2.2 Euler定理和Fermat小定理及其应用

Euler 定理和 Fermat 小定理是数论中两个重要的定理，在具体讲述之前，我们首先来解决 Euler 函数的计算方法问题。

定理 2.2.1 设 n 和 m 是正整数，且 $(n,m)=1$. 如果 $a_1,\cdots,a_t$ 和 $b_1,\cdots,b_s$ 分别是模 n 和模 m 的一个完系（缩系），则所有形如

$$nb_i + ma_j (1 \le i \le s, 1 \le j \le t)$$

的数构成模 mn 的一个完系（缩系）。特别有 $\varphi(nm)=\varphi(n)\varphi(m)$。

证明：我们先证$a_1,\cdots,a_t$和$b_1,\cdots,b_s$是完系的情况，此时$t=n,s=m$。

模mn的完系共有mn个元，而所有形如

$$nb_i+ma_j(1\le i\le s,1\le j\le t)$$

的数共有$ts=nm$个，故只需证明它们模mn两两不同余即可。

再来证$a_1,\cdots,a_t$和$b_1,\cdots,b_s$是缩系的情况，此时$t=\varphi(n),s=\varphi(m)$。

由完系的情况知，所有形如$nb_i+ma_j(1\le i\le s,1\le j\le t)$的数是模$mn$不同余的，要证其为模$mn$的一缩系，需要证明两个事实：

(1) $\forall 1\le i\le s,1\le j\le t$，都有$(nb_i+ma_j,mn)=1$；

(2) 若$(c,mn)=1$，则$\exists 1\le i_0\le s,1\le j_0\le t$使得$c\equiv nb_{i_0}+ma_{j_0}(\mathrm{mod}\,mn)$。

例 1 $n=3$，取其完系$0,1,2$，$m=8$，取其完系$0,1,2,3,4,5,6,7$，由定理 2.2.1 知，

此时所有形如

$$3b_i+8a_j(1\le i\le 8,1\le j\le 3)$$

的数

$$0,8,16,3,11,19,6,14,22,9,17,25,12,20,28,15,23,31,18,26,34,21,29,37$$

为模 24 的完系。

取模 3 的缩系$1,2$，模 8 的缩系$1,3,5,7$，由定理 2.2.1 知，

此时所有形如

$$3b_i+8a_j(1\le i\le 4,1\le j\le 2)$$

的数

$$11,19,17,25,23,31,29,37$$

为模 24 的缩系，且$8=\varphi(24)=\varphi(3\times 8)=\varphi(3)\varphi(8)=2\times 4=8$。

定理 2.2.2 $\varphi(1)=1$. 当$n\geq 2$时，设$n=p_1^{e_1}\cdots p_s^{e_s}$是$n$的标准分解式，则

$$\varphi(n)=\prod_{l=1}^{s}(p_l^{e_l}-p_l^{e_l-1})=n\prod_{l=1}^{s}(1-\frac{1}{p_l})。$$

$$\varphi(n)=n\prod_{p|n}(1-\frac{1}{p})$$

证明： 由定理 2.2.1 可知，当$(n,m)=1$时，$\varphi(nm)=\varphi(n)\varphi(m)$。

利用数学归纳法可知，当$n_1,n_2,\cdots,n_s$两两互素时，$\varphi(\prod_{l=1}^{s}n_l)=\prod_{l=1}^{s}\varphi(n_l)$。因此由题设

$$知\varphi(n)=\prod_{l=1}^{s}\varphi(p_l^{e_l})，$$

问题转化为如何求$\varphi(p_l^{e_l})$。

利用欧拉函数的定义求得$\varphi(p_l^{e_l})=p_l^{e_l}-p_l^{e_l-1}$。

例 2 p 为素数，则 $\varphi(p)=p-1=p(1-\frac{1}{p})$。

$$\varphi(286)=\varphi(2\times11\times13)=\varphi(2)\varphi(11)\varphi(13)=1\times10\times12=120。$$

例 3 利用 Euler 函数的求值公式重新证明定理 2.1.5：对任意正整数 n 有

$$\sum_{d|n,d>0}\varphi(d)=n.$$

证明： 设 $n=p_1^{e_1}\cdots p_s^{e_s}$ 是 n 的标准分解式。

由定理 1.2.3(2)知， n 的每个正因子均有形式

$$d=p_1^{a_1}\cdots p_s^{a_s}，\ 0\le a_i\le e_i,1\le i\le s，$$

于是

$$\sum_{d|n,d>0}\varphi(d)=\sum_{a_1=0}^{e_1}\cdots\sum_{a_s=0}^{e_s}\varphi(\prod_{i=1}^{s}p_i^{a_i})$$

而

$$\sum_{a_i=0}^{e_i} \varphi(p_i^{a_i}) = \varphi(1) + \varphi(p_i) + \varphi(p_i^2) + \cdots + \varphi(p_i^{e_i})$$

故有

例 4 取 $n=20$，则

$$\sum_{d|20,d>0}\varphi(d)=\varphi(1)+\varphi(2)+\varphi(4)+\varphi(5)+\varphi(10)+\varphi(20)$$

???

$=20$

d	a: $(a,20)=d$	$\varphi(n/d)$
1	1，3，7，9，11，13，17，19	$\varphi(20/1)=\varphi(20)=8$
2	2，6，14，18	$\varphi(20/2)=\varphi(10)=4$
4	4，8，12，16	$\varphi(20/4)=\varphi(5)=4$
5	5，15	$\varphi(20/5)=\varphi(4)=2$
10	10	$\varphi(20/10)=\varphi(2)=1$
20	20	$\varphi(20/20)=\varphi(1)=1$

定理 2.2.3（Euler 定理） 设 n 为正整数， a 为整数，并且 $(a,n)=1$，则

$$a^{\varphi(n)} \equiv 1 (\mathrm{mod}\, n)。$$

证明：取模 n 的一个缩系 $b_1,\cdots,b_{\varphi(n)}$，考虑 $ab_1,\cdots,ab_{\varphi(n)}$。

定理 2.2.4（Fermat 小定理）设 p 为素数，则对于每个整数 a，有 $a^p \equiv a (\mathrm{mod}\, p)$。

几个应用

Euler定理和Fermat小定理是数论中两个重要的定理，它们有很多应用，例如利用这两个定理，我们可以求解同余方程，还可以得到一个概率性素性检验的方法。

例 5 设 $(a,n)=1$，证明同余方程 $ax\equiv b(\mathrm{mod}\,n)$ 的解为 $x\equiv a^{\varphi(n)-1}b(\mathrm{mod}\,n)$。

证明： 将 $x\equiv a^{\varphi(n)-1}b(\mathrm{mod}\,n)$ 代入到同余方程 $ax\equiv b(\mathrm{mod}\,n)$，由 Euler 定理知

例 6 解同余方程 $21x \equiv 7 (\mathrm{mod} 100)$。

解： 因为 $(21,100) = 1$，所以由例 5 知，该同余方程的解为

$$x \equiv 21^{\varphi(100)-1} \times 7 \equiv 21^{39} \times 7 (\mathrm{mod} 100)$$

下面来求解 $21^{39} \bmod 100$。依次计算如下，

，

例 6 中我们遇到一个求解模指数运算的问题，上面的求解方法利用了模运算的性质，但当指数很大时，这样的方法似乎不是很有效，这就需要我们寻找一个求解该问题的快速方法。这对于密码学有着很重要的应用价值。

考虑求解 x^{16}

$$xx = x^2, x^2x = x^3, \cdots, x^{15}x = x^{16}$$

$$xx = x^2, (x^2)^2 = x^4, (x^4)^2 = x^8, (x^8)^2 = x^{16}$$

将此方法推而广之就得到了所谓的快速指数算法

我们以求解 $x^a \bmod n$ 为例来说明快速指数算法，其中 x 为整数，a 为正整数，$n>1$。

将 a 表示为二进制形式，设 $(a)_2 = a_k a_{k-1} \cdots a_1 a_0$，即

$$a = a_k 2^k + a_{k-1} 2^{k-1} + \cdots + a_1 2 + a_0,$$

其中 $a_i \in \{0,1\}$，$0 \le i \le k$。

则

$$\begin{aligned} x^a \bmod n &= x^{a_k 2^k + a_{k-1} 2^{k-1} + \cdots + a_1 2 + a_0} \bmod n \\ &= (\cdots((x^{a_k})^2 x^{a_{k-1}})^2 \cdots x^{a_1})^2 x^{a_0} \bmod n \end{aligned}$$

。

该算法具体描述如下：

输入：整数 x， $a>0$， $n>1$

输出： $x^a \bmod n$

1. 将 a 表示为二进制形式，即 $(a)_2 = a_k a_{k-1} \cdots a_1 a_0$；

2. $y \leftarrow 1$； $i \leftarrow k$；

3. while(i> =0) do

(i) $y = (y \times y) \bmod n$;

(ii) if $a_i = 1$ then $y \leftarrow (y \times x) \bmod n$;

(iii) $i \leftarrow i - 1$;

4. return $y = x^a \bmod n$。

下面我们用此算法来重新计算例 6 中的模指数运算。

例 7 计算 $21^{39} \bmod 100$。

解： 易知 $39 = 2^5 + 0\cdot 2^4 + 0\cdot 2^3 + 2^2 + 2 + 1$，即

$$k = 5,\ a_5 = 1, a_4 = 0, a_3 = 0, a_2 = 1, a_1 = 1,\ a_0 = 1.$$

利用快速指数算法计算如下：

i		5	4	3	2	1	0
a_i		1	0	0	1	1	1
y	1	21	41	81	81	81	81

利用 Fermat 小定理，我们还可以来进行素性检验，即给定一个自然数 n，判断 n 是不是素数。

如果 n 是素数，整数 a 与 n 互素，即 $n \nmid a$，则由 Fermat 小定理可知

$$a^{n-1} \equiv 1 (\mathrm{mod}\, n) \qquad (*)$$

如果能找到一个与 n 互素的整数 a，使得(*)式不成立，则可以断定 n 是合数。

但是相反的结论是不成立的，即(*)式成立时，我们并不能断定 n 是素数。

事实上，存在能使(*)式对任意与其互素的 a 都成立的合数 n，例如

$$561 = 3 \times 11 \times 17, 1105 = 5 \times 13 \times 17, 1729 = 7 \times 13 \times 19$$

均满足这一要求。这类合数我们称之为 Carmichael 数。

当(*)式成立时，称 n 为以 a 为基的伪素数。

下面我们介绍一个概率性素性检验算法——Miller-Rabin 素性检验。

我们先给出强伪素数的定义。设$n-1=2^s t$，$2\nmid t$，b与n互素。若$b^t \equiv 1(\mathrm{mod}\, n)$或存在$r, 0 \le r < s$使$b^{2^r t} \equiv -1(\mathrm{mod}\, n)$，则称$n$为以$b$为基的强伪素数。

由前面 Willson 定理的证明过程知，当n为素数时，仅有± 1的平方模n为 1。由此，当n为素数，b与n互素时，若将同余式$b^{n-1} \equiv 1(\mathrm{mod}\, n)$两端逐次开方，得到

$$b^{\frac{n-1}{2}}, b^{\frac{n-1}{4}}, \cdots, b^{\frac{n-1}{2^s}} \quad \text{其中} \ 2 \nmid \frac{n-1}{2^s}$$

则这列数中第一个模n不等于 1 的数必模n等于-1。因此将满足以上条件的数称强伪素数。

当n为素数时，它一定是以任何数b（b与n互素）为基的强伪素数，以b为基的强伪素数一定是以b为基的伪素数。

下面的定理给 Miller-Rabin 素性检验的提出提供了理论依据。

定理 2.2.7 若n是奇合数，则在区间$0<b<n$中，最多有 25%的数b，能使n是以b为基的强伪素数。

下面给出 Miller-Rabin 素性检验的具体描述。

1. 将$n-1$表示为$2^s t$；
2. 在 0 与n之间随机选取整数b；
3. 计算$b^t \pmod n$；
4. 若$b^t \pmod n$为± 1，则n通过强伪素数检验，可能为素数；
5. 若$b^t \pmod n$不为± 1，则依次计算$b^{2t}, b^{4t}, \cdots, b^{2^{s-1}t} \pmod n$；
6. 若$b^{2t}, b^{4t}, \cdots, b^{2^{s-1}t} \pmod n$中有$-1$，则$n$通过强伪素数检验，可能为素数；
7. 若$b^{2t}, b^{4t}, \cdots, b^{2^{s-1}t} \pmod n$中没有$-1$，则$n$对该$b$不能通过强伪素数检验，一定为合数。

若重复步骤 2—7 共k次，即随机选取k个b（$0 < b < n$）来进行 Miller-Rabin 素性检验，且n对这k个b均能通过强伪素数检验，则由定理 2.2.7 知，可以大于$1-\frac{1}{4^k}$的概率判定n为一个素数。

2.3 孙子定理

我国隋朝之前有一部算术著作《孙子算经》(具体成书年代及著者不详)，其中提出一个“物不知数”的问题：

“今有物，不知其数，三三数之剩二，五五数之剩三，七七数之剩二，问物几何？”

明朝程大位在《算法统宗》中，以四句口诀记录上述问题的解法，即：

三人同行七十稀，

五树梅花廿一枝，

七子团圆正半月，

除百零五便得知。

上述“物有几何”的问题等价于求解下述同余方程组：

$$\begin{cases} x \equiv 2 (\mathrm{mod}\, 3) \\ x \equiv 3 (\mathrm{mod}\, 5) \\ x \equiv 2 (\mathrm{mod}\, 7) \end{cases}$$

其解法为，先计算

$$2 \times 70 + 3 \times 21 + 2 \times 15 = 233,$$

再计算

$$233 - 105 - 105 = 23,$$

所得正整数 23 即为解。

一般性的算法：南宋数学家秦九韶创立的“大衍求一术”

Gauss 在 1801 年出版的《算术研究》

“孙子定理”—— “中国剩余定理（Chinese Remainder Theorem）”

这个方法不但在古代数学史占有一定地位，而且在近代代数学上还常被采用。

下面我们将给出该定理的更一般的表述。

定理 2.3.1（孙子定理） 设正整数 $m_1, m_2, \cdots, m_k$ 两两互素，那么对于任意 k 个整数

$$a_1,\ a_2,\ \cdots,\ a_k,$$

同余方程组

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \quad\vdots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

必有解，且解数为 1。事实上，该解是

$$x \equiv M_1 M_1^{-1} a_1 + \cdots + M_k M_k^{-1} a_k \pmod{m},$$

其中 $m = \prod_{j=1}^{k} m_j$，$\forall 1 \le j \le k,\ M_j = \dfrac{m}{m_j}$，$M_j^{-1}$ 是满足 $M_j M_j^{-1} \equiv 1 \pmod{m_j}$ 的一个整数。

证明：先证定理中给出的 $y_0 = M_1 M_1^{-1} a_1 + \cdots + M_k M_k^{-1} a_k$ 是该同余方程组的解。

再证若该方程组有解 y_1 和 y_2，则必有 $y_1 \equiv y_2 (\mathrm{mod}\, m)$。

例 1 求解下面的同余方程组

$$\begin{cases} 7x \equiv 5 (\mathrm{mod}\, 18) \\ 13x \equiv 2 (\mathrm{mod}\, 15) \end{cases}。$$

解： 因为 $(18,15) \neq 1$，所以不能直接运用孙子定理。注意到

$$7x \equiv 5 (\mathrm{mod}\, 18)$$

原方程组等价于下面的方程组

$$\begin{cases} x \equiv 3 (\mathrm{mod}\, 2) \\ x \equiv 2 (\mathrm{mod}\, 9) \\ x \equiv 4 (\mathrm{mod}\, 5) \end{cases}$$

对于上述方程组可以运用孙子定理求解。此时有，

$$m_1=2，\ m_2=9，\ m_3=5，\ a_1=3，\ a_2=2，\ a_3=4，\ m=m_1m_2m_3=90，$$

从而由孙子定理可得方程组的解为

$$x\equiv M_1M_1^{-1}a_1+M_2M_2^{-1}a_2+M_3M_3^{-1}a_3(\mathrm{mod}\,m)$$

例 2 求 3^{462} 被 253 去除所得的余数。

设 r 为 3^{462} 被 253 去除所得的余数，则 r 便是此同余方程组的最小非负整数解。

例 3 解同余方程$59x \equiv 27(\mathrm{mod}\,91)$。

解：我们利用孙子定理来求解该同余方程。$91 = 7 \times 13$，所以该同余方程等价于下面的同余方程组，

$$\begin{cases} 59x \equiv 27(\mathrm{mod}\,7) \\ 59x \equiv 27(\mathrm{mod}\,13) \end{cases}$$

2.3 同余方程的一般理论

定理 2.4.1 方程$ax+by=n$有整数解的充分必要条件是$(a,b)\mid n$。

证明：利用最大公约数的显性表达式。

定理 2.4.2 若$(a,b)=1$，且x_0,y_0为方程$ax+by=n$的一个整数解，则

$$\begin{cases} x=x_0+bt \\ y=y_0-at \end{cases}，\text{其中}\ t\in Z$$

为该方程的通解。

例 1 求一次不定方程$2x+3y=7$的通解。

定理 2.4.3 同余方程 $ax+b\equiv 0(\mathrm{mod}\,m)$ 有解当且仅当 $(a,m)\mid b$。

若 $ax+b\equiv 0(\mathrm{mod}\,m)$ 有解，则在模 m 的意义下解数为 (a,m) 个；

记 x_0 为同余方程

$$\frac{a}{(a,m)}x+\frac{b}{(a,m)}\equiv 0(\mathrm{mod}\frac{m}{(a,m)})$$

的一个解，则同余方程 $ax+b\equiv 0(\mathrm{mod}\,m)$ 的通解为

$$x_0+t\frac{m}{(a,m)}(\mathrm{mod}\,m)，\ 其中\ 0\le t<(a,m),\ t\in Z。$$

$ax+b\equiv 0(\mathrm{mod}\,m)$

先考查 $(a,m)=1$ 的情形；

例 2 求解同余方程$32x \equiv 12 (\mathrm{mod}\, 8)$。

解： 由定理 2.4.3，先判断$(32,8) = 8 \nmid 12$，由此可知该同余方程无解。

例 3 求解同余方程$6x \equiv 2 (\mathrm{mod}\, 8)$。

解： 先判断$(6,8) = 2 \mid 2$，所以该同余方程有解，且模 8 有两个解。

我们先来求解同余方程$3x \equiv 1 (\mathrm{mod}\, 4)$，此方程模 4 解唯一，易知其解为

$$x \equiv 3 (\mathrm{mod}\, 4)。$$

取$x_0 = 3$，则

$$x = x_0 + \frac{8}{2}t = 3 + 4t,\ t = 0,1$$

为原方程的解，原方程的所有解为

$$x \equiv 3 (\mathrm{mod}\, 8)，\quad x \equiv 3 + 4 \equiv -1 (\mathrm{mod}\, 8)。$$

定理 2.4.4 n 元一次同余方程 $a_1x_1+\cdots+a_nx_n+b\equiv 0(\mathrm{mod}\,m)$ 有解的充分必要条件为 $(a_1,\cdots a_n,m)\,|\,b$；若方程有解，则其解数为 $m^{n-1}(a_1,\cdots a_n,m)$。

证明：我们用数学归纳法来证明。

记 $(a_1,\cdots a_n,m)=d_n$，$(a_1,\cdots a_{n-1},m)=d_{n-1}$，显然有 $(a_n,d_{n-1})=d_n$。

例 4 求解同余方程 $2x_1+3x_2\equiv 4(\mathrm{mod}\,6)$。

解：因为 $(2,3,6)=1\mid 4$，所以由定理 2.4.4，该同余方程有解，且有 $6^{2-1}(2,3,6)=6$ 个解。

此时，$d_2=(a_1,a_2,m)=(2,3,6)=1$，$d_1=(a_1,m)=(2,6)=2$。

先求 $a_2x_2+b\equiv 0(\mathrm{mod}\,d_1)$，即 $3x_2\equiv 4(\mathrm{mod}\,2)$，易知其解为 $x_2\equiv 0(\mathrm{mod}\,2)$；

在模 6 意义下其解为 $x_2\equiv 0+\frac{6}{3}\cdot t(\mathrm{mod}\,6)$，$t=0,1,2$，即 $x_2\equiv 0,2,4(\mathrm{mod}\,6)$。

将它们分别代入原同余方程得

$$\begin{aligned}&2x_1+3\times 0\equiv 4(\mathrm{mod}\,6)\\&2x_1+3\times 2\equiv 4(\mathrm{mod}\,6),\\&2x_1+3\times 4\equiv 4(\mathrm{mod}\,6)\end{aligned}$$

易得它们的解均为 $x_1\equiv 2(\mathrm{mod}\,6), x_1\equiv 5(\mathrm{mod}\,6)$。

所以原同余方程的 6 个解为

$$\begin{cases}x_1\equiv 2(\mathrm{mod}\,6)\\x_2\equiv 0(\mathrm{mod}\,6)\end{cases}\begin{cases}x_1\equiv 5(\mathrm{mod}\,6)\\x_2\equiv 0(\mathrm{mod}\,6)\end{cases}\begin{cases}x_1\equiv 2(\mathrm{mod}\,6)\\x_2\equiv 2(\mathrm{mod}\,6)\end{cases}\begin{cases}x_1\equiv 5(\mathrm{mod}\,6)\\x_2\equiv 2(\mathrm{mod}\,6)\end{cases}\begin{cases}x_1\equiv 2(\mathrm{mod}\,6)\\x_2\equiv 4(\mathrm{mod}\,6)\end{cases}\begin{cases}x_1\equiv 5(\mathrm{mod}\,6)\\x_2\equiv 4(\mathrm{mod}\,6)\end{cases}$$

前面的讨论完全解决了一次同余方程的求解问题，下面讨论一元高次同余方程。

一元同余方程的一般形式为

$f(x)\equiv 0(\mathrm{mod}\, m)$，其中 $f(x)=a_n x^n+\cdots+a_1 x+a_0$ 为一个整系数多项式。

对于高次同余方程$(n\geq 2)$而言，即便是二次同余方程，也没有一般的求解方法，而且其解数并不规则，例如：

(1) $x^2+1\equiv 0(\mathrm{mod}\, 3)$无解；

一般地，若m有标准分解式$\prod_{i=1}^{s} p_i^{e_i}$，则有

$$f(x) \equiv 0 (\mathrm{mod}\ p^l)$$

定理 2.4.5 设 p 为素数，整数 $l \geq 2$，同余方程 $f(x) \equiv 0 (\mathrm{mod}\ p^l)$ 满足 $x \equiv u (\mathrm{mod}\ p^{l-1})$ 的解是

$$x \equiv u + y_i p^{l-1} (\mathrm{mod}\ p^l),\ i = 1, \cdots, s,$$

其中 u 是同余方程 $f(x) \equiv 0 (\mathrm{mod}\ p^{l-1})$ 的解，$y \equiv y_1, \cdots, y_s (\mathrm{mod}\ p)$ 是一次同余方程

$$f'(u) y \equiv -f(u) p^{1-l} (\mathrm{mod}\ p)$$

的全部解，$f'(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \cdots + 2 a_2 x + a_1$。

证明：注意到实际上我们要求的是下述同余方程组的解

$$\begin{cases} f(x) \equiv 0 (\mathrm{mod}\ p^l) & (1) \\ x \equiv u (\mathrm{mod}\ p^{l-1}) & (2) \end{cases},$$

例 5 解同余方程 $x^3-2x+4\equiv 0(\mathrm{mod}\,5^3)$。

解： 先求解同余方程

$$x^3-2x+4\equiv 0(\mathrm{mod}\,5) \qquad (1)$$

易知(1)有两个解

$$x\equiv 3,4(\mathrm{mod}\,5)。$$

我们有 $f(x)=x^3-2x+4$，$f'(x)=3x^2-2$，$f'(3)=25$，$f'(4)=46$，所以 $5\mid f'(3)$，$5\nmid f'(4)$。

进而求解同余方程

$$x^3-2x+4\equiv 0(\mathrm{mod}\,5^2) \qquad (2)$$

此时l=2

先求同余方程(2)相应于 $x\equiv 3(\mathrm{mod}\,5)$ 的解。由定理 2.4.5，该解形如 $x\equiv 3+y_i5^{2-1}(\mathrm{mod}\,5^2)$，其中 y_i 为下述同余方程的解

$$x\equiv u+y_ip^{l-1}(\mathrm{mod}\,p^l)$$

$$f'(u)y\equiv -f(u)p^{1-l}(\mathrm{mod}\,p)$$

$$f'(3)y\equiv -f(3)5^{1-2}(\mathrm{mod}\,5)。$$

因为 $5\mid f'(3)$，$f(3)=25\equiv 0(\mathrm{mod}\,5^2)$，所以 $y\equiv 0,1,2,3,4(\mathrm{mod}\,5)$，从而

$x\equiv 3,8,13,18,23(\mathrm{mod}\,5^2)$。

再求同余方程(2)相应于$x\equiv 4(\mathrm{mod}\,5)$的解。由定理 2.4.5，该解形如$x\equiv 4+y_i 5^{2-1}(\mathrm{mod}\,5^2)$，其中$y_i$为下述同余方程的解

$x\equiv u+y_i p^{l-1}(\mathrm{mod}\,p^l)$

$$f'(4)y\equiv -f(4)5^{1-2}(\mathrm{mod}\,5)。$$

$f'(u)y\equiv -f(u)p^{1-l}(\mathrm{mod}\,p)$

因为$5\nmid f'(4)$，所以可计算得$y\equiv 3(\mathrm{mod}\,5)$，从而

$$x\equiv 19(\mathrm{mod}\,5^2)。$$

进而求解同余方程

$$x^3-2x+4\equiv 0(\mathrm{mod}\,5^3) \qquad (3)$$

此时l=3

先求同余方程(3)相应于$x\equiv 3,8,13,18,23(\mathrm{mod}\,5^2)$的解。由定理 2.4.5，相应解分别形如

$$x\equiv 3+y_i^{(1)}5^{3-1}(\mathrm{mod}\,5^3)，\quad x\equiv 8+y_i^{(2)}5^{3-1}(\mathrm{mod}\,5^3)，\quad x\equiv 13+y_i^{(3)}5^{3-1}(\mathrm{mod}\,5^3)，$$

$$x\equiv 18+y_i^{(4)}5^{3-1}(\mathrm{mod}\,5^3)，\quad x\equiv 23+y_i^{(5)}5^{3-1}(\mathrm{mod}\,5^3)$$

其中$y_i^{(1)},y_i^{(2)},y_i^{(3)},y_i^{(4)},y_i^{(5)}$分别是下述同余方程的解

$$f'(3)y^{(1)}\equiv -f(3)5^{1-3}(\mathrm{mod}\,5) \qquad (4)$$

$$f'(8)y^{(2)}\equiv -f(8)5^{1-3}(\mathrm{mod}\,5) \qquad (5)$$

$$f'(13)y^{(3)}\equiv -f(13)5^{1-3}(\mathrm{mod}\,5) \qquad (6)$$

$$f'(18)y^{(4)}\equiv -f(18)5^{1-3}(\mathrm{mod}\,5) \qquad (7)$$

$$f'(23)y^{(5)}\equiv -f(23)5^{1-3}(\mathrm{mod}\,5) \qquad (8)$$

因为 $5 \mid f'(3)=25$，且$5 \nmid f(3)5^{1-3}=1$，

$$f'(3)y^{(1)} \equiv -f(3)5^{1-3} \pmod 5$$

所以同余方程(4)无解；

因为 $5 \mid f'(8)=190$，且$5 \mid f'(8)5^{1-3}=20$，

$$f'(8)y^{(2)} \equiv -f(8)5^{1-3} \pmod 5$$

所以同余方程(5)的解为 $y^{(2)} \equiv 0,1,2,3,4 \pmod 5$，从而相应的

$$x \equiv 8+25k \pmod{5^3} (k=0,1,2,3,4)；$$

$$f'(13)y^{(3)} \equiv -f(13)5^{1-3} \pmod 5$$

因为 $5 \mid f'(13)=505$，且$5 \nmid f(13)5^{1-3}=87$，

所以同余方程(6)无解；

$$f'(18)y^{(4)} \equiv -f(18)5^{1-3} \pmod 5$$

因为 $5 \mid f'(18)=970$，且$5 \nmid f(18)5^{1-3}=232$，

所以同余方程(7)无解；

$$f'(23)y^{(5)} \equiv -f(23)5^{1-3} \pmod 5$$

因为 $5 \mid f'(23)=1585$，且$5 \mid f(23)5^{1-3}=485$，

所以同余方程(8)的解为 $y^{(5)} \equiv 0,1,2,3,4 \pmod 5$，从而相应的

$$x \equiv 23+25k \pmod{5^3} (k=0,1,2,3,4)。$$

再求同余方程(3)相应于 $x \equiv 19 (\mathrm{mod}\, 5^2)$ 的解。由定理 2.4.5，该解形如 $x \equiv 19 + y_i 5^{3-1} (\mathrm{mod}\, 5^3)$，其中 y_i 为下述同余方程的解

$$x \equiv u + y_i p^{l-1} (\mathrm{mod}\, p^l)$$

$$f'(19) y \equiv -f(19) 5^{1-3} (\mathrm{mod}\, 5) \qquad f'(u) y \equiv -f(u) p^{1-l} (\mathrm{mod}\, p)$$

因为 $5 \nmid f'(19) = 1081$，所以可计算得 $y \equiv 2 (\mathrm{mod}\, 5)$，从而

$$x \equiv 19 + 2 \cdot 5^{3-1} \equiv 69 (\mathrm{mod}\, 5^3)。$$

综上，原同余方程的解共有 11 个，分别为

$$x \equiv 69,\ 8 + 25k,\ 23 + 25k\ (\mathrm{mod}\, 5^3)，$$

其中 $k = 0, 1, 2, 3, 4$。

关于n次同余方程$f(x)\equiv 0(\mathrm{mod}\ p)$在同余意义下的解数，我们有以下定理：

定理 2.4.6 设整系数多项式$f(x)=a_nx^n+\cdots+a_1x+a_0$，$p$为素数，若$p\nmid a_n$，则同余方程$f(x)\equiv 0(\mathrm{mod}\ p)$的解数$s\le \min(n,p)$。

证明： 显然有$s\le p$，我们利用数学归纳法来证明$s\le n$。

为了表述方便，我们允许$n=0$。

定理 2.4.7 设 p 为素数，若整系数多项式同余方程

$$f(x)=a_n x^n+\cdots+a_1 x+a_0\equiv 0(\mathrm{mod}\ p)$$

的解数大于 n，则必有 $\forall 0\le i\le n$，必有 $p\mid a_i$。

证明：使用反证法。

定理 2.4.8 设 p 为素数， $f(x)=a_nx^n+\cdots+a_1x+a_0$ 为整系数多项式， $p\nmid a_n$。若有 m 个模 p 不同的数 $x_1,\cdots,x_m$，使得 $\forall 1\le i\le m$，有 $f(x_i)\equiv 0(\mathrm{mod}\ p)$，则

(1) $f(x)$ 可以唯一地表示成为 $g(x)\prod_{i=1}^{m}(x-x_i)+pr(x)$，其中 $g(x),r(x)$ 均为整系数多项式，且 $r(x)$ 的次数低于 m；

(2) 若有模 p 不同于 $x_1,\cdots,x_m$ 的数 c 使得 $f(c)\equiv 0(\mathrm{mod}\ p)$，则必有 $g(c)\equiv 0(\mathrm{mod}\ p)$。

定理 2.4.9 设 $p, f(x), x_1,\cdots,x_m$ 同定理 2.4.8，则存在唯一的一组正整数 $e_1,\cdots,e_m$ 以及唯一的整系数多项式 $g(x),r(x)$，使得 $f(x)=g(x)\prod_{i=1}^{m}(x-x_i)^{e_i}+pr(x)$，其中 $r(x)$ 的次数低于 $\sum_{i=1}^{m}e_i$，并且 $\forall 1\le i\le m$， $g(x_i)\not\equiv 0(\mathrm{mod}\ p)$.