1 一次同余方程

该一次同余式有解的充要条件是 x 的系数 9 不能被模数 15 整除，这是显然成立的。考虑

$$\frac{9}{(9,15)}x \equiv \frac{12}{(9,15)} \mod \frac{15}{(9,15)}$$

即

$$3x \equiv 4 \mod 5$$

的解。易知 $3^{-1} \mod 5 = 2$，故其解为 $x \equiv 3 \mod 5$。

而 $9x \equiv 12 \mod 15$ 的解数为 (9,15)=3 个，故其解为

$$x \equiv 3, 8, 13 \mod 15$$

2 辗转相除法相关

a=4864，b=3458，

$$\begin{aligned}
4864 &= 3458 * 1 + 1406 \\
3458 &= 1406 * 2 + 646 \\
1406 &= 646 * 2 + 114 \\
646 &= 114 * 5 + 76 \\
114 &= 76 + 38 \\
76 &= 38 * 2 + 0
\end{aligned}$$

故 4864 和 3458 的最大公因数是 38。

$$\begin{aligned}
38 &= 114 - 76 \\
&= 114 - (646 - 5 * 114) \\
&= 6 * 114 - 646 \\
&= 6 * (1406 - 646 * 2) - 646 \\
&= 6 * 1406 - 646 * 13 \\
&= 6 * 1406 - (3458 - 1406 * 2) * 13 \\
&= 32 * 1406 - 3458 * 13 \\
&= 32 * (4864 - 3458) - 3458 * 13 \\
&= 32 * 4864 - 45 * 3458
\end{aligned}$$

故 $s=32, t=45$. 将 (s,t) 减去 $(\frac{3458}{38}, -\frac{4864}{38})=(91,-128)$ 可得到 。

3 重复平方乘方法

令 $a=1, b=2$，$29=1+4+8+16=1+0\cdot 2+1\cdot 2^2+1\cdot 2^3+1\cdot 2^4$。

(1) 计算 $a_0\equiv a\cdot b^1\equiv 2 \mod 37$，再计算 $b_1\equiv b^2\equiv 4 \mod 37$

(2) 计算 $a_1\equiv a_0\cdot b_1^0\equiv 2 \mod 37$，再计算 $b_2\equiv b_1^2\equiv 16 \mod 37$

(3) 计算 $a_2\equiv a_1\cdot b_2^1\equiv 32 \mod 37$，再计算 $b_3\equiv b_2^2\equiv 34 \mod 37$

(4) 计算 $a_3\equiv a_2\cdot b_3^1\equiv 15 \mod 37$，再计算 $b_4\equiv b_3^2\equiv 9 \mod 37$

(5) 计算 $a_4\equiv a_3\cdot b_4^1\equiv 24 \mod 37$，再计算 $b_5\equiv b_4^2\equiv 7 \mod 37$

故 $2^{29}\equiv 24 \mod 37$

4 中国剩余定理

$m_1=5, m_2=6, m_3=7, m_4=11.$
令 $m=5\cdot 6\cdot 7\cdot 11=2310$

$$M_1=6*7*11=462, M_2=5*7*11=385,$$

$$M_3=5*6*11=330, M_4=5*6*7=210.$$

而 $M_1^{'}\equiv M_1^{-1}\equiv 2^{-1}\equiv 3 \mod 5$
$M_2^{'}\equiv M_2^{-1}\equiv 1^{-1}\equiv 1 \mod 6$
$M_3^{'}\equiv M_3^{-1}\equiv 1^{-1}\equiv 1 \mod 7$
$M_4^{'}\equiv M_4^{-1}\equiv 1^{-1}\equiv 1 \mod 11$
故 $x\equiv 2*462*3+1*385*1+3*330*1+0*210*1\equiv 1837 \mod 2310$

5 求解同余式方程组

由于 $49=7^2$，令 $p=7$，考虑同余式 $x^2+4x-5\equiv (x+5)(x-1)\equiv 0 \mod 7$，可验算得到其解为 $x\equiv 1,2 \mod 7$。对于 $x_1\equiv 1 \mod 7$，可以计

算对应的 $x^2+4x-5\equiv 0 \mod 49$ 的解 x_2。其中 $t_1\equiv -\frac{f(x_1)}{p}(f'(x_1)^{-1} \mod 7)\equiv -\frac{0}{7}(6^{-1} \mod 7)\equiv 0 \mod 7$

故 $x_2\equiv x_1+pt_1\equiv 1 \mod 49$

对于 $x_1'\equiv 2 \mod 7$，可以计算对应的 $x^2+4x-5\equiv 0 \mod 49$ 的解 x_2'。其中 $t_1'\equiv -\frac{f(x_1')}{p}(f'(x_1')^{-1} \mod 7)\equiv -\frac{7}{7}(1^{-1} \mod 7)\equiv 6 \mod 7$

故 $x_2'\equiv x_1+pt_1\equiv 2+7\cdot 6\equiv 44 \mod 49$

故 $x^2+4x-5\equiv 0 \mod 49$ 的解为 $x\equiv 1,44 \mod 49$。

$x^2+4x-5\equiv 0 \mod 27$ 的解。

令 $p=3$，考虑同余式 $x^2+4x-5\equiv 0 \mod 3$，即 $x^2+x-2\equiv 0 \mod 3$，直接验算，其解为 $x\equiv 1 \mod 3$。满足 $f(x_1')\equiv 0 \mod 3$ 且 $f(x_1')\equiv 0 \mod 3$ 的 x_1' 为 $x_1'\equiv 1 \mod 3$

- $f(1)\equiv 0 \mod 9$，所以 $f(x)\equiv 0 \mod 9$ 存在着模 9 意义下模 3 同余于 1 的 3 个解，这三个解为 $x_2'\equiv 1,1+3,1+6 \mod 27$。

所以 $f(x)\equiv 0 \mod 9$ 的解为 $x\equiv 1,4,7 \mod 9$。

满足 $f(x_2')\equiv 0 \mod 9$ 且 $f(x_2')\equiv 0 \mod 3$ 的 x_2' 为 $x_2'\equiv 1,4,7 \mod 9$

- $f(1)\equiv 0 \mod 27$，所以 $f(x)\equiv 0 \mod 27$ 存在着模 27 意义下模 9 同余于 1 的 3 个解，这三个解为 $x_2'\equiv 1,1+9,1+18 \mod 27$。
- $f(4)\equiv 0 \mod 27$，所以 $f(x)\equiv 0 \mod 27$ 存在着模 27 意义下模 9 同余于 4 的 3 个解，这三个解为 $x_2'\equiv 4,4+9,4+18 \mod 27$。
- $f(7)\equiv 18\not\equiv 0 \mod 27$，所以 $f(x)\equiv 0 \mod 27$ 不存在着模 27 意义下模 9 同余于 7 的解。

所以 $f(x)\equiv 0 \mod 27$ 的解为 $x\equiv 1,4,10,13,19,22 \mod 27$。

6 勒让德符号

$$
\begin{aligned}
(\frac{173}{401}) &= (-1)^{\frac{173-1}{2}\frac{401-1}{2}}(\frac{401}{173}) \\
&= (\frac{401}{173}) \\
&= (\frac{55}{173}) \\
&= (\frac{5}{173})(\frac{11}{173}) \\
&= (-1)^{\frac{5-1}{2}\frac{173-1}{2}}(\frac{173}{5})(-1)^{\frac{11-1}{2}\frac{173-1}{2}}(\frac{173}{11}) \\
&= (\frac{3}{5})(\frac{8}{11}) \\
&= (-1)^{1\cdot 2}(\frac{5}{3})(\frac{2}{11})(\frac{2}{11})(\frac{2}{11}) \\
&= (\frac{2}{3})\frac{2}{11} \\
&= (-1)^{\frac{3^2-1}{8}}(-1)^{\frac{11^2-1}{8}} \\
&= 1 \\
(\frac{174}{401}) &= (\frac{2}{401})(\frac{3}{401})(\frac{29}{401}) \\
&= (-1)^{\frac{401^2-1}{8}}(-1)^{1\cdot 200}(\frac{401}{3})(-1)^{14\cdot 200}(\frac{401}{29}) \\
&= (\frac{2}{3})(\frac{24}{29}) \\
&= -1\cdot(\frac{4}{29})(\frac{2}{29})(\frac{3}{29}) \\
&= -1\cdot(-1)^{\frac{29^2-1}{8}}(-1)^{1\cdot 14}(\frac{2}{3}) \\
&= -1
\end{aligned}
$$

7 开平方根算法

$a = 173$，对 $p = 401$，$p - 1 = 400 = 2^4 \cdot 25$，即 $t = 4, s = 25$ 是奇数。

(1) 任选一个模 401 的平方非剩余 6，即 $n = 6$ 使得 $(\frac{6}{401}) = -1$. 再令 $b := 6^{25} \equiv 371 \mod 401$

(2) 计算 $x_3 := 173^{\frac{25+1}{2}} \equiv 256 \mod 401$. $a^{-1} = 51 \mod 401$

(3) 因为 $(a^{-1}x_3^2)^{2^2} \equiv (51\cdot 256^2)^4 \equiv 1 \mod 401$。故令 $j_0 = 0, x_2 \equiv x_3 b^{j_0} \equiv x_3 \equiv 256 \mod 401$.

(4) 因为 $(a^{-1}x_2^2)^2 \equiv (51\cdot 256^2)^2 \equiv 1 \mod 401$。故令 $j_1 = 0, x_1 \equiv x_2 b^{2\times j_1} \equiv x_2 \equiv 256 \mod 401$.

(5) 因为 $(a^{-1}x_1^2) \equiv (51\cdot 256^2) \equiv 1 \mod 401$。故令 $j_2 = 0, x_0 \equiv x_1 b^{2^2\times j_2} \equiv x_1 \equiv 256 \mod 401$.

则 $x \equiv x_0 \equiv 256 \mod 401$ 满足同余式

$$x^2 \equiv 173 \mod 401$$

$(\frac{174}{401}) = -1$，故

$$x^2 \equiv 174 \mod 401$$

无解。

8 多项式的最大公因式

$$\begin{pmatrix} x^5+x^3+x+1 & 1 & 0 \\ x^3+x^2+x+1 & 0 & 1 \end{pmatrix} \to \begin{pmatrix} x^4+x^2+x+1 & 1 & x^2 \\ x^3+x^2+x+1 & 0 & 1 \end{pmatrix}$$
$$\to \begin{pmatrix} x^3+1 & 1 & x^2+x \\ x^3+x^2+x+1 & 0 & 1 \end{pmatrix} \to \begin{pmatrix} x^3+1 & 1 & x^2+x \\ x^3+x^2+x+1 & 0 & 1 \end{pmatrix}$$
$$\to \begin{pmatrix} x^3+1 & 1 & x^2+x \\ x^2+x & 1 & x^2+x+1 \end{pmatrix} \to \begin{pmatrix} x+1 & x & x^3+x^2+x+1 \\ x^2+x & 1 & x^2+x+1 \end{pmatrix}$$
$$\to \begin{pmatrix} x+1 & x & x^3+x^2+x+1 \\ 0 & 0 & x^4+x^3+1 \end{pmatrix}$$

故 $x+1$ 是 x^5+x^3+x+1 和 x^3+x^2+x+1 的最大公因式。且 $x+1 = x(x^5+x^3+x+1)+(x^3+x^2+x+1)(x^3+x^2+x+1)$，即 $s(x) = x, t(x) = (x^3+x^2+x+1)$

9 8 元域上的加法表和乘法表

表 1: 加法表

	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
1	1	0	$x+1$	x	x^2+1	x^2	x^2+x+1	x^2+x
x	x	$x+1$	0	1	x^2+x	x^2+x+1	x^2	x^2+1
$x+1$	$x+1$	x	1	0	x^2+x+1	x^2+x	x^2+1	x^2
x^2	x^2	x^2+1	x^2+x	x^2+x+1	0	1	x	$x+1$
x^2+1	x^2+1	x^2	x^2+x+1	x^2+x	1	0	$x+1$	x
x^2+x	x^2+x	x^2+x+1	x^2	x^2+1	x	$x+1$	0	1
x^2+x+1	x^2+x+1	x^2+x	x^2+1	x^2	$x+1$	x	1	0

表 2: 乘法表

	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	0	0	0	0	0	0	0
1	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
x	0	x	x^2	x^2+x	$x+1$	1	x^2+x+1	x^2+1
$x+1$	0	$x+1$	x^2+x	x^2+1	x^2+x+1	x^2	1	x
x^2	0	x^2	$x+1$	x^2+x+1	x^2+x	x	x^2+1	1
x^2+1	0	x^2+1	1	x^2	x	x^2+x+1	$x+1$	x^2+x
x^2+x	0	x^2+x	x^2+x+1	1	x^2+1	$x+1$	x	x^2
x^2+x+1	0	x^2+x+1	x^2+1	x	1	x^2+x	x^2	$x+1$