充分必要条件是$x^p - x$ 被$f(x)$ 除所得余式的所有系数都是p的倍数.

证 因为$f(x)$ 是首一多项式, 由多项式的欧几里得除法, 知存在整系数多项式$q(x)$和$r(x)$ 使得

$$x^p - x = q(x) \cdot f(x) + r(x) \tag{10}$$

其中$r(x)$ 的次数$< n$, $q(x)$的次数是$p - n$.

现在, 若(9)式有n 个解, 则由§2.4 定理2.4.2 (费马小定理), 这n个解都是 $x^p - x \equiv 0 \pmod p$ 的解. 又由(10)式知这n 个解也是

$$r(x) \equiv 0 \pmod p$$

的解. 但$r(x)$ 的次数$< n$, 故由定理3.4.4 之推论, $r(x)$的系数都是p的倍数.

反过来, 若多项式$r(x)$ 的系数都被p 整除, 则由定理3.4.4 之推论, $r(x)$ 所有整数x 取值模p 为零. 根据§2.4 定理2.4.2 (费马小定理), 对任何整数x, 又有

$$x^p - x \equiv 0 \pmod p.$$

因此, 对任何整数x, 有

$$q(x) \cdot f(x) \equiv \pmod p. \tag{11}$$

这就是说, (11)式有p 个不同的解,

$$x \equiv 0,\ 1,\ \ldots,\ p-1 \pmod p.$$

由此可得$f(x) \equiv 0 \pmod p$的解数$k = n$. 否则, $k < n$. 但次数为$p-n$ 的多项式$q(x)$ 的同余式$q(x) \equiv \pmod p$的解数$h \leq p-n$, 所以(11)式的解数$\leq k+h < p$. 矛盾. 证毕

推论 设p是一个素数, d 是$p-1$ 的正因数. 那么多项式x^d-1 模p 有d 个不同的根.

证 因为$d \mid p-1$, 所以存在整数q 使得$p-1=q\cdot d$. 这样有因式分解式:

$$x^{p-1}-1=(x^d)^p-1=(x^{d(p-1)}+x^{d(p-2)}+\cdots+x^d+1)(x^d-1).$$

根据定理3.4.5, 多项式x^d-1 模p 有d 个不同的根. 证毕

例3.4.3判断同余式

$$2x^3+5x^2+6x+1\equiv 0 \pmod 7$$

是否有三个解.

解 为应用定理3.4.5, 须将多项式变成首一的. 注意到$4\cdot 2\equiv 1 \pmod 7$, 我们有

$$4(2x^3+5x^2+6x+1)\equiv x^3-x^2+3x-3 \pmod 7.$$

此同余式与原同余式等价. 作多项式的欧几里得除法, 我们有

$$x^7-x=x(x^3+x^2-2x-2)\cdot(x^3-x^2+3x-3)+7x(x^2-1).$$

根据定理3.4.5, 原同余式的解数为3.

例3.4.4 求解同余式

$$21x^{18}+2x^{15}-x^{10}+4x-3\equiv 0 \pmod 7.$$

解 首先, 去掉系数为7 的倍数的项, 得到

$$2x^{15}-x^{10}+4x-3\equiv \quad \pmod 7.$$

其次, 作多项式的欧几里得除法, 我们有

$$2x^{15}-x^{10}+4x-3=(2x^8-x^3+2x^2)(x^7-x)+(-x^4+2x^3+4x-3).$$

原同余式等价于同余式

$$x^4-2x^3-4x+3\equiv 0 \pmod 7.$$

直接验算$x=0,\pm1,\pm2,\pm3$, 知同余式无解.

例3.4.5 求解同余式

$$3x^{14}+4x^{13}+2x^{11}+x^9+x^6+x^3+12x^2+x\equiv 0 \pmod 5.$$

解一 作多项式的欧几里得除法, 我们有

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

应用定理3.4.1 , 原同余式等价于

$$3x^3+16x^2+6x\equiv 3x^3+x^2+x \pmod 5.$$

直接验算, 解为

$$x\equiv 0,\ 1,\ 2 \pmod 5.$$

解二 应用定理2.4.2 之推论, 对于任意正整数t, k,

$$x^{t+k(p-1)} \equiv x^t \pmod p.$$

我们有($p=5$),

$$\begin{aligned} &x^{14} \equiv x^{10} \equiv x^6 \equiv x^2, \quad x^{13} \equiv x^9 \equiv x^5 \equiv x, \\ &x^{11} \equiv x^7 \equiv x^3, \qquad\qquad \pmod 5. \end{aligned}$$

因此, 原同余式等价于

$$3x^3 + 16x^2 + 6x \equiv 0 \pmod 5.$$

进而等价于

$$2(3x^3 + 16x^2 + 6x) \equiv x^3 - 3x^2 + 2x \equiv x(x-1)(x-2) \equiv 0 \pmod 5.$$

直接验算, 同余式的解为

$$x \equiv 0,\ 1,\ 2 \pmod 5.$$