第三章 同余式
2015年04月07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

*第三章 同余式

思考题:

如何将$\mathbf{Z}$ 上的多项式$f(x)$ 求解推广到$\mathbf{Z}/m\mathbf{Z}$ 上: 同余式?

$$f(x) \equiv 0 \pmod{m} \tag{1}$$

1. 同余式(1)有解的判断?
2. 同余式(1)有解的个数?
3. 同余式(1)求解的方法和过程?

模为素数的同余式 $f(x) \equiv 0 \pmod{p} f(x) \equiv 0 \pmod{p}$

$f(x) = x^{20140512} + x^{201405} + x^{2014} + x^2 + 1 \equiv 0 \pmod{7}$

模为素数幂的同余式$f(x) \equiv 0 \pmod{p} f(x) \equiv 0 \pmod{p^\alpha}$

$f(x) = x^{20140512} + x^{201405} + x^{2014} + x^2 + 1 \equiv 0 \pmod{7^7}$

物不知数(中国剩余定理) $\begin{cases} x \equiv 2 \pmod{3}, \\ x \equiv 3 \pmod{5}, \\ x \equiv 2 \pmod{7}. \end{cases}$

本章主要讲述如下问题:

1. 同余式的基本概念
2. 一次同余式的求解
3. 中国剩余定理
4. 大模计算的简化
5. $x^p - x$ 与高次同余式
6. 高次同余式的解数
7. 模素数幂同余式及解的提升
8. 模素数同余式

3.1.1 同余式的基本概念

定义3.1.1 设m 是一个正整数. 设$f(x)a_nx^n + \cdots + a_1x + a_0$ 为多项式, 其中a_i是整数, 则

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

叫做模m **同余式**. 若$a_n \not\equiv 0 \pmod{m}$, 则$n$ 叫做$f(x)$ 的 **次数**, 记为$\deg f$. 此时, (2)式又叫做模m 的 n **次同余式**.

如果整数$x = a$ 使得(2) 成立, 即

$$f(a) \equiv 0 \pmod{m}$$

则a 叫做该同余式(2) 的**解**. 事实上, 满足$x \equiv a \pmod{m}$ 的所有整数都使得同余式(2) 成立, 即a 所在剩余类

$$C_a = \{c \mid c \in \mathbf{Z},\ c \equiv a \pmod{m}\}$$

中的每个剩余都使得同余式(2)成立, 因此, 同余式(2)的解a 通常写成

$$x \equiv a \pmod{m}.$$

在模m 的完全剩余系中, 使得同余式(2)成立的剩余个数叫做同余式(2)的**解数**.

例3.1.1 $x^5 + x + 1 \equiv 0 \pmod 7$ 是首项系数为1 的模7 同余式.

$$x \equiv 2,\ 4 \pmod 7$$

是该同余式的解. 事实上, 我们有

$$\begin{aligned}
&0^5 + 0 + 1 = 1 && \pmod 7.\\
&1^5 + 1 + 1 = 3. && \\
&2^5 + 2 + 1 = 35 = 5 \cdot 7 \equiv 0 && \pmod 7.\\
&3^5 + 3 + 1 = 247 = 35 \cdot 7 + 2 \equiv 2 && \pmod 7.\\
&(-3)^5 + (-3) + 1 = -245 = (-35) \cdot 7 \equiv 0 && \pmod 7.\\
&(-2)^5 + (-2) + 1 = -33 = (-5) \cdot 7 + 2 \equiv 2 && \pmod 7.\\
&(-1)^5 + (-1) + 1 = -1 && \pmod 7.
\end{aligned}$$

解数为2.

同余式求解的基本思路

1. 求解归约

   $f(x) \pmod m \ \Longleftarrow\ f(x) \pmod{p^\alpha} \ \Longleftarrow\ f(x) \pmod p$;

2. 解的存在性 (如定理3.1.1) ;

3. 解的个数 (如定理3.1.3, 定理3.4.4, 定理3.4.5) ;

4. 具体求解 (如定理3.2.1, 定理3.4.1) .

3.1.2 一次同余式

现在我们先考虑常数项为1 的一次同余式的求解.

一次同余式求解的基本思路

$$(a, m) = 1, ax \equiv 1 \pmod{m}$$
$$\Downarrow$$
$$(a, m) = 1, ax \equiv b \pmod{m}$$
$$\Downarrow$$
$$ax \equiv b \pmod{m}$$

定理3.1.1 设m 是正整数, a 是满足$m \nmid a$ 的整数. 则一次同余式

$$a\,x \equiv 1 \pmod{m} \tag{3}$$

有解的充分必要条件是$(a, m) = 1$. 而且, 当同余式(3)有解时, 其解是惟一的.

证 充分性. (存在性) 因为$(a, m) = 1$, 根据广义欧几里得除法(定理1.3.7, 可找到整数s, t 使得

$$s \cdot a + t \cdot m = (a, m) = 1.$$

因此, $x = s \pmod{m}$ 是同余式(3)的解.

(惟一性) 若还有解x', 即$ax' \equiv 1 \pmod{m}$, 则有

$$a(x - x') \equiv 0 \pmod{m}.$$

因为$(a, m) = 1$, 所以$x \equiv x' \pmod{m}$. 解是惟一的.

再证必要性. 若同余式(3)有解$x \equiv x_0 \pmod{m}$, 则存在整数q, 使得$a \cdot x_0 = 1 + q \cdot m$. 根据定理1.3.8, 有$(a, m) = 1$. 定理成立. 证毕

定义3.1.2 设m 是一个正整数, a 是一个整数. 如果存在整数a' 使得

$$a \cdot a' \equiv a' \cdot a \equiv 1 \pmod m$$

成立, 则a 叫做模m **可逆元**.

根据定理3.1.1, 在模m 的意义下, a' 是惟一存在的. 这时a' 叫做a 的模m **逆元**, 记作

$$a' = a^{-1} \pmod m.$$

因此, 在定理3.1.1 的条件下, 同余式(3) 即

$$a\,x \equiv 1 \pmod m$$

的解可写成:

$$x \equiv a^{-1} \pmod m.$$

其次, 我们给出模简化剩余的一个等价描述.

定理3.1.2 设m 是一个正整数. 则整数a 是模m 简化剩余的充要条件是整数a 是模m 逆元.

证 必要性. 如果整数a 是模m 简化剩余, 则$(a, m) = 1$. 根据定理3.1.1, 存在整数a' 使得

$$a \cdot a' \equiv a' \cdot a \equiv 1 \pmod{m}.$$

因此, 由定义3.1.2, a 是模m 逆元.

充分性. 如果a 是模m 逆元, 则存在整数a' 使得

$$a \cdot a' \equiv 1 \pmod{m}.$$

即同余式

$$a\,x \equiv 1 \pmod{m}$$

有解$x \equiv a' \pmod{m}$. 根据定理3.1.1, 有$(a, m) = 1$. 因此, 整数a 是模m 简化剩余. 证毕

最后, 考虑通常的一次同余式的求解.

定理3.1.3 设m 是一个正整数, a 是满足$m \nmid a$ 的整数. 则一次同余式

$$a\,x \equiv b \pmod{m} \tag{4}$$

有解的充分必要条件是$(a,m) \mid b$. 而且, 当同余式(4)有解时, 其解

$$x \equiv \frac{b}{(a,m)} \cdot \left(\left(\frac{a}{(a,m)} \right)^{-1} \left(\bmod \frac{m}{(a,m)}\right) \right) + t \cdot \frac{m}{(a,m)} \pmod{m},$$

$t = 0,\ 1, \ldots,\ (a,m)-1.$

证 必要性. 设同余式(4)有解$x \equiv x_0 \pmod{m}$, 即存在整数y_0 使得

$$a\,x_0 - m\,y_0 = b.$$

因为$(a,m) \mid a,\ \ (a,m) \mid m$, 所以根据定理1.1.3,

$$(a,m) \mid a\,x_0 - m\,y_0 = b.$$

因此, 必要性成立.

充分性. 设$(a,m)\mid b$. 则$\dfrac{b}{(a,m)}$为整数.

首先, 我们考虑同余式

$$\frac{a}{(a,m)}\,x\equiv 1 \pmod{\frac{m}{(a,m)}}. \tag{5}$$

因为$\left(\dfrac{a}{(a,m)},\dfrac{m}{(a,m)}\right)=1$, 根据定理3.1.1, 存在惟一解$x_0$, 或运用广义欧几里得除法求出该解 $x_0\equiv\left(\frac{a}{(a,m)}\right)^{-1} \pmod{\frac{m}{(a,m)}}$,
使得同余式(5)成立.

其次, 写出同余式

$$\frac{a}{(a,m)}\,x\equiv \frac{b}{(a,m)} \pmod{\frac{m}{(a,m)}} \tag{6}$$

的惟一解

$$x\equiv x_1\equiv \frac{b}{(a,m)}\cdot x_0 \pmod{\frac{m}{(a,m)}}. \tag{7}$$

而且, $x\equiv x_1\equiv \dfrac{b}{(a,m)}\cdot x_0 \pmod{m}$是同余式(4) , 即

$$a\,x\equiv b \pmod{m}$$

的一个特解.

最后, 写出同余式(4) , 即

$$a\,x \equiv b \pmod{m}$$

的全部解

$$x \equiv x_1 + t \cdot \frac{m}{(a,m)} \pmod{m}, \qquad t = 0,\ 1, \ldots,\ (a,m) - 1. \tag{8}$$

事实上, 如果同时有同余式

$$a\,x \equiv b \pmod{m} \quad \text{和} \quad a\,x_1 \equiv b \pmod{m}$$

成立, 两式相减得到

$$a\,(x - x_1) \equiv 0 \pmod{m}.$$

根据定理2.1.10 和定理2.1.8, 这等价于

$$x \equiv x_1 \pmod{\frac{m}{(a,m)}}.$$

因此, 同余式(4) 的全部解可写成(8)式. 证毕

例3.1.2 求解一次同余式

$$33x \equiv 22 \pmod{77}.$$

解 首先, 计算最大公因数$(33, 77) = 11$, 并且有$(33, 77) = 11 \mid 22$, 所以原同余式有解.

其次, 运用广义欧几里得除法, 求出同余式 $3x \equiv 1 \pmod 7$ 的一个特解$x_0' \equiv 5 \pmod 7$.

第三, 写出同余式 $3x \equiv 2 \pmod 7$ 的一个特解$x_0 \equiv 2 \cdot x_0' \equiv 2 \cdot 5 \equiv 3 \pmod 7$.

最后, 写出原同余式的全部解

$$x \equiv 3 + t \cdot \frac{77}{(33, 77)} \equiv 3 + t \cdot 7 \pmod{77}, \qquad t = 0,\ 1, \ldots,\ 10.$$

或者

$$x \equiv 3,\ 10,\ 17,\ 24,\ 31,\ 38,\ 45,\ 52,\ 59,\ 66,\ 73 \pmod{77}.$$

3.2 中国剩余定理

思考题:

物不知数(中国剩余定理) $\begin{cases} x \equiv 2 \pmod 3, \\ x \equiv 3 \pmod 5, \\ x \equiv 2 \pmod 7. \end{cases}$

如何提高模运算效率?

$$m^e \equiv c \,(\mathrm{mod}\; p \cdot q)$$

1. 简化上述计算 $\begin{cases} m^e \equiv c_1 \pmod p, \\ m^e \equiv c_2 \pmod q, \end{cases}$

2. 还原$x \equiv c$ 满足: $\begin{cases} x \equiv c_1 \pmod p, \\ x \equiv c_2 \pmod q, \end{cases}$

3.2.1 中国剩余定理：“物不知数”与韩信点兵

中国剩余定理，又称为孙子剩余定理,古有“韩信点兵”、“孙子定理”、求一术（宋沈括）“鬼谷算”（宋周密）、“隔墙算”（宋周密）、“剪管术”（宋杨辉）、“秦王暗点兵”、“物不知数”之名.

关于中国剩余定理或孙子定理, 其最早见于《孙子算经》的“物不知数”题(卷下第28题), 原文如下:

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?

即“今有物不知其数, 三三数之有二, 五五数之有三, 七七数之有二, 问物有多少?”

答案: 二十三.

解答过程为: 三三数之有二对应于一百四十, 五五数之有三对应于六十三, 七七数之有二对应于三十, 将这些数相加得到二百三十三, 再减去二百一十, 即得数之数二十三.

将“物不知数”问题用同余式组表示就是: $\begin{cases} x \equiv 2 \pmod 3, \\ x \equiv 3 \pmod 5, \\ x \equiv 2 \pmod 7. \end{cases}$

而解答过程就为:

$$\begin{aligned} 2\cdot 2\cdot 5\cdot 7 &= 2\cdot 70 = 140, & 3\cdot 1\cdot 3\cdot 7 &= 3\cdot 21 = 63, \\ 2\cdot 1\cdot 3\cdot 5 &= 2\cdot 15 = 30, & (-2)\cdot 3\cdot 5\cdot 7 &= (-2)\cdot 105 = -210, \\ 140+63+30 &= 233, & 233-210 &= 23. \end{aligned}$$

在“物不知数”问题中, 如果我们将

- 2, 3, 2 分别看作$b_1,\ b_2,\ b_3$;
- 3, 5, 7 分别看作模$m_1,\ m_2,\ m_3$;
- $5\cdot 7,\ 3\cdot 7,\ 3\cdot 5$ 分别看作$M_1,\ M_2,\ M_3$;
- 2, 1, 1 分别看作$M_1',\ M_2',\ M_3'$;
- 233 作为所构造的整数$b_1\cdot M_1'\cdot M_1 + b_2\cdot M_2'\cdot M_2 + b_3\cdot M_3'\cdot M_3$;
- 105 作为模$m = m_1\cdot m_2\cdot m_3$, -210 作为105 的q 倍.

即有对应图:

$$
\begin{array}{ccccccccc}
2 & \cdot & 2 & \cdot & 5 & \cdot & 7 & = & 140 \\
\updownarrow & & \updownarrow & & \updownarrow & & \updownarrow & & \\
b_1 & \cdot & M_1' & \cdot & m_2 & \cdot & m_3 & \cdot &
\end{array}
\qquad
\begin{array}{ccccccccc}
3 & \cdot & 1 & \cdot & 3 & \cdot & 7 & = & 63 \\
\updownarrow & & \updownarrow & & \updownarrow & & \updownarrow & & \\
b_2 & \cdot & M_2' & \cdot & m_1 & \cdot & m_3 & &
\end{array}
$$

$$
\begin{array}{ccccccccc}
2 & \cdot & 1 & \cdot & 3 & \cdot & 5 & = & 30 \\
\updownarrow & & \updownarrow & & \updownarrow & & \updownarrow & & \\
b_3 & \cdot & M_3' & \cdot & m_1 & \cdot & m_2 & &
\end{array}
\qquad
\begin{array}{ccccccccc}
(-2) & \cdot & 3 & \cdot & 5 & \cdot & 7 & = & -210 \\
\updownarrow & & \updownarrow & & \updownarrow & & \updownarrow & & \\
q & \cdot & m_1 & \cdot & m_2 & \cdot & m_3 & &
\end{array}
$$

则它们满足关系式:

$$
\begin{cases}
x = b_1 \cdot M_1' \cdot M_1 + b_2 \cdot M_2' \cdot M_2 + b_3 \cdot M_3' \cdot M_3 + q \cdot m, \\
M_i' \cdot M_i \equiv 1 \pmod{m_i}, \quad i = 1,\ 2,\ 3.
\end{cases}
$$

又淮安民间传说着一则故事——“韩信点兵”. 韩信带1500 名兵士打仗, 战死四五百人, 站3 人一排， 多出2 人; 站5 人一排, 多出4 人; 站7 人一排, 多出6 人. 韩信马上说出人数: 1049.

将上述问题用同余式组表示就是:

$$\begin{cases} x \equiv 2 \pmod 3, \\ x \equiv 4 \pmod 5, \\ x \equiv 7 \pmod 7. \end{cases}$$

其解答过程就为(人数介于1000 到1100 之间):

$$\begin{aligned} 2\cdot 2\cdot 5\cdot 7 &= 2\cdot 70 = 140, & 4\cdot 1\cdot 3\cdot 7 &= 4\cdot 21 = 84, \\ 6\cdot 1\cdot 3\cdot 5 &= 6\cdot 15 = 90, & 7\cdot 3\cdot 5\cdot 7 &= 7\cdot 105 = 735, \\ 140+84+90 &= 314, & 314+735 &= 1049. \end{aligned}$$

相应的对应图为:

$$
\begin{array}{ccccccccc}
2 & \cdot & 2 & \cdot & 5 & \cdot & 7 & = & 140 \\
\updownarrow & & \updownarrow & & \updownarrow & & \updownarrow & & \\
b_1 & \cdot & M_1' & \cdot & m_2 & \cdot & m_3 & \cdot &
\end{array}
\qquad
\begin{array}{ccccccccc}
4 & \cdot & 1 & \cdot & 3 & \cdot & 7 & = & 84 \\
\updownarrow & & \updownarrow & & \updownarrow & & \updownarrow & & \\
b_2 & \cdot & M_2' & \cdot & m_1 & \cdot & m_3 & &
\end{array}
$$

$$
\begin{array}{ccccccccc}
6 & \cdot & 1 & \cdot & 3 & \cdot & 5 & = & 90 \\
\updownarrow & & \updownarrow & & \updownarrow & & \updownarrow & & \\
b_3 & \cdot & M_3' & \cdot & m_1 & \cdot & m_2 & &
\end{array}
\qquad
\begin{array}{ccccccccc}
7 & \cdot & 3 & \cdot & 5 & \cdot & 7 & = & 735 \\
\updownarrow & & \updownarrow & & \updownarrow & & \updownarrow & & \\
q & \cdot & m_1 & \cdot & m_2 & \cdot & m_3 & &
\end{array}
$$

它们也满足关系式:

$$
\begin{cases}
\qquad\qquad x = b_1 \cdot M_1' \cdot M_1 + b_2 \cdot M_2' \cdot M_2 + b_3 \cdot M_3' \cdot M_3 + q \cdot m, \\
M_i' \cdot M_i \equiv 1 \pmod{m_i}, \quad i = 1,\ 2,\ 3.
\end{cases}
$$

注1与“物不知数”问题作比较, $m_1,\ m_2,\ m_3$, 以及

$$m = m_1 {\cdot} m_2 {\cdot} m_3,\ M_1 = \frac{m}{m_1} = m_2 {\cdot} m_3,\ M_2 = \frac{m}{m_2} = m_1 {\cdot} m_3,\ M_3 = \frac{m}{m_3} = m_1 {\cdot} m_1,$$

和

$$M_1' \equiv (M_1)^{-1} \pmod{m_1},\ \ M_2' \equiv (M_2)^{-1} \pmod{m_2},\ \ M_3' \equiv (M_3)^{-1} \pmod{m_3}$$

都是不变数, 而$b_1,\ b_2,\ b_3$ 和q 是可变数.

$$x = b_1 \cdot \underbrace{M_1' \cdot M_1}_{\text{不变}} + b_2 \cdot \underbrace{M_2' \cdot M_2}_{\text{不变}} + b_3 \cdot \underbrace{M_3' \cdot M_3}_{\text{不变}} + q \cdot \underbrace{m}_{\text{不变}}$$

注2 明朝数学家程大位有《孙子歌》：

三人同行七十希, 五树梅花廿一支, 七子团圆正半月, 除百零五使得知

从中可看出:

- 三人指模$m_1 = 3$; 五树指模$m_2 = 5$; 七子指模$m_3 = 7$;
- 七十稀指$M_1' \cdot m_2 \cdot m_3 = 70$; 二十一支指$M_2' \cdot m_1 \cdot m_3 = 21$; 正半月指$M_3' \cdot m_1 \cdot m_2 = 13$;
- 百零五指$m_1 \cdot m_2 \cdot m_3 = 105$.

最后, 将物不知数归纳为:

例3.2.1 (物不知数) 同余式组
$$\begin{cases} x \equiv b_1 \pmod 3, \\ x \equiv b_2 \pmod 5, \\ x \equiv b_3 \pmod 7. \end{cases}$$
的整数解为

$$x = b_1 \cdot 70 + b_2 \cdot 21 + b_3 \cdot 15 + q \cdot 105, \qquad q = 0, \pm 1, \pm 2, \ldots$$

现在我们考虑“物不知数”问题的推广形式, 即非常重要的中国剩余定理或孙子定理.

定理3.2.1 (中国剩余定理) 设$m_1, \ldots, m_k$ 是k 个两两互素 的正整数. 则对任意的整数$b_1, \ldots, b_k$, 同余式组

$$\begin{cases} x \equiv b_1 \pmod{m_1}, \\ \quad \cdots\cdots \\ x \equiv b_k \pmod{m_k}. \end{cases} \tag{9}$$

一定有解, 且解是惟一的. 事实上,

(i) 若令

$$m = m_1 \cdots m_k, \quad m = m_i \cdot M_i, \quad i = 1, \ldots, k,$$

则同余式组(9)的解可表示为

$$x \equiv b_1 \cdot M_1' \cdot M_1 + b_2 \cdot M_2' \cdot M_2 + \cdots + b_k \cdot M_k' \cdot M_k \pmod{m}, \tag{10}$$

其中 $M_i' \cdot M_i \equiv 1 \pmod{m_i},\ i = 1, 2, \ldots, k.$

(ii) 若令

$$N_i = m_1 \cdots m_i, \quad i = 1, \ldots, k-1,$$

则同余式组(9)的解可表示为:

$$x \equiv x_k \pmod{m_1 \cdots m_k},$$

其中$N_i' \cdot N_i \equiv 1 \pmod{m_{i+1}}$, $i = 1, 2, \ldots, k-1$, 而x_i 是同余式组

$$\begin{cases} x \equiv b_1 \pmod{m_1}, \\ \ldots\ldots \\ x \equiv b_i \pmod{m_i}. \end{cases}$$

的解, $i = 1, \ldots, k$, 并满足递归关系式

$$x_i \equiv x_{i-1} + ((b_i - x_{i-1})N_{i-1}' \pmod{m_i}) \cdot N_{i-1} \pmod{m_1 \cdots m_i} \quad (11)$$

$i = 2, \ldots, k$

3.2.2 2 个方程的中国剩余定理

2 个方程的中国剩余定理及Rabin 应用.

定理3.2.2 设m_1, m_2 是互素的两个正整数. 则对任意的整数b_1, b_2, 同余式组

$$\begin{cases} x \equiv b_1 \pmod{m_1}, \\ x \equiv b_2 \pmod{m_2}. \end{cases} \tag{12}$$

一定有解, 且解是惟一的. 事实上, 若令

$$m = m_1 \cdot m_2, \quad m = m_i \cdot M_i, \quad i = 1, 2,$$

则同余式组(12)的解可表示为

$$x \equiv b_1 \cdot M_1' \cdot M_1 + b_2 \cdot M_2' \cdot M_2 \pmod{m}, \tag{13}$$

其中

$$M_i' \cdot M_i \equiv 1 \pmod{m_i}, \ i = 1, 2.$$

证明 由(12) 式的第1 个同余式有解$x \equiv b_1 \pmod{m_1}$, 我们可以将同余式组的解表示为(y_1 待定参数)

$$x = b_1 + y_1 \cdot m_1 = b_1 + y_1 \cdot M_2.$$

将x代入同余式组(12) 式的第2 个同余式, 我们有

$$b_1 + y_1 \cdot M_2 \equiv b_2 \pmod{m_2},$$

或

$$y_1 \cdot M_2 \equiv b_2 - b_1 \pmod{m_2}. \tag{14}$$

运用广义欧几里得除法, 对整数M_2 及模m_2, 存在整数s, t 使得

$$s \cdot M_2 + t \cdot m_2 = 1$$

从而, 分别得到整数$M_2' = s$, $M_1' = t$, 使得(利用$M_2 = m_1$, $m_2 = M_1$)

$$M_2' \cdot M_2 \equiv 1 \pmod{m_2}, \qquad M_1' \cdot M_1 = t \cdot m_2 \equiv 1 \pmod{m_1},$$

将同余式(14) 的两端同乘M_2', 我们有

$$y_1 \equiv (b_2 - b_1)M_2' \pmod{m_2}.$$

或

$$y_1 = (b_2 - b_1)M_2' + q \cdot m_2.$$

故同余式组(13)的解为

$$\begin{aligned} x &= b_1 + ((b_2 - b_1)M_2' + q \cdot m_2)M_2 \\ &= b_1(1 - M_2'M_2) + b_2 \cdot M_2' \cdot M_2 + q \cdot m_2 \cdot M_2 \\ &= b_1 \cdot M_1' \cdot M_1 + b_2 \cdot M_2' \cdot M_2 + q \cdot m_1 \cdot m_2 \\ &= b_1 \cdot M_1' \cdot M_1 + b_2 \cdot M_2' \cdot M_2 \pmod{m} \end{aligned}$$

证毕

为更好应用2 个方程的中国剩余定理(定理3.2.2), 并基于定理3.2.2的证明过程, 我们给出定理3.2.2的如下表述:

定理3.2.3 设m_1, m_2 是互素的两个正整数. 则对任意的整数b_1, b_2, 同余式组(12)即

$$\begin{cases} x \equiv b_1 \pmod{m_1}, \\ x \equiv b_2 \pmod{m_2}. \end{cases}$$

有整数解

$$x \equiv b_1 \cdot s \cdot m_2 + b_2 \cdot t \cdot m_1 + q \cdot m_1 \cdot m_2, \tag{15}$$

其中s, t 满足

$$s \cdot m_2 + t \cdot m_1 = 1.$$

例3.2.2 设p, q 是不同的素数. 求解同余式组

$$\begin{cases} x \equiv b_1 \pmod{p}, \\ x \equiv b_2 \pmod{q}. \end{cases}$$

解 根据定理3.2.3, 计算整数s, t 使得

$$s \cdot q + t \cdot p = 1.$$

进而得到同余式组的解为

$$x \equiv b_1 \cdot s \cdot q + b_2 \cdot t \cdot p \pmod{p \cdot q}.$$

3.2.3 中国剩余定理之构造证明

本节用构造的方法给出中国剩余定理的证明.

证 首先, 证明解的惟一性.

设x, x' 都是满足同余式(9)式的解, 则

$$x \equiv b_i \equiv x' \pmod{m_i}, \quad i = 1, \ldots, k.$$

因为$m_1, \ldots, m_k$ 是两两互素的正整数, 根据定理2.1.2, 我们得到

$$x \equiv x' \pmod{m}.$$

再证明解的存在性.

(i) 直接构造同余式组的解:

根据假设条件, 对任意给定的i, $1 \le i \le k$, 我们有

$$(m_i, m_j) = 1,\ 1 \le j \le k,\ j \ne i,$$

又根据定理1.3.12, 有 $(m_i, M_i) = 1.$

再根据定理3.1.11, 或直接运用广义欧几里得除法, 可分别求出整数M_i', $i = 1, 2, \ldots, k$, 使得 $M_i' \cdot M_i \equiv 1 \pmod{m_i}$, $i = 1, 2, \ldots, k.$

这样, 我们就构造出一个形为(10)式的整数, 即

$$x = b_1 \cdot M_1' \cdot M_1 + b_2 \cdot M_2' \cdot M_2 + \cdots + b_k \cdot M_k' \cdot M_k \pmod{m}.$$

因为$m = m_i \cdot M_i$ 及$m_i \mid M_j$, $1 \le j \le k$, $j \ne i$, 所以这个整数x 满足同余式

$$x \equiv 0 + \cdots + 0 + b_i \cdot M_i' \cdot M_i + 0 + \cdots + 0 \equiv b_i \pmod{m_i}, \quad i = 1, \ldots, k.$$

也就是说, 形为(10) 式的整数是同余式(9) 式的解.

例3.2.3 求解同余式组 $\begin{cases} x \equiv b_1 \pmod{5}, \\ x \equiv b_2 \pmod{6}, \\ x \equiv b_3 \pmod{7}, \\ x \equiv b_4 \pmod{11}. \end{cases}$

解 令$m = 5 \cdot 6 \cdot 7 \cdot 11 = 2310$,

$$M_1 = 6 \cdot 7 \cdot 11 = 462, \quad M_2 = 5 \cdot 7 \cdot 11 = 385,$$
$$M_3 = 5 \cdot 6 \cdot 11 = 330, \quad M_4 = 5 \cdot 6 \cdot 7 = 210.$$

分别求解同余式

$$M_i' \cdot M_i \equiv 1 \pmod{m_i}, \quad i = 1, 2, 3, 4.$$

得到 $M_1' = 3, \quad M_2' = 1, \quad M_3' = 1, \quad M_4' = 1.$

故同余式组的解为

$$\begin{aligned} x &\equiv b_1 \cdot 3 \cdot 462 + b_2 \cdot 1 \cdot 385 + b_3 \cdot 1 \cdot 330 + b_4 \cdot 1 \cdot 210 \\ &\equiv b_1 \cdot 1386 + b_2 \cdot 385 + b_3 \cdot 330 + b_4 \cdot 210 \quad \pmod{2310}. \end{aligned}$$

3.2.4 中国剩余定理之递归证明

本节用递归的方法给出中国剩余定理的证明.

证明二: 归纳构造同余式组的解.

$k=1$时, 同余式 $x \equiv b_1 \pmod{m_1}$, 的解为 $x \equiv x_1 \equiv b_1 \pmod{m_1}$;

$k=2$时, 原同余式组等价于

$$\begin{cases} x \equiv b_1 \pmod{N_1}, \\ x \equiv b_2 \pmod{m_2}. \end{cases} \tag{16}$$

由(16) 式的第一个同余式有解$x \equiv x_1 \equiv b_1 \pmod{N_1}$, 我们可以将同余式组的解表示为($y_1$ 待定参数) $x = x_1 + y_1 \cdot N_1$.

将x代入同余式组(16) 式的第二个同余式, 我们有

$x_1 + y_1 \cdot N_1 \equiv b_2 \pmod{m_2}$, 或

$$y_1 \cdot N_1 \equiv b_2 - x_1 \pmod{m_2}. \tag{17}$$

运用广义欧几里得除法, 对N_1 及模m_2, 可求出N_1' 使得

$N_1' \cdot N_1 \equiv 1 \pmod{m_2}$,

将同余式(17) 的两端同乘N_1', 我们有 $y_1 \equiv (b_2 - x_1) \cdot N_1' \pmod{m_2}$.

故同余式组(16)的解为

$$x = x_2 = x_1 + ((b_2 - x_1)N_1' \pmod{m_2}) \cdot N_1 \pmod{m_1 m_2}.$$

假设$i-1,\ (i\geq 2)$ 时, 命题成立. 即 $\begin{cases} x\equiv b_1 & (\mathrm{mod}\ m_1), \\ \ldots\ldots \\ x\equiv b_{i-1} & (\mathrm{mod}\ m_{i-1}). \end{cases}$

有解 $x\equiv x_{i-1}\ (\mathrm{mod}\ m_1\cdots m_{i-1})$.

对于i, 同余式组 $\begin{cases} x\equiv b_1 & (\mathrm{mod}\ m_1), \\ \ldots\ldots \\ x\equiv b_i & (\mathrm{mod}\ m_i). \end{cases}$ 等价于同余式组

$$\begin{cases} x\equiv x_{i-1} & (\mathrm{mod}\ N_{i-1}), \\ x\equiv b_i & (\mathrm{mod}\ m_i). \end{cases} \tag{18}$$

类似于$k=2$, 由(18) 式的第一个同余式有解$x\equiv x_{i-1}\ (\mathrm{mod}\ N_{i-1})$, 可以将同余式组的解表示为($y_{i-1}$ 待定参数) $x=x_{i-1}+y_{i-1}\cdot N_{i-1}$.
将x代入(18) 式的第二个同余式, 有 $x_{i-1}+y_{i-1}\cdot N_{i-1}\equiv b_i\ (\mathrm{mod}\ m_i)$, 或

$$y_{i-1}\cdot N_{i-1}\equiv b_i-x_{i-1}\ (\mathrm{mod}\ m_i). \tag{19}$$

对整数N_{i-1} 及模m_i, 求出整数N'_{i-1} 使得 $N'_{i-1}\cdot N_{i-1}\equiv 1\ (\mathrm{mod}\ m_i)$,
将同余式(19) 的两端同乘N'_{i-1}, 我们有 $y_{i-1}\equiv (b_i-x_{i-1})N'_{i-1}\ (\mathrm{mod}\ m_i)$.
故同余式组(17) 的解为

$$x=x_i=x_{i-1}+((b_i-x_{i-1})N'_{i-1}\ (\mathrm{mod}\ m_i))\cdot N_{i-1}\ (\mathrm{mod}\ m_1\cdots m_i).$$

根据数学归纳法原理, 命题是成立的. 证毕

例3.2.4 韩信点兵之二: 有兵一队, 若列成五行纵队, 则末行一人; 成六行纵队, 则末行五人; 成七行纵队, 则末行四人; 成十一行纵队, 则末行十人. 求兵数.

解 韩信点兵问题可转化为同余式组

$$\begin{cases} x \equiv 1 \pmod 5, \\ x \equiv 5 \pmod 6, \\ x \equiv 4 \pmod 7, \\ x \equiv 10 \pmod{11}. \end{cases}$$

解一 对$b_1 = 1,\ b_2 = 5,\ b_3 = 4,\ b_4 = 10$ 应用例**??**,得到

$$\begin{aligned} x &\equiv 1 \cdot 1386 + 5 \cdot 385 + 4 \cdot 330 + 10 \cdot 210 \\ &\equiv 6731 \\ &\equiv 2111 \pmod{2310}. \end{aligned}$$

解二: 归纳构造同余式组的解.

令$N_1 = 5$. 同余式组的第一个同余式有解$x \equiv x_1 \equiv 1 \pmod 5$, 我们将同余式组的解表示为($y$ 待定参数)

$$x = 1 + y \cdot 5.$$

将x代入同余式组的第二个同余式, 我们有

$$1 + y \cdot 5 \equiv 5 \pmod 6, \quad \text{或} \quad y \cdot 5 \equiv 4 \pmod 6.$$

运用广义欧几里得除法, 对整数$N_1 = 5$ 及模$m_2 = 6$, 可求出整数$N_1' \equiv N_1^{-1} \equiv 5 \pmod 6$, 我们有

$$y \equiv 4 \cdot 5 \equiv 2 \pmod 6.$$

故同余式组的解为

$$x = x_2 = 1 + 2 \cdot 5 \equiv 11 \pmod{30}.$$

我们将它表示为(y 待定参数) $x = x_2 = 11 + y \cdot 30.$
将x代入同余式组的第三个同余式, 我们有

$$11 + y \cdot 30 \equiv 4 \pmod 7, \quad \text{或} \quad y \cdot 30 \equiv 4 - 11 \equiv 0 \pmod 7.$$

运用广义欧几里得除法, 对整数$N_2 = 30$ 及模$m_3 = 7$, 可求出整数$N_2' \equiv N_2^{-1} \equiv 4 \pmod 7$, 我们有 $y \equiv 0 \cdot 4 \pmod 7$.
故同余式组的解为 $x = x_3 = 11 + 0 \cdot 30 \equiv 11 \pmod{210}$.
我们将它表示为(y 待定参数) $x = x_3 = 11 + y \cdot 210$. 将$x$代入同余式组的第四个同余式, 我们有

$$11 + y \cdot 210 \equiv 10 \pmod{11}, \quad \text{或} \quad y \cdot 210 \equiv 10 - 11 \equiv 10 \pmod{11}.$$

运用广义欧几里得除法, 对整数$N_3 = 210$ 及模$m_4 = 11$, 可求出整数$N_3' \equiv N_3^{-1} \equiv 1 \pmod{11}$, 我们有 $y \equiv 10 \cdot 1 \pmod{11}$.
故同余式组的解为

$$x = x_3 = 11 + 10 \cdot 210 \equiv 2111 \pmod{2310}.$$

3.2.5 中国剩余定理之应用-算法优化

应用中国剩余定理, 我们可以将一些复杂的运算转化为较简单的运算.

例3.2.5 计算$2^{1000000} \pmod{77}$.

解一 利用定理2.4.1(Euler 定理)及模重复平方计算法直接计算.

因为$77 = 7 \cdot 11, \varphi(77) = \varphi(7)\varphi(11) = 60$, 所以, $\quad 2^{60} \equiv 1 \pmod{77}$.

又$1000000 = 16666 \cdot 60 + 40$, 所以

$$2^{1000000} = (2^{60})^{16666} \cdot 2^{40} \equiv 2^{40} \pmod{77}.$$

设$m = 77,\ b = 2$. 令$a = 1$. 将40 写成二进制, $\quad 40 = 2^3 + 2^5$.

运用模重复平方法, 我们依次计算如下:

1). $n_0 = 0$. 计算 $a_0 = a \equiv 1, \quad b_1 \equiv b^2 \equiv 4 \pmod{77}$.

2). $n_1 = 0$. 计算 $a_1 = a_0 \equiv 1, \quad b_2 \equiv b_1^2 \equiv 16 \pmod{77}$.

3). $n_2 = 0$. 计算 $a_2 = a_1 \equiv 1, \quad b_3 \equiv b_2^2 \equiv 25 \pmod{77}$.

4). $n_3 = 1$. 计算 $a_3 = a_2 \cdot b_3 \equiv 25, \quad b_4 \equiv b_3^2 \equiv 9 \pmod{77}$.

5). $n_4 = 0$. 计算 $a_4 = a_3 \equiv 25, \quad b_5 \equiv b_4^2 \equiv 4 \pmod{77}$.

6). $n_5 = 1$. 计算 $a_5 = a_4 \cdot b_5 \equiv 23 \pmod{77}$.

最后, 计算出 $2^{1000000} \equiv 23 \pmod{77}$.

解二 令$x = 2^{1000000}$. 因为$77 = 7 \cdot 11$, 所以计算$x \pmod{77}$ 等价于求解同余式组

$$\begin{cases} x \equiv b_1 \pmod 7 \\ x \equiv b_2 \pmod{11}. \end{cases}$$

因为Euler 定理给出

$$2^{\varphi(7)} \equiv 2^6 \equiv 1 \pmod 7$$

以及$1000000 = 166666 \cdot 6 + 4$, 所以

$$b_1 \equiv 2^{1000000} \equiv (2^6)^{166666} \cdot 2^4 \equiv 2 \pmod 7.$$

类似地, 因为$2^{\varphi(11)} \equiv 2^{10} \equiv 1 \pmod{11}$, $\quad 1000000 = 100000 \cdot 10$, 所以$b_2 \equiv 2^{1000000} \equiv (2^{10})^{100000} \equiv 1 \pmod{11}$.

令$m_1 = 7,\ m_2 = 11,\ m = m_1 \cdot m_2 = 77,\ M_1 = m_2 = 11, \quad M_2 = m_1 = 7,$

分别求解同余式 $\quad 11M_1' \equiv 1 \pmod 7, \quad 7M_2' \equiv 1 \pmod{11}.$

得到 $\quad M_1' = 2, \quad M_2' = 8.$

故 $\quad x \equiv 2 \cdot 11 \cdot 2 + 8 \cdot 7 \cdot 1 \equiv 100 \equiv 23 \pmod{77}.$

因此, $2^{1000000} \equiv 23 \pmod{77}$.

例3.2.6 计算 $312^{13} \pmod{667}$.

解 运用中国剩余定理及模重复平方法.

令$x = 312^{13}$. 因为$667 = 23 \cdot 29$, 所以计算$x \pmod{667}$ 等价于求解同余式组

$$\begin{cases} x \equiv b_1 \pmod{23} \\ x \equiv b_2 \pmod{29}. \end{cases}$$

由模重复平方法, 我们有: $b_1 \equiv 312^{13} \equiv 8 \pmod{23}$.

类似地, 我们有 $b_2 \equiv 312^{13} \equiv 4 \pmod{29}$.

令$m_1 = 23,\ m_2 = 29,\ m = m_1 \cdot m_2 = 667$,

$$M_1 = m_2 = 29, \quad M_2 = m_1 = 23,$$

分别求解同余式 $29M_1' \equiv 1 \pmod{23}$, $\quad 23M_2' \equiv 1 \pmod{29}$.

得到 $M_1' = 4, \quad M_2' = -5$.

事实上, 由广义欧几里得除法, 我们有

$$\begin{array}{rcrcr} 29 & = & 1 \cdot 23 & + & 6 \\ 23 & = & 4 \cdot 6 & - & 1 \end{array} \quad \text{以及} \quad \begin{array}{rclcl} 1 & = & -23 & + & 4 \cdot 6 \\ & = & (-1) \cdot 23 & + & 4 \cdot (29 - 1 \cdot 23) \\ & = & 4 \cdot 29 & + & (-5) \cdot 23. \end{array}$$

故 $x \equiv 4 \cdot 29 \cdot 8 + (-5) \cdot 23 \cdot 4 \equiv 468 \pmod{667}$.

因此, $312^{13} \equiv 468 \pmod{667}$.

例3.2.7 用RSA公钥密码系统对"math"加解密.

假设公钥密码系统使用$N = 26$ 字符集$\mathcal{N}$. 明文信息空间为$k = 2$-字符组组成的集合$\mathcal{M} = \mathcal{N}^k$. 密文信息空间为$l = 3$-字符组组成的集合$\mathcal{C} = \mathcal{N}^l$.

运用素数对$p = 23, q = 29$.

a) 计算$n = pq = 667$和$\varphi = (p-1)(q-1) = 616$;

b) 随机选取整数$e = 13, 1 < e < \phi$, 使得$\gcd(e, \varphi) = 1$;

c) 运用广义欧几里得算法具体计算唯一的整数$d = 237, 1 < d < \varphi$, 使得

$$e \cdot d \equiv 1 \pmod{\varphi}$$

$$\begin{aligned} 616 &= 47 \cdot 13 + 5 \\ 13 &= 2 \cdot 5 + 3 \\ 5 &= 1 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1. \end{aligned} \qquad \begin{aligned} 1 &= 3 - 1 \cdot (5 - 1 \cdot 3) \\ &= (-1) \cdot 5 + 2 \cdot (13 - 2 \cdot 5) \\ &= 2 \cdot 13 + (-5) \cdot (616 - 47 \cdot 13) \\ &= (-5) \cdot 616 + 237 \cdot 13. \end{aligned}$$

d) 说明公钥是$K_e = (n, e) = (667, 13)$, 私钥是$K_d = d = 237$.

e) 以两字符为一组给出明文的数字信息, 加密后的数字信息及密文字符;

"ma"$= 12 \cdot 26 + 0 = 312 \quad \longmapsto \quad 468 = 18 \cdot 26 + 0 =$ "sa",

"th"$= 19 \cdot 26 + 7 = 501 \quad \longmapsto \quad 163 = 6 \cdot 26 + 7 =$ "gh".

加密过程. 为加密信息"ma", 将明文"ma"转换为数字信息: "ma"$= 12 \cdot 26 + 0 = 312$,; 为加密信息"th", 将明文"th"转换为数字信息: "th" $= 19 \cdot 26 + 7 = 501$,

发送者B 计算

$$c = m^e \pmod{n} = 312^{13} \pmod{667} = 468,$$

将数字信息转换为: $468 = 18 \cdot 26 + 0 =$ "sa", 即密文字符为"sa" .

计算

$$c = m^e \pmod{n} = 501^{13} \pmod{667} = 163,$$

将数字信息转换为: $163 = 6 \cdot 26 + 7 =$ "gh", 即密文字符为"gh" .

f) 说明如何恢复密文为明文.

"sa"$= 18 \cdot 26 + 0 = 468 \quad \longmapsto \quad 312 = 12 \cdot 26 + 0 =$ "ma",

"gh"$= 6 \cdot 26 + 7 = 163 \quad \longmapsto \quad 501 = 19 \cdot 26 + 7 =$ "th".

解密过程. 为解密c, A 将密文"sa "转换为数字信息: "sa"$= 18 \cdot 26 + 0 = 468$, 将密文"gh "转换为数字信息: "gh"$= 6 \cdot 26 + 7 = 163$,
再用私钥$d = 237$计算

$$c^d \pmod{n} = 468^{237} \pmod{667} = 312.$$

并将数字信息转换为文字. $312 = 12 \cdot 26 + 0 =$ "ma" , 即明文为"ma".
再计算

$$c^d \pmod{n} = 163^{237} \pmod{667} = 501.$$

并将数字信息转换为文字. $501 = 19 \cdot 26 + 7 =$ "th" , 即明文为"th".

现在我们推广定理2.2.4.

定理3.2.4 在定理3.2.1的条件下，若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

$$x \equiv b_1 \cdot M_1' \cdot M_1 + b_2 \cdot M_2' \cdot M_2 + \cdots + b_k \cdot M_k' \cdot M_k \pmod{m}$$

遍历模$m = m_1 \cdot m_2 \cdots m_k$ 的完全剩余系.

证 令

$$x_0 = b_1 \cdot M_1' \cdot M_1 + b_2 \cdot M_2' \cdot M_2 + \cdots + b_k \cdot M_k' \cdot M_k \pmod{m},$$

则当b_1, b_2, $\ldots$, b_k 分别遍历模m_1, m_2, $\ldots$, m_k的完全剩余系时, x_0 遍历$m_1 \cdot m_2 \cdots m_k$ 个数. 如果能够证明它们模m 两两不同余, 则定理成立. 事实上, 若

$$b_1 \cdot M_1' \cdot M_1 + b_2 \cdot M_2' \cdot M_2 + \cdots + b_k \cdot M_k' \cdot M_k \equiv b_1' \cdot M_1' \cdot M_1 + b_2' \cdot M_2' \cdot M_2 + \cdots + b_k' \cdot M_k' \cdot M_k \pmod{m}$$

则根据定理2.1.11, $b_i \cdot M_i' \cdot M_i \equiv b_i' \cdot M_i' \cdot M_i \pmod{m_i}$, $\quad i = 1, \ldots, k$.
因为$M_i' \cdot M_i \equiv 1 \pmod{m_i}$, $\quad i = 1, \ldots, k$, 所以, $b_i \equiv b_i' \pmod{m_i}$, $i = 1, \ldots, k$.
但b_i, b_i'是同一个完全剩余系中的两个数,故 $b_i = b_i'$, $i = 1, \ldots, k$. 定理成立. 证毕

命题3.2.1 设$m_1, \ldots, m_k$ 是k 个互素的正整数. 令$m = m_1 \cdots m_k$ 则对任意的整数$0 \le b < m$, 存在唯一的一组整数$b_i,\ 0 \le b_i < m_i,\ \ 1 \le i \le k$, 使得

$$b_1 \cdot M_1' \cdot M_1 + \cdots + b_k \cdot M_k' \cdot M_k \equiv b \pmod m$$

其中$m_i \cdot M_i = m,\ M_i' \cdot M_i \equiv 1 \pmod{m_i},\ 1 \le i \le k$. 进一步, $(b, m) = 1$ 的充要条件是$(b_i, m_i) = 1,\ 1 \le i \le k$.

证 令b_i 为b 模m_i 的最小非负余数, $1 \le i \le k$, 则该组数是唯一的, 并使得

$$b_1 \cdot M_1' \cdot M_1 + \cdots + b_k \cdot M_k' \cdot M_k \equiv b \pmod m.$$

事实上, 对于$1 \le i \le k$, 有

$$\begin{aligned} & b_1 \cdot M_1' \cdot M_1 + \cdots + b_{i-1} \cdot M_{i-1}' \cdot M_{i-1} + b_i \cdot M_i' \cdot M_i + b_{i+1} \cdot M_{i+1}' \cdot M_{i+1} \\ & + \cdots + b_k \cdot M_k' \cdot M_k \\ & \equiv b_i \cdot M_i' \cdot M_i \equiv b_i \equiv b \pmod{m_i}. \end{aligned}$$

又$m_1, \ldots, m_k$ 是k 个互素的正整数, 所以

$$b_1 \cdot M_1' \cdot M_1 + \cdots + b_k \cdot M_k' \cdot M_k \equiv b \pmod m.$$

进一步, 当$(b,m)=1$时, 有$(b,m_i)=1,\ 1\le i\le k$, 又因为

$$b_i\equiv b \pmod{m_i},\ 1\le i\le k,$$

所以

$$(b_i,m_i)=(b,m_i)=1,\ 1\le i\le k.$$

反过来, 当$(b_i,m_i)=1,\ 1\le i\le k$时, 有

$$(b,m_i)=(b_i,m_i)=1,\ 1\le i\le k.$$

从而$(b,m_1\cdots m_k)=1$, 即$(b,m)=1$.

推论 设$m_1,\ \dots,\ m_k$是k个互素的正整数. 令

$$m=m_1\cdots m_k,\ m_i\cdot M_i=m,\ M_i'\cdot M_i\equiv 1 \pmod{m_i},\ \ 1\le i\le k.$$

则对任意的整数$b_1,\ \dots,\ b_k$,

$$(b_1\cdot M_1'\cdot M_1+\cdots+b_k\cdot M_k'\cdot M_k,m)=1$$

的充要条件是

$$(b_i,m_i)=1,\ 1\le i\le k.$$