初等数论
第三章 同余方程

卢 伟
Email: luwei3@mail.sysu.edu.cn

中山大学 数据科学与计算机学院

1. 基本概念

- 同余式：

$m \in \mathbb{Z}^+$, 称

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

为模m同余式，其中$a_i \in \mathbb{Z}, i = 1, 2, \cdots, n$
如果$m \nmid a_n$, 称为多项式$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$的次数，记为$\deg f$. 这样上述同余式就称为模$m$的$n$次同余式.
如果恰好有$a \in \mathbb{Z}$, $s.t., a_n a^n + a_{n-1}a^{n-1} + \cdots + a_1 a + a_0 \equiv 0 \bmod m$, 这个$a$就称为上述同余式的一个解。
这时可以验证：如果a是同余式的一个解，则所有满足$a' \equiv a \bmod m$的a'也都是该同余式的解，换句话说，a所在的剩余类

$$C_a = \{a' | a \in \mathbb{Z}, a' \equiv a \bmod m\}$$

中的任一元素也都满足该同余式。这些解可以看做是相同的，把他们的全体算作该同余式的一个解。

这样，我们一般把同余式的解写成模m同余的形式，比如$x \equiv a \bmod m$

当a_1, a_2都是同余式的解，并且他们对模m不同余(即$a_1 \bmod m$和$a_2 \bmod m$是不同的剩余类)时，才把它们看作是同余式的不同的解。

把所有对模m两两不同余的同余式的解的个数(即满足同余式的模m的剩余类的个数)称为该同余式的解数.

因此,我们只要在模m的一组完全剩余系中来解模m的同余式即可. 显然, 模m同余式的解数至多为m.

示例:

$$x^5 + x + 1 \equiv 0 \bmod 7$$

是模7的5次同余式,

$$\because 2^5 + 2 + 1 \equiv 0 \bmod 7$$

所以, $x \equiv 2 \bmod 7$是该同余式的一个解.

类似的,可以检查到$x \equiv 4 \bmod 7$也是该同余式的一个解.

但

$$1^5 + 1 + 1 \not\equiv 0 \bmod 7$$

所以$x \equiv 1 \bmod 7$不是该同余式的解. 类似地,可以检查$x \equiv 3 \bmod 7, x \equiv 5 \bmod 7, x \equiv 6 \bmod 7, x \equiv 0 \bmod 7$都不是该同余式的解.

所以该同余式的解数为2.

定理

$m \in \mathbb{Z}^{+}, m \nmid a, d = (a, m)$,则$ax \equiv b \bmod m$有解 $\Longleftrightarrow$ $d|b$. 且当这个一次同余式有解的话, 解数必为d.

证明: " $\Longrightarrow$ ": 该同余式有解

$$x \equiv x_0 \bmod m$$

也就是说,

$$m|(ax_0 - b)$$

所以我们有

$$\left.\begin{aligned} (a,m)|m, m|(ax_0 - b) \Longrightarrow (a,m)|(ax_0 - b) \\ (a,m)|a \Longrightarrow (a,m)|(ax_0) \end{aligned}\right\} \Longrightarrow (a,m)|b$$

" $\Longleftarrow$ ": 设$d = (a, m)$, 这样我们知道$\frac{a}{d}$与$\frac{m}{d}$互素,从而存在s, t使得

$$s \cdot \frac{a}{d} + t \cdot \frac{m}{d} = 1$$

即

$$\frac{m}{d}|(\frac{a}{d}\cdot s-1)$$

从而

$$\frac{m}{d}|(\frac{a}{d}\cdot s-1)\cdot\frac{b}{d}$$

即

$$\frac{m}{d}|[\frac{a}{d}\cdot(s\cdot\frac{b}{d})-\frac{b}{d}]$$

从而我们有

$$m|[a\cdot(s\cdot\frac{b}{d})-b]$$

这说明$x\equiv s\cdot\frac{b}{d} \bmod m$是

$$ax\equiv b \bmod m$$

的一个解.
第一部分证完.

另一方面，如果同时有两个解: $x \equiv x_1 \bmod m, x \equiv x_2 \bmod m$使得

$$ax_1 \equiv b \bmod m, \quad ax_2 \equiv b \bmod m$$

所以:

$$a(x_1 - x_2) \equiv 0 \bmod m$$

从而(根据:$a \equiv b \bmod c, d|a, d|b, d|c \Rightarrow \frac{a}{d} \equiv \frac{b}{d} \bmod \frac{c}{d}$)

$$\frac{a}{d} \cdot (x_1 - x_2) \equiv 0 \bmod \frac{m}{d}$$

从而(根据:$ad \equiv bd \bmod m, (d, m) = 1 \Rightarrow a \equiv b \bmod m$)

$$x_1 - x_2 \equiv 0 \bmod \frac{m}{d}, i.e., x_1 \equiv x_2 \bmod \frac{m}{d}$$

即$x_1 = k \cdot \frac{m}{d} + x_2, k \in \mathbb{Z}$

所以, $ax \equiv b \bmod m$的全部解就是

$$x \equiv s \cdot \frac{b}{d} + k \cdot \frac{m}{d} \bmod m, \quad (k \in \mathbb{Z})$$

即

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

所以,求解一次同余式

$$ax \equiv b \bmod m$$

的步骤就是:

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

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

所以,求解一次同余式

$$ax \equiv b \bmod m$$

的步骤就是:

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

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

示例:
求解$33x \equiv 22 \bmod 77$, 这里$a=33, b=22, m=77$

$d=(a,m)=11$, d能够整除b, 所以有解.
$\frac{a}{d}=3, \frac{b}{d}=1, \frac{m}{d}=7$
$(3,7)=1$, 求出$3s+7t=1$的$s=5$;
$x \equiv s\cdot\frac{b}{d}+k\cdot\frac{m}{d} \bmod m, \quad (k=0,1,2,\cdots,d-1)$即为

$$x \equiv 5\cdot 2+k\cdot 7 \bmod 77, \quad k=0,1,2\cdots,10$$

因为$x_1 \equiv x_2 \bmod \frac{m}{d}$, 而$10 \equiv 3 \bmod 7$, 所以结果也可以写成$x \equiv 3 + 7k \bmod 77, k = 0, 1, 2, \ldots, 10$, 都表示$3, 10, 17, 24, 31, 38, 45, 52, 59, 66, 73$

此外, 根据这个定理, $(a, m) = 1 \Longrightarrow ax \equiv 1 \bmod m$有唯一解:
$d = 1$时,

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

就退化为

$$x \equiv s \cdot b \bmod m$$

逆元

$m \in \mathbb{Z}^+, a \in \mathbb{Z}$, 如果存在$a' \in \mathbb{Z}$使得

$$aa' \equiv 1 \bmod m$$

成立, 则称a为模m可逆元.

根据前面的结论, 我们知道这个逆元在模m的意义下是唯一的, 所以可称a'为a的模m可逆元, 记作$a^{-1} (\bmod m)$.

因此, 我们前面说的求解s使得$s \cdot \frac{a}{d} + t \cdot \frac{m}{d} = 1$, 或是使得$s \cdot \frac{a}{d} \equiv 1 \bmod \frac{m}{d}$, 这个$s$其实就是$\frac{a}{d}$模$\frac{m}{d}$的逆元.

这样一次同余式$ax \equiv b \bmod m$的解就可以表示为

$$x \equiv [(\frac{a}{d})^{-1} (\bmod \frac{m}{d})] \cdot \frac{b}{d} + k \cdot \frac{m}{d} \bmod m$$

类似地, 模m的简化剩余系也可以用逆元的概念来表述:
a是模m的简化剩余 $\Longleftrightarrow$ a是模m的可逆元.

推论

a是模m的简化剩余 $\Longleftrightarrow$ a是模m的可逆元.

"$\Longrightarrow$:" a是模m的简化剩余$\Longrightarrow$ $(a,m)=1$, 所以$ax \equiv 1 \bmod m$有解($\because d|b$), 也就是说存在a'使得$aa' \equiv 1 \bmod m$成立, 这就是说a是模m的可逆元.

"$\Longleftarrow$:" a是模m的可逆元$\Longrightarrow$ 存在整数a'使得$aa' \equiv 1 \bmod m$, 这就是说同余式$ax \equiv 1 \bmod m$有解, 所以应该有$d|b$, 所以$d=1$, 即a与m互素, 从而a是模m的简化剩余.

2. 中国剩余定理(孙子定理)

设$f_1(x), f_2(x), \ldots, f_k(x)$是整系数多项式, 我们把含有变量$x$的一组同余式

$$\begin{cases} f_1(x) \equiv 0 \bmod m_1 \\ f_2(x) \equiv 0 \bmod m_2 \\ \cdots\cdots \\ f_k(x) \equiv 0 \bmod m_k \end{cases}$$

称为是同余方程组 如有整数c满足

$$\begin{cases} f_1(c) \equiv 0 \bmod m_1 \\ f_2(c) \equiv 0 \bmod m_2 \\ \cdots\cdots \\ f_k(c) \equiv 0 \bmod m_k \end{cases}$$

则称c是这个同余方程组的解.

令$m=[m_1,m_2,\ldots,m_k]$, 如果c是同余方程组的解, 而且$c'\equiv c \bmod m$, 则$c'\equiv c \bmod m_1$, 从而$f_1(c')\equiv f_1(c) \bmod m_1$, 从而$f_1(c')\equiv 0 \bmod m_1$,

同样的, 由$c'\equiv c \bmod m$, 知$c'\equiv c \bmod m_2$, 从而$f_2(c')\equiv f_2(c) \bmod m_2$, 从而$f_2(c')\equiv 0 \bmod m_2$,..., $f_k(c')\equiv 0 \bmod m_k$,

亦即与c模m同余的c'也满足这个同余方程组.

这样c所在的剩余类中的每个元素都是这个同余方程组的解, 它们可以看作是一个解, 记为$x\equiv c \bmod m$.
只有当c_1和c_2都是这个同余式组的解, 且c_1和c_2对模m不同余时, 才把它们看作是这个同余式方程组的不同的解.

把所有对模m不同余的解的个数称为是这个同余方程组的解数. 因此,我们只需要在模m的一组完全剩余系中来求解这个方程组, 它们的解数至多为m.

另外, 只要同余方程组中任一同余方程无解, 那么整个方程组自然也无解.

孙子定理

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

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

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

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

关于唯一性, 比较简单: 假设r与s都满足上述同余式组:

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

从而有

$$\begin{cases} r \equiv s \bmod m_1 \\ r \equiv s \bmod m_2 \\ \ldots\ldots \\ r \equiv s \bmod m_k \end{cases}$$

从而

$$r \equiv s \bmod [m_1, m_2, \ldots, m_k]$$

而$m_1, m_2, \ldots, m_k$两两互素($[m_1, m_2] = \frac{m_1 m_2}{(m_1, m_2)} = m_1 m_2$, $[m_1, m_2, m_3] = [[m_1, m_2], m_3] = [m_1 m_2, m_3] = \frac{m_1 m_2 m_3}{(m_1 m_2, m_3)} = m_1 m_2 m_3, \ldots$, $[m_1, m_2, \ldots, m_k] = m_1 m_2 \ldots m_k$), 所以

$$r \equiv s \bmod (m_1 m_2 \ldots m_k), \quad r \equiv s \bmod M$$

即r与s在模M意义下相等.

再看存在性：构造型证明.

$$(m_1, m_2) = 1, (m_1, m_3) = 1, \ldots, (m_1, m_k) = 1 \Longrightarrow (m_1, m_2 m_3 \ldots m_k) = 1$$

即

$$(m_1, M_1) = 1$$

从而

$$M_1 y \equiv 1 \bmod m_1$$

有解，记为M_1'：$M_1' M_1 \equiv 1 \bmod m_1$
类似地，可以构造出

$$M_2' M_2 \equiv 1 \bmod m_2, M_3' M_3 \equiv 1 \bmod m_3, \ldots, M_k' M_k \equiv 1 \bmod m_k$$

计算整数

$$M_1' M_1 b_1 + M_2' M_2 b_2 + M_3' M_3 b_3 + \ldots + M_k' M_k b_k$$

我们可以检查

$$M_1' M_1 b_1 + M_2' M_2 b_2 + M_3' M_3 b_3 + \ldots + M_k' M_k b_k \equiv b_1 \bmod m_1$$

$$M_1' M_1 b_1 + M_2' M_2 b_2 + M_3' M_3 b_3 + \ldots + M_k' M_k b_k \equiv b_2 \bmod m_2$$

$$\cdots\cdots$$

$$M_1' M_1 b_1 + M_2' M_2 b_2 + M_3' M_3 b_3 + \ldots + M_k' M_k b_k \equiv b_k \bmod m_k$$

所以数字$M_1' M_1 b_1 + M_2' M_2 b_2 + M_3' M_3 b_3 + \ldots + M_k' M_k b_k$是满足上述同余式组的一个解.

又根据唯一性证明知道:
任意两个同余式组的解r, s模M同余:$r \equiv s \bmod M$, 所以同余式组的解就可以表达为:

$$x \equiv M_1' M_1 b_1 + M_2' M_2 b_2 + M_3' M_3 b_3 + \ldots + M_k' M_k b_k \bmod M$$

$\diamond$

有了上述的证明过程, 我们在回过来看中国剩余定理表达的意思: 它一方面说明了要求同余式组

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

的解(其中模数$m_1, m_2, \ldots, m_k \in \mathbb{Z}^+$, 两两互素), 只要写出表达式

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

就可以了, 此即为该同余式组的解;

另一方面, 如果给定了数字$M_1' M_1 b_1 + M_2' M_2 b_2 + \ldots + M_k' M_k b_k$(或是与它模$M$同余的数字, 可能是一个很大的数字), 要求计算它模M后的值, 我们只需要将M分解成两两互素的$m_1, m_2, \ldots, m_k$之后, 计算这个大数字模m_1后的值记为b_1, 计算这个大数字模m_2后的值记为b_2, …, 计算这个大数字模m_k后的值记为b_k, 建立一个同余式组

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

要求那个大数字模M后的值, 就只要求解这个同余式组的解即可.

计算$2^{1000000} \bmod 77$

$77 = 7 \times 11$

$$1000000 = 166666 \times 6 + 4 \Longrightarrow 2^{1000000} \equiv 2 \bmod 7, i.e., b_1 = 2$$

$$1000000 = 100000 \times 10 \Longrightarrow 2^{1000000} \equiv 1 \bmod 11, i.e., b_2 = 1$$

求解同余式组

$$\begin{cases} y \equiv 2 \bmod 7 \\ y \equiv 1 \bmod 11 \end{cases}$$

对这个同余式组, $m_1 = 7$, $m_2 = 11$, $M_1 = 11$, $M_2 = 7$, $M = 77$, $M_1' = 2$, $M_2' = 8$, 从而同余式组的解为23, 从而

$$2^{1000000} \bmod 77 = 23$$

(注: 模指数运算自然也可以直接通过模重复平方计算法求出)

示例: 求解同余式组

$$\begin{cases} x \equiv 1 \bmod 3 \\ x \equiv -1 \bmod 5 \\ x \equiv 2 \bmod 7 \\ x \equiv -2 \bmod 11 \end{cases}$$

$$m_1 = 3, m_2 = 5, m_3 = 7, m_4 = 11, M = 3 \cdot 5 \cdot 7 \cdot 11 = 1155$$

$$M_1 = 5 \cdot 7 \cdot 11, M_2 = 3 \cdot 7 \cdot 11, M_3 = 3 \cdot 5 \cdot 11, M_4 = 3 \cdot 5 \cdot 7$$

$$M_1' = 1, M_2' = 1, M_3' = 2, M_4' = 2$$

所以同余式组的解为:

$$x \equiv 385 - 231 + 660 - 420 \bmod 1155$$

即

$$x \equiv 394 \bmod 1155$$

示例: 求解同余式组

$$\begin{cases} x \equiv b_1 \bmod 5 \\ x \equiv b_2 \bmod 6 \\ x \equiv b_3 \bmod 7 \\ x \equiv b_4 \bmod 11 \end{cases}$$

$$m_1 = 5, m_2 = 6, m_3 = 7, m_4 = 11, M = 5 \cdot 6 \cdot 7 \cdot 11 = 2310$$

$$M_1 = 462, M_2 = 385, M_3 = 330, M_4 = 210$$

$$M_1' = 3, M_2' = 1, M_3' = 1, M_4' = 1$$

所以同余式组的解为:

$$x \equiv 3 \times 462 \times b_1 + 385 \times b_2 + 330 \times b_3 + 210 \times b_4 \bmod 2310$$

示例: 求解同余式组$\begin{cases} x \equiv 3 \bmod 8 \\ x \equiv 11 \bmod 20 \\ x \equiv 1 \bmod 15 \end{cases}$

这里的模数$8, 20, 15$不是两两互素的, 所以无法直接使用孙子定理. 需要对这个方程组做变形.

事实上容易看到第二个同余方程等价于方程组:

$$\begin{cases} x \equiv 11 \bmod 4 \\ x \equiv 11 \bmod 5 \end{cases}$$

事实上容易看到第三个同余方程等价于方程组:

$$\begin{cases} x \equiv 1 \bmod 3 \\ x \equiv 1 \bmod 5 \end{cases}$$

这样要求解同余方程组就等价于求解同余方程组

$$\begin{cases} x \equiv 3 \bmod 8 & (1) \\ x \equiv 11 \bmod 4 & (2) \\ x \equiv 11 \bmod 5 & (3) \\ x \equiv 1 \bmod 3 & (4) \\ x \equiv 1 \bmod 5 & (5) \end{cases}$$

$$\begin{cases} x \equiv 3 \bmod 8 & (1) \\ x \equiv 11 \bmod 4 & (2) \\ x \equiv 11 \bmod 5 & (3) \\ x \equiv 1 \bmod 3 & (4) \\ x \equiv 1 \bmod 5 & (5) \end{cases}$$

这里可以看到:
满足(1)式的整数$x_0 : 8|(x_0 - 3)$, 对这个整数自然也有$4|(x_0 - 3)$, 而$4|8$, 所以也有$4|(x_0 - 11)$, 即这个整数也满足$x_0 \equiv 11 \bmod 4$, 这也就意味着凡是式(1)的解就肯定是式(2)的解, 这样, 在上述同余式组中可以不要式(2);
满足(5)式的整数$x_0 : 5|(x_0 - 1)$, 而$5|10$, 所以对这个整数自然也有$5|(x_0 - 11)$, 即这个整数也满足$x_0 \equiv 11 \bmod 5$, 这也就意味着凡是式(5)的解就肯定是式(3)的解, 这样, 在上述同余式组中可以不要式(3);
所以我们就得到一个等价的同于方程组:

$$\begin{cases} x \equiv 3 \bmod 8 & (1) \\ x \equiv 1 \bmod 3 & (4) \\ x \equiv 1 \bmod 5 & (5) \end{cases}$$

这个方程组满足孙子定理条件, 可以使用孙子定理求解.
这个例子告诉我们在模不两两互素情况下的同余方程组的求解方法.

示例: 求解同余式组

$$\begin{cases} x \equiv 3 \bmod 7 \\ 6x \equiv 10 \bmod 8 \end{cases}$$

这个同余方程组不是孙子定理所适用的形式,
但我们可以将它转换为满足孙子定理的形式:
考虑同余式$6x \equiv 10 \bmod 8$: 可以看到它确实有解且解数为2:

$$x \equiv -1 \bmod 8 \ \text{和} \ x \equiv 3 \bmod 8$$

这样要求解的同余方程组就相当于要求解两个同余方程组了:

$$\begin{cases} x \equiv 3 \bmod 7 \\ x \equiv -1 \bmod 8 \end{cases}$$

和

$$\begin{cases} x \equiv 3 \bmod 7 \\ x \equiv 3 \bmod 8 \end{cases}$$

它们的解分别为$x \equiv 31 \bmod 56, x \equiv 3 \bmod 56$, 原同余方程组的解也就出来了.

3. 同余方程的恒等变形

如同为了求解代数方程需要对代数方程进行恒等变形一样，为了求解同余方程也需要利用同余的性质对同余方程进行变形，也就是把要求解的同余方程变为解完全相同的另一个同余方程(称两个同余方程是等价的)，而后者更易于求解．我们现在就给出几个恒等变形.

(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$\forall x_0 \in \mathbb{Z}$:

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

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

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

这也就说明了: x_0使得$f(x_0) \equiv 0 \bmod m$当且仅当x_0使得$f(x_0) + ms(x_0) \equiv 0 \bmod m$.
也就是说, 一个整数是方程$f(x) \equiv 0 \bmod m$的解, 当且仅当这个整数是方程$f(x) + ms(x) \equiv 0 \bmod m$的解.

比如, $4x^2 - 3x + 3 \equiv 0 \bmod 15 \iff 4x^2 - 3x + 3 + 15(x-1) \equiv 0 \bmod 15$, 也就是说, 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, 则同余方程$f(x) \equiv 0 \bmod m$与同余方程$f(x) + s(x) \equiv s(x) \bmod m$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$\forall x_0 \in \mathbb{Z}$:

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

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

这个式子也就说明了: 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, 一个整数是方程$f(x) \equiv 0 \bmod m$的解当且仅当这个整数是方程$f(x) + s(x) \equiv s(x) \bmod m$的解.

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

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

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

这个结论显然成立:
因为a与m互素, 所以对$\forall x_0\in\mathbb{Z}$:

$$m|f(x_0) \iff m|af(x_0)$$

即

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

这个式子也就说明了: 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, 一个整数是方程$f(x)\equiv 0 \bmod m$的解当且仅当这个整数是方程$af(x)\equiv 0 \bmod m$的解.

比如, $4x^2+12x-12\equiv 0 \bmod 15 \iff x^2+3x-3\equiv 0 \bmod 15$;
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.
这三个性质可以交替使用: 比如2与15互素, 所以同余方程$7x^6+6\equiv 0 \bmod 15$与$2(7x^6+6)\equiv 0 \bmod 15$ 等价, 后者即方程$14x^6+12\equiv 0 \bmod 15$, 它又与方程$(14x^6+12)+15(-x^6-1)\equiv 0 \bmod 15$即$-x^6-3\equiv 0 \bmod 15$等价, 而$-1$与15互素, 所以$-x^6-3\equiv 0 \bmod 15$与$(-1)(-x^6-3)\equiv 0 \bmod 15$即$x^6+3\equiv 0 \bmod 15$等价, 从而我们可以说同余方程$7x^6+6\equiv 0 \bmod 15$与$x^6+3\equiv 0 \bmod 15$等价.

(3-4) 设同余方程$h(x) \equiv 0 \bmod m$有m个解(即任意整数带入此式都成立，比如$x^p - x \equiv 0 \bmod p$)，如果有整系数多项式$q(x)$, $r(x)$ 使得$f(x) = q(x)h(x) + r(x)$，则同余方程等价：

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

这个结论显然成立：
因为对$\forall x_0 \in \mathbb{Z} : f(x_0) = q(x_0)h(x_0) + r(x_0)$

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

这个式子也就说明了：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，一个整数是方程$f(x) \equiv 0 \bmod m$的解当且仅当这个整数是方程$r(x) \equiv 0 \bmod m$的解.

比如：多项式$f(x) = 2x^7 - x^5 - 3x^3 + 6x + 1 = (2x^2 - 1)(x^5 - x) + (-x^3 + 5x + 1)$，而对任意整数$x^5 - x \equiv 0 \bmod 5$，所以$2x^7 - x^5 - 3x^3 + 6x + 1 \equiv 0 \bmod 5 \iff -x^3 + 5x + 1 \equiv 0 \bmod 5$，而同余方程$-x^3 + 5x + 1 \equiv 0 \bmod 5$与同余方程$-x^3 + 1 \equiv 0 \bmod 5$等价，同余方程$-x^3 + 1 \equiv 0 \bmod 5$与同余方程$x^3 - 1 \equiv 0 \bmod 5$等价，同余方程$x^3 - 1 \equiv 0 \bmod 5$与同余方程$x^3 \equiv 1 \bmod 5$等价，所以$2x^7 - x^5 - 3x^3 + 6x + 1 \equiv 0 \bmod 5 \iff x^3 \equiv 1 \bmod 5$

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$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$,
$g(x) = x^m + b_{m-1}x^{m-1} + \ldots + b_1 x + b_0$, 则存在整系数多项式$q(x)$和$r(x)$使得:
$f(x) = g(x)q(x) + r(x)$, 且$\deg(r(x)) < \deg(g(x))$.

这里可以看到, 如果$g(x)$的次数m比$f(x)$的次数n大的话, 直接去$q(x) = 0$,
$r(x) = f(x)$: $f(x) = g(x) \cdot 0 + f(x)$即满足要求.

如果f的次数比g的大:

$$\begin{array}{rl} & x^4 \\ x^3-x^2+3x-3 \,\big) & x^7-x \\ - & x^7-x^6+3x^5-3x^4 \\ \hline & x^6-3x^5+3x^4-x \end{array}$$

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:
整系数多项式$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$,
$g(x) = x^m + b_{m-1}x^{m-1} + \ldots + b_1 x + b_0$, 则存在整系数多项式$q(x)$和$r(x)$使得:
$f(x) = g(x)q(x) + r(x)$, 且$\deg(r(x)) < \deg(g(x))$.

这里可以看到, 如果$g(x)$的次数m比$f(x)$的次数n大的话, 直接去$q(x) = 0$,
$r(x) = f(x)$: $f(x) = g(x) \cdot 0 + f(x)$即满足要求.

如果f的次数比g的大:

$$
\begin{array}{r l}
 & x^4+x^3 \\
x^3-x^2+3x-3 \;\big/ & x^7-x \\
- & x^7-x^6+3x^5-3x^4 \\
\hline
 & x^6-3x^5+3x^4-x \\
- & x^6-x^5+3x^4-3x^3 \\
\hline
 & -2x^5+3x^3-x
\end{array}
$$

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:
整系数多项式$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$,
$g(x) = x^m + b_{m-1}x^{m-1} + \ldots + b_1 x + b_0$, 则存在整系数多项式$q(x)$和$r(x)$使得:
$f(x) = g(x)q(x) + r(x)$, 且$\deg(r(x)) < \deg(g(x))$.

这里可以看到, 如果$g(x)$的次数m比$f(x)$的次数n大的话, 直接去$q(x) = 0$,
$r(x) = f(x)$: $f(x) = g(x) \cdot 0 + f(x)$即满足要求.

如果f的次数比g的大:

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

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:
整系数多项式$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$,
$g(x) = x^m + b_{m-1}x^{m-1} + \ldots + b_1 x + b_0$, 则存在整系数多项式$q(x)$和$r(x)$使得:
$f(x) = g(x)q(x) + r(x)$, 且$\deg(r(x)) < \deg(g(x))$.

这里可以看到, 如果$g(x)$的次数m比$f(x)$的次数n大的话, 直接去$q(x) = 0$,
$r(x) = f(x)$: $f(x) = g(x) \cdot 0 + f(x)$即满足要求.

如果f的次数比g的大:

$$
\begin{array}{rl}
 & x^4+x^3-2x^2-2x+7 \\
x^3-x^2+3x-3 \,\big/ & x^7-x \\
- & x^7-x^6+3x^5-3x^4 \\
\hline
 & x^6-3x^5+3x^4-x \\
- & x^6-x^5+3x^4-3x^3 \\
\hline
 & -2x^5+3x^3-x \\
- & -2x^5+2x^4-6x^3+6x^2 \\
\hline
 & -2x^4+9x^3-6x^2-x \\
- & -2x^4+2x^3-6x^2+6x \\
\hline
 & 7x^3-6x-x \\
- & 7x^3-7x^2+21x-21 \\
\hline
 & 7x^2-28x+21
\end{array}
$$

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，则同余方程$f(x) \equiv 0 \bmod m$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.

这也是显然的：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：如果同余方程$f(x) \equiv 0 \bmod d$ 无解，则同余方程$f(x) \equiv 0 \bmod m$ 无解.

比如，为了说明$4x^2 + 27x - 9 \equiv 0 \bmod 15$ 无解，只需要说明$4x^2 + 27x - 9 \equiv 0 \bmod 5$ 无解，而同余方程$4x^2 + 27x - 9 \equiv 0 \bmod 5 \iff -x^2 + 2x + 1 \equiv 0 \bmod 5 \iff (x-1)^2 \equiv 2 \bmod 5$，可以验算最后的这个同余方程无解，所以可以说同余方程$4x^2 + 27x - 9 \equiv 0 \bmod 15$ 无解.

4. 高次同余式

(4.1.) 一般高次同余式

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

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

与同余式组

$$\begin{cases} f(x) \equiv 0 \bmod m_1 & (2.1) \\ f(x) \equiv 0 \bmod m_2 & (2.2) \\ \cdots\cdots & \\ f(x) \equiv 0 \bmod m_k & (2.k) \end{cases} \qquad (2)$$

等价. 即

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

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$T = T_1 T_2 \ldots T_k$.

$m_1, m_2, \ldots, m_k \in \mathbb{Z}^+$两两互素, $m = m_1 m_2 \ldots m_k$, 则

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

设$f(x) \equiv 0 \bmod m_i (i = 1, \ldots, k)$的解数为$T_i$, $f(x) \equiv 0 \bmod m$的解数为T, 则$T = T_1 T_2 \ldots T_k$.

事实上: 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: $a \equiv b \bmod m, d|m \Longrightarrow a \equiv b \bmod d$), 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

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

即$f(x_0)$是$m_1, m_2, \dots, m_k$的公倍数, 所以有$m_1, m_2, \dots, m_k$的最小公倍数应该整除$f(x_0)$, 即$[m_1, m_2, \dots, m_k] | f(x_0)$, 又因为$m_1, m_2, \dots, m_k$两两互素, 所以$[m_1, m_2, \dots, m_k] = m_1 \cdot m_2 \cdot \dots \cdot m_k$, 则有$m_1 \cdot m_2 \cdot \dots \cdot m_k | f(x_0)$, 即

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

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

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

设同余方程组(2)中:
第1个同余方程的解为$x \equiv a_{11} \bmod m_1, x \equiv a_{12} \bmod m_1, \dots, x \equiv a_{1T_1} \bmod m_1$
第2个同余方程的解为$x \equiv a_{21} \bmod m_2, x \equiv a_{22} \bmod m_2, \dots, x \equiv a_{2T_2} \bmod m_2$
$\dots\dots$
第k个同余方程的解为$x \equiv a_{k1} \bmod m_k, x \equiv a_{k2} \bmod m_k, \dots, x \equiv a_{kT_k} \bmod m_k$
设同余方程(1)的解为$x \equiv b_1 \bmod m, x \equiv b_2 \bmod m, \dots, x \equiv b_T \bmod m$
对同余方程(1)的解b_1来说,

$$m|f(b_1)\begin{cases}\Longrightarrow m_1|f(b_1) \Longrightarrow b_1\text{是(2.1)的一个解} \Longrightarrow \exists a_{1j_1}, s.t., b_1 \equiv a_{1j_1} \bmod m_1\\ \Longrightarrow m_2|f(b_1) \Longrightarrow b_1\text{是(2.2)的一个解} \Longrightarrow \exists a_{2j_2}, s.t., b_1 \equiv a_{2j_2} \bmod m_2\\ \dots\dots\\ \Longrightarrow m_k|f(b_1) \Longrightarrow b_1\text{是(2.k)的一个解} \Longrightarrow \exists a_{kj_k}, s.t., b_1 \equiv a_{kj_k} \bmod m_k\end{cases}$$

这也就是说, 对(1)的解b_1, $(2.1) \sim (2.k)$有唯一的一组数$(a_{1j_1}, a_{2j_2}, \dots, a_{kj_k})$(比如$(a_{11}, a_{21}, \dots, a_{k1})$)与它相对应.
类似可以分析,
对(1)的解b_2, $(2.1) \sim (2.k)$有唯一的一组数与它对应,
$\dots\dots$,
对(1)的解b_T, $(2.1) \sim (2.k)$有唯一的一组数与它对应,
对(2)来说, 这样的数字有$T_1T_2\dots T_k$个, 所以$T \le T_1T_2\dots T_k$.
下面我们反过来说明对每一个这样的一组数(比如$(a_{11}, a_{21}, \dots, a_{k1})$), 也能够找到一个$b_i$(比如$b_i$)与之相对应, 这样就有$T_1T_2\dots T_k \le T$, 从而$T = T_1T_2\dots T_k$

事实上,给定一组这样的数，比如$(a_{11}, a_{21}, \ldots, a_{k1})$，
这就意味着$x \equiv a_{11} \bmod m_1$ 是(2.1)的解，$x \equiv a_{21} \bmod m_2$ 是(2.2)的解，...，
$x \equiv a_{k1} \bmod m_k$ 是(2.k)的解，
这样可以建立同余方程组

$$\begin{cases} x \equiv a_{11} \bmod m_1 \\ x \equiv a_{21} \bmod m_2 \\ \cdots\cdots \\ x \equiv a_{k1} \bmod m_k \end{cases}$$

我们知道它存在唯一解，记为$x \equiv c \bmod m$(即c与a_{11}模m_1同余，与a_{21}模m_2同余，...，与a_{k1}模m_k同余)，从而$f(c) \equiv f(a_{11}) \bmod m_1$，$f(c) \equiv f(a_{21})$，...，$f(c) \equiv f(a_{k1})$，从而$f(c) \equiv 0 \bmod m_1$，$f(c) \equiv 0 \bmod m_2$，...，$f(c) \equiv 0 \bmod m_k$，即$c$满足同于方程组(2)，所以它也是同余方程(1)的解.
这样就存在唯一一个b_i使得$c \equiv b_i \bmod m$，也就是说，给定一组数$(a_{11}, a_{21}, \ldots, a_{k1})$，存在唯一一个$b_i$与之对应，所以$T_1 T_2 \ldots T_k \leq T$. $\diamond$

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. 求解$f(x) \equiv 0 \bmod m_1$得到a_{11}, 求解$f(x) \equiv 0 \bmod m_2$得到a_{21}, ... , 求解$f(x) \equiv 0 \bmod m_k$得到a_{k1};
3. 求解同余式组

$$\begin{cases} x \equiv a_{11} \bmod m_1 \\ x \equiv a_{21} \bmod m_2 \\ \ldots\ldots \\ x \equiv a_{k1} \bmod m_k \end{cases}$$

4. 得到全部$T_1 T_2 \ldots T_k$个解.

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

$$\begin{cases} x\equiv a_1 \bmod 5 \\ x\equiv a_2 \bmod 7 \end{cases}$$

的解为

$$x\equiv 21a_1+15a_2 \bmod 35$$

将$a_1=1$或4, $a_2=3$或5或6代入记得$x^4+2x^3+8x+9\equiv 0 \bmod 35$的6个解.

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. 求解$f(x) \equiv 0 \bmod m_1$得到a_{11}, 求解$f(x) \equiv 0 \bmod m_2$得到a_{21}, ... , 求解$f(x) \equiv 0 \bmod m_k$得到a_{k1};
3. 求解同余式组

$$\begin{cases} x \equiv a_{11} \bmod m_1 \\ x \equiv a_{21} \bmod m_2 \\ \ldots\ldots \\ x \equiv a_{k1} \bmod m_k \end{cases}$$

4. 得到全部$T_1 T_2 \ldots T_k$个解.

当m的素因数分解式

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

时, 我们可以取$m_1 = p_1^{\alpha_1}$, $m_2 = p_2^{\alpha_2}$, ... , $m_k = p_k^{\alpha_k}$
这样解一般模数的同余方程$f(x) \equiv 0 \bmod m$, 就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: 如果同余方程

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

有解, 另外有正因子$d|m$, 则同余方程

$$f(x) \equiv 0 \bmod d \qquad (2)$$

也有解. 设$x \equiv c_1 \bmod d$, $x \equiv c_2 \bmod d$, ... , $x \equiv c_s \bmod d$ 为(2)的全部解, $x \equiv a_1 \bmod m$为(1)的一个解, 则$c_1, c_2, \ldots, c_k$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(1)的解, 即有$m|f(x_0)$, 从而$d|f(x_0)$, 即$f(x_0) \equiv 0 \bmod d$, 即$x \equiv x_0 \bmod m$必定也是(2)的解, 所以定理第一部分成立.

如果$x \equiv a \bmod m$为(1)的一个解, 根据前一部分的证明知道, 它肯定也是(2)的解, 而$x \equiv c_1 \bmod d$, $x \equiv c_2 \bmod d$, ... , $x \equiv c_s \bmod d$ 为(2)的全部解, 所以a必定处于这模d的s个剩余类中的一个, 比如处于第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. $\diamond$

这个结论告诉我们, 为了求较大模m的同余方程的解, 可以先找一个较小的正因子d, 求出模d的同余方程(2)的全部解((2)无解的话当然(1)肯定无解)

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

对(1)的每个解$x \equiv a \bmod m$, 我们知道对这个a有且仅有一个c_i(比如c_1)使得$a \equiv c_1 \bmod d$, 即$a = dk + c_1$, 所以应该有$f(dk + c_1) \equiv 0 \bmod m$成立, 对左边加以整理, 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$k$的同余方程非常简单便于求解(比如一次方程), 我们就可以得到对应于这个c_1的(1)的解.

对每个c_i都这么做, 我们就可以得到(1)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(从而使易求的)?

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，如前所述，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

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

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

$\ldots\ldots$

$$(c+kd)^2=c^2+2c(kd)+(kd)^2$$
$$(c+kd)^1=c+kd$$
$$a_n(c+kd)^n=a_nc^n+a_nnc^{n-1}(kd)+a_n@\cdot(kd)^2+a_n@\cdot(kd)^3+\ldots+a_n@\cdot(kd)^n$$
$$a_{n-1}(c+kd)^{n-1}=a_{n-1}c^{n-1}+a_{n-1}(n-1)c^{n-2}(kd)+a_{n-1}@\cdot(kd)^2+\ldots+$$
$$a_{n-2}(c+kd)^{n-2}=a_{n-2}c^{n-2}+a_{n-2}(n-2)c^{n-3}(kd)+a_{n-2}@\cdot(kd)^2+\ldots+$$

$\ldots\ldots$

$$a_2(c+kd)^2=a_2c^2+a_22c(kd)+a_2(kd)^2$$
$$a_1(c+kd)=a_1c+a_1(kd)$$
$$a_0=a_0$$

整理有: $a_0 + a_1 c + a_2 c^2 + a_3 c^3 + \ldots + a_{n-2} c^{n-2} + a_{n-1} c^{n-1} + a_n c^n$, 即$f(c)$.

kd的一次项: $a_1(kd) + a_2 2c(kd) + \ldots + a_{n-1}(n-1)c^{n-3}(kd) + a_n n c^{n-1}(kd)$,
即: $[a_1 + 2a_2 c + \ldots + (n-1)a_{n-1}c^{n-3} + n a_n c^{n-1}](kd)$,
用数学分析中导数的说法($f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_3 x^3 + a_2 x^2 + a_1 x + a_0 \Longrightarrow f'(x) = n a_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \ldots + 3a_3 x^2 + 2a_2 x + a_1$) 就是: $f'(c)(kd)$

其它都是(kd)的2次项, 3次项, 4次项, ..., n次项.
注意到由于$\alpha \geq 2$, 所以$2\alpha - 2 \geq \alpha$, 从而$p^\alpha | p^{2\alpha-2}$, 即(kd)的2次项是p^α的倍数, 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.

所以我们可以得道同余式:

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

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$k \equiv 0 \bmod p$, $k \equiv 1 \bmod p$, ..., $k \equiv p-1 \bmod p$;

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.

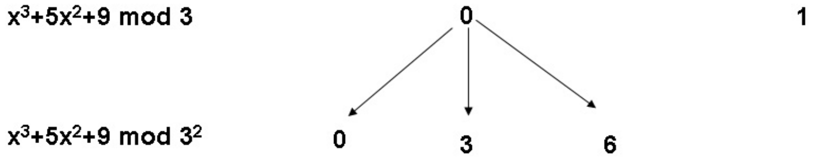
$x \equiv c + p^{\alpha-1} k_1 \bmod m$, 或者
$x \equiv c \bmod m$, $x \equiv c + p^{\alpha-1} \bmod m$, $x \equiv c + p^{\alpha-1} \cdot 2 \bmod m$, ... ,
$x \equiv c + p^{\alpha-1} \cdot (p-1) \bmod m$.

至此, 我们看到, 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$f(x) \equiv 0 \bmod p^{1}$,
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.

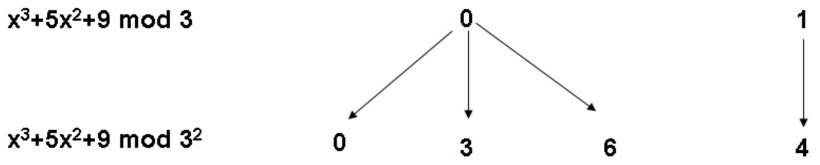
示例：求解$x^3+5x^2+9\equiv 0 \bmod 3^4$，即$p=3, f(x)=x^3+5x^2+9$，所以$f'(x)=3x^2+10x$.

必须先从$x^3+5x^2+9\equiv 0 \bmod 3$开始求解：检查$0,1,2$发现$x\equiv 0 \bmod 3, x\equiv 1 \bmod 3$是它的解，我们现在利用$x^3+5x^2+9\equiv 0 \bmod 3$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$k\equiv 0 \bmod 3$，$k\equiv 1 \bmod 3$，$k\equiv 2 \bmod 3$，从而得到对应于$x^3+5x^2+9\equiv 0 \bmod 3$的解$x\equiv 0 \bmod 3$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$x\equiv 0 \bmod 3^2$，$x\equiv 3 \bmod 3^2$，$x\equiv 6 \bmod 3^2$



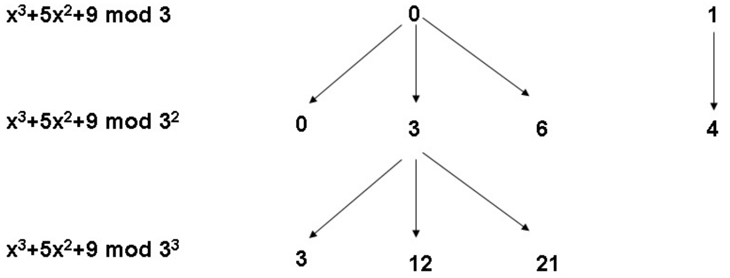
对$x^3+5x^2+9\equiv 0 \bmod 3$的解$x\equiv 1 \bmod 3$即$c=1$时，所以$f(c)=15$，$f'(c)=13$，
$\frac{-f(c)}{p^{\alpha-1}}=-5$，这时有$p\nmid f'(c)$，所以关于$k$的方程$13k\equiv -5 \bmod 3$有一个解，
即$k\equiv 1 \bmod 3$，从而得到对应于$x^3+5x^2+9\equiv 0 \bmod 3$的解$x\equiv 1 \bmod 3$
的$x^3+5x^2+9\equiv 0 \bmod 3^2$的解$x\equiv 1+3\cdot 1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



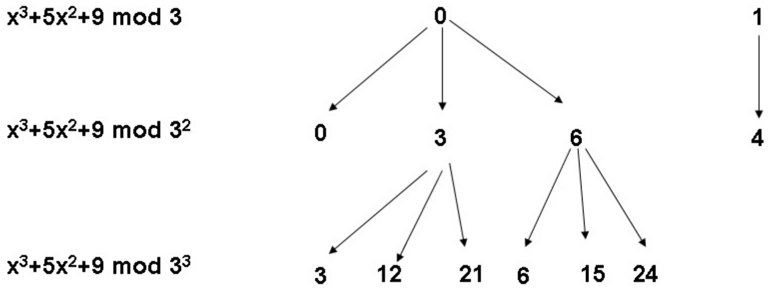
有了$x^3+5x^2+9\equiv 0 \bmod 3^2$的解$x\equiv 0 \bmod 3^2$, $x\equiv 3 \bmod 3^2$, $x\equiv 6 \bmod 3^2$, $x\equiv 4 \bmod 3^2$ 之后要利用他们来求方程$x^3+5x^2+9\equiv 0 \bmod 3^3$(即这是$\alpha=3$)的解:

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.

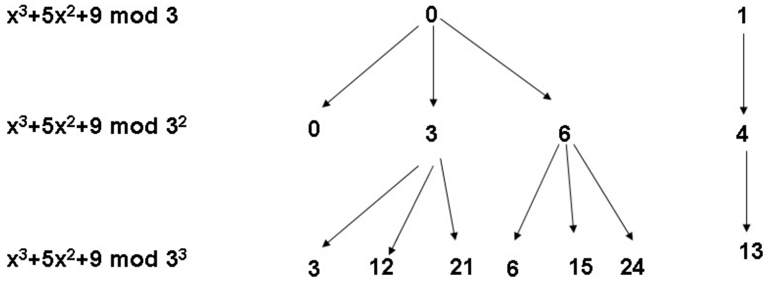
对$x^3+5x^2+9\equiv 0 \bmod 3^2$的解$x\equiv 3 \bmod 3^2$即$c=3$, 所以$f(c)=81$, $f'(c)=57$, $\frac{-f(c)}{p^{\alpha-1}}=-9$, 这时有$p|f'(c)$, $p|\frac{-f(c)}{p^{\alpha-1}}$, 所以关于$k$的方程有$p$个解: 即$k\equiv 0 \bmod 3$, $k\equiv 1 \bmod 3$, $k\equiv 2 \bmod 3$,
从而得到对应于$x^3+5x^2+9\equiv 0 \bmod 3^2$的解$x\equiv 3 \bmod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



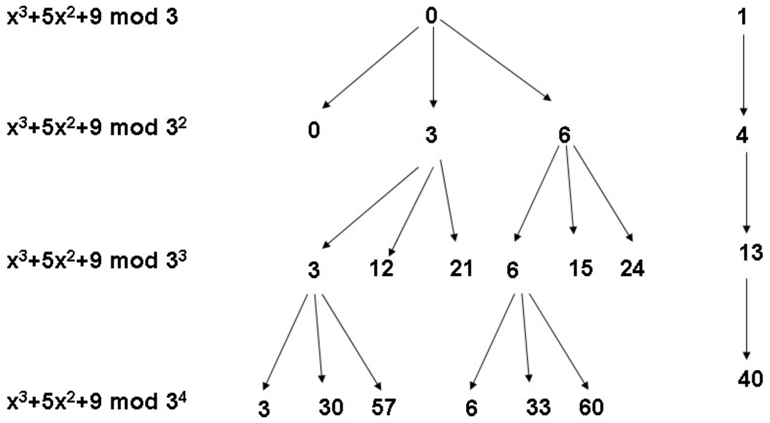
对$x^3+5x^2+9\equiv 0 \bmod 3^2$的解$x\equiv 6 \bmod 3^2$即$c=6$，所以$f(c)=405$，$f'(c)=168$，
$\frac{-f(c)}{p^{\alpha-1}}=-45$，这时有$p|f'(c)$，$p|\frac{-f(c)}{p^{\alpha-1}}$，所以关于$k$的方程有$p$个解：即$k\equiv 0 \bmod 3$，
$k\equiv 1 \bmod 3$，$k\equiv 2 \bmod 3$，
从而得到对应于$x^3+5x^2+9\equiv 0 \bmod 3^2$的解$x\equiv 6 \bmod 3^2$
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$x\equiv 3 \bmod 3^4$，$x\equiv 6 \bmod 3^4$，$x\equiv 30 \bmod 3^4$，$x\equiv 33 \bmod 3^4$，$x\equiv 40 \bmod 3^4$，$x\equiv 57 \bmod 3^4$，$x\equiv 60 \bmod 3^4$。
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？

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$p|f_1(a_2)$
但$p|(a_2 - a_1)$不可能，因为如果$p|(a_2 - a_1)$，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$p \nmid (a_2 - a_1)$，从而$p|f_1(a_2)$，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，那么就存在$n-2$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$f(x) \equiv (x - a_1)(x - a_2)f_2(x) \bmod p$.

如果还有$x \equiv a_3 \bmod p$是同余方程$f(x) \equiv 0 \bmod p$的另一个解，
则存在$n-3$次的首项系数为a_n的多项式$f_3(x)$使得对任意整数x都有$f(x) \equiv (x - a_1)(x - a_2)(x - a_3)f_3(x) \bmod p$

一般情况下就是，如果$x \equiv a_1 \bmod p$，$x \equiv a_2 \bmod p$，$x \equiv a_3 \bmod p$，...，$x \equiv a_k \bmod p$是同余方程$f(x) \equiv 0 \bmod p$的另一个解，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$f(x) \equiv (x - a_1)(x - a_2)(x - a_3)\dots(x - a_k)f_k(x) \bmod p$

从这里也可以看出，次数为n的同余方程，它的解数k至多为n，否则的话多项式$f_k(x)$的次数$n-k$就无意义. 另外我们知道任一模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$k \le \min(p, n)$.

特例: 如果$f(x)$中每个系数都是p的倍数的话, 即使$f(x)$的次数$n < p$, 它的解数也是p: 比如$11x^2 + 22x + 33 \bmod 11$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.

这是因为根据欧拉定理($(a, m) = 1$, 则$a^{\varphi(m)} \equiv 1 \bmod m$):

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

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

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

$$\dots\dots$$

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

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定理的内容.

定理: 设$f(x)=x^n+a_{n-1}x^{n-1}+\ldots+a_2x^2+a_1x+a_0$, $n\le p$,
$x^p-x=f(x)q(x)+r(x)$ ($r(x)$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 $\iff$ $r(x)$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(当然也可能是两个都成立),
这样它们的解数之和就$=p$:

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$=n$

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

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

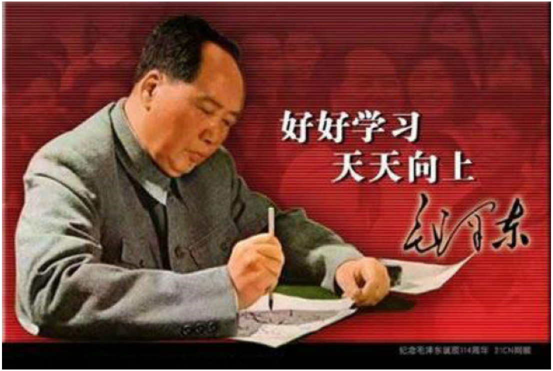
$$=(x^d-1)(x^{d(q-1)}+x^{d(q-2)}+\ldots+x^d+1)x$$
$$=(x^d-1)(x^{d(q-1)+1}+x^{d(q-2)+1}+\ldots+x^{d+1}+x)$$

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.


好好学习
天天向上
毛泽东