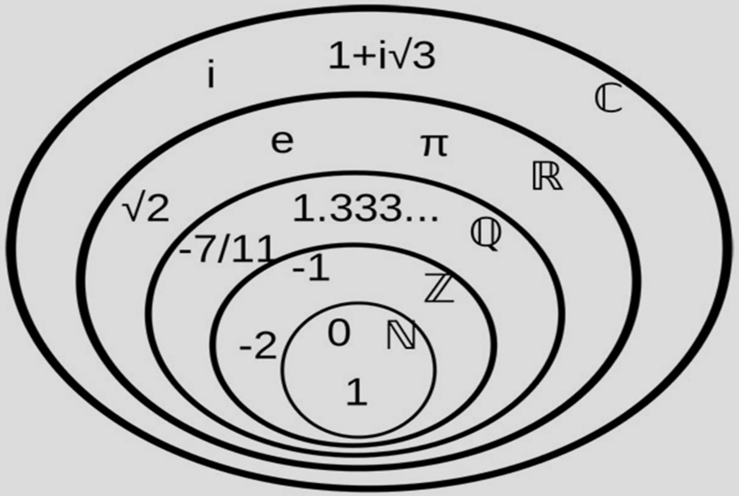

第1.4节 求解同余方程

Section 1.4: Solving Congruences

知识要点

1. 线性同余方程
2. 线性同余方程组
3. 大整数计算应用
4. 费马小定理
5. 伪素数
6. 原根、离散对数

1.4.1 同余

- 回顾同余的定义:
- 【定义】：如果a和b为整数，而m为正整数，则当m整除$a-b$时，称a模m同余b，或者称a和b是模m同余的，记作$a \equiv b \pmod{m}$．我们称$a \equiv b \pmod{m}$为**同余式**，而m是它的模．如果a和b不是模m同余的，则记作 $a \not\equiv b \pmod{m}$.

1.4.1 同余的性质

- 同余关系是等价关系, 即同余关系具有如下特征和性质(证明略):
- ① 自反性:$a \equiv a(mod\ m)$
- ② 传递性:$a \equiv b(mod\ m) \wedge b \equiv c(mod\ m) \Rightarrow a \equiv c(mod\ m)$.
- ③ 对称性:$a \equiv b(mod\ m) \Rightarrow b \equiv a(mod\ m)$.

  可以扩展缩写为$a_1 \equiv a_2 \equiv \cdots \equiv a_k\ (mod\ m)$.
- 性质1:若$a \equiv b(mod\ m)$, $c \equiv d(mod\ m)$, 则

  $a \pm c \equiv b \pm d(mod\ m)$; $ac \equiv bd(mod\ m)$;

  $a^k \equiv b^k(mod\ m)$, 其中k是非负整数;
- 性质2:设$d \geq 1$, $d|m$, 则$a \equiv b(mod\ m) \Rightarrow a \equiv b(mod\ d)$.
- 性质3:设$d \geq 1$, 则$a \equiv b(mod\ m) \Leftrightarrow da \equiv db(mod\ dm)$.
- 性质4:设c,m互素, 则$a \equiv b(mod\ m) \Leftrightarrow ca \equiv cb(mod\ m)$.

【基础知识: $\wedge$理解为“并且” $\Rightarrow$理解为“那么”】

1.4.1 线性同余方程

- 【定义】：具有$ax \equiv b(mod\ m)$形式称为**线性同余方程**, 其中m为正整数, a和b为整数, x为变量.
- 求解线性同余方程就是找到所有满足这一同余方程的整数x. 接下来介绍一种方法就是利用a模m的逆$\bar{a}$, 如果$\bar{a}$存在的话.

- 【定义】：整数$\bar{a}$, 使得$\bar{a}a \equiv 1(mod\ m)$, 那么$\bar{a}$就称为**$a$模$m$的逆**.
- 也可以写作a^{-1}或者$a^{-1}(mod\ m)$
- 例如:5是3模7的逆, 因为$5*3 = 15 \equiv 1(mod\ 7)$

1.4.1 线性同余方程

- 下面的定理就能够找到a模m的逆，当a, m互素的情况下[互素的定义:a和m互素，当$\gcd(a, m) \ = \ 1$]
- 【定理1】：如果a和m为互素的整数，且$m>1$，则a模m的逆存在. 并且这个逆是唯一存在(即存在唯一小于m的正整数$\bar{a}$是a模m的逆，并且a模m的其他每个逆均和$\bar{a}$模m同余.)
- 证:因为$\gcd(a, m) = 1$，根据贝祖定理所以存在整数s和t,使得$sa \ + \ tm \ = \ 1.$
  - 这蕴含了$sa \ + \ tm \ \equiv \ 1 \ (mod \ m)$.
  - 因为$tm \ \equiv \ 0 \ (mod \ m)$，所以有$sa \ \equiv \ 1 \ (mod \ m)$.
  - 因此，s是a模m的逆.
  - 唯一性的证明留着练习.

1.4.1 求a模m的逆

- 例: 求3模7的逆.
- 解: 因为gcd(3,7) = 1, 那么3模7的逆一定存在.
  - 利用欧几里得算法可得$7 = 2 \cdot 3 + 1$.
  - 因此$-2 \cdot 3 + 1 \cdot 7 = 1$, 所以$-2$和1是贝祖系数.
  - 所以, -2是3模7的一个逆.
  - 此外, 模7同余-2的每一个整数也是3模7的逆, 例如5, -9, 12等.

1.4.1 求a模m的逆

- 例: 求101模4620的逆.
- 解: 首先用欧几里得算法证明gcd(101,4620) = 1.

$$
\begin{aligned}
4620 &= 45\cdot101+75\\
101 &= 1\cdot75+26\\
75 &= 2\cdot26+23\\
26 &= 1\cdot23+3\\
23 &= 7\cdot3+2\\
3 &= 1\cdot2+1\\
2 &= 2\cdot1
\end{aligned}
$$

由于最后一个非零余数为1,
所以gcd(101,4620) = 1

反向操作:

$$
\begin{aligned}
1 &= 3-1\cdot2\\
1 &= 3-1\cdot(23-7\cdot3) = -1\cdot23+8\cdot3\\
1 &= -1\cdot23+8\cdot(26-1\cdot23) = 8\cdot26-9\cdot23\\
1 &= 8\cdot26-9\cdot(75-2\cdot26) = 26\cdot26-9\cdot75\\
1 &= 26\cdot(101-1\cdot75)-9\cdot75\\
&= 26\cdot101-35\cdot75\\
1 &= 26\cdot101-35\cdot(42620-45\cdot101)\\
&= -35\cdot4620+1601\cdot101
\end{aligned}
$$

贝祖系数 : − 35和1601

所以1601 是101模4620的逆

1.4.1 求解线性同余方程

- 求解线性同余方程, 可以通过在方程两边同时乘以逆来求解.
- 例: 求解线性同余方程3x≡ 4(mod 7).
- 解:
  - 前面例中已经知道-2是3模7的逆. 在方程的两边同时乘以-2得到$-2 \cdot 3x \equiv -2 \cdot 4(mod\ 7)$.
  - 因为$-6 \equiv 1\ (mod\ 7)$,$-8 \equiv 6\ (mod\ 7)$, 所以如果x是解, 则有$x \equiv -8 \equiv 6\ (mod\ 7)$
  - 我们需要判断是否每个满足$x \equiv 6\ (mod\ 7)$ 的都是解.
  - 假定$x \equiv 6\ (mod\ 7)$, 可得 $3x \equiv 3 \cdot 6 = 18 \equiv 4(mod\ 7)$.
  - 这表明所有这样的x都满足同余方程. 从而得出结论$3x \equiv 4(mod\ 7)$的解是使得$x \equiv 6\ (mod\ 7)$的整数x, 即 6,13,20 … 以及−1,−8,−15,…

1.4.1 求解线性同余方程

- 总结:如果需要求$ax \equiv b(\bmod m)$，先求解a模m的逆$\bar{a}$是否存在. 如果存在那么$x \equiv \bar{a}b(\bmod m)$.
  - $ax \equiv b(\bmod m)$, 那么$\bar{a}ax \equiv \bar{a}b(\bmod m)$, 即$m|\bar{a}ax - \bar{a}b$
  - $\bar{a}a \equiv 1(\bmod m)$, 那么$\bar{a}ax \equiv x(\bmod m)$, 即$m|\bar{a}ax - x$
  - 那么, $m|x - \bar{a}b$[推论:如果 a, b, c 是整数, 其中$a \neq 0$, 使得 $a|b$ 和$a|c$, 那么当m和n是整数时, 有$a \mid mb + nc$], 即$x \equiv \bar{a}b(\bmod m)$.

1.4.1 求解线性同余方程

- 例: 求解线性同余方程$101x \equiv 2(mod\ 4620)$.
- 解:
  - 在前面的例子中已经求解到101模4620的逆为1601.
  - 因此在同余方程两边同时乘以1601得：$1601 * 101 * x \equiv 2 * 1601(mod\ 4620)$.
  - 其中$1601 * 101 \equiv 1(mod\ 4620)$, 化解可得$x \equiv 2 * 1601(mod\ 4620) \equiv 3202(mod\ 4620)$.
  - 所以，该同余方程的解是使得$x \equiv 3202(mod\ 4620)$的所有整数x，比如3202,7822,...以及-1418,-6038,...

【备注:前面的例子中已经求解101模4620的逆为1601】

1.4.1 求解线性同余方程

- 如果线性同余方程中$ax \equiv b(mod\ m)$，a,m不互素的情况下该如何求解呢?
- 【定理】:方程$ax≡b(\mathrm{mod}\ m)$有解的充要条件是$\gcd(a,m)|b$.
- 证明:
  - 充分性. 记$d = \gcd(a,m)$, $a = da_1$, $m = dm_1$, $b = db_1$, 其中a_1与m_1互素．由定理(定理:整数a和b互素的充分必要条件是存在整数x和y使得$xa + yb = 1$)可知，存在x_1和y_1使得$a_1x_1+m_1y_1 = 1$．假设令$x=b_1x_1$，$y=b_1y_1$，得$a_1x+m_1y=b_1$．等式两边同乘d，得$ax + my = b$. 所以，$ax \equiv b(mod\ m)$.
  - 然后必要性. 设x是方程的解, 则存在y使得$ax + my = c$．由性质(如果a，b，c是整数，其中$a \neq 0$，使得$a|b$ 和$a|c$，那么当m和n是整数时，有$a|mb+nc$), 有$d \mid b$.

1.4.1 求解线性同余方程

- 例: 求解线性同余方程$35x \equiv 10\ (mod\ 15)$
- 解:
  - 求解 gcd(35,15)=5, 因此不能直接使用模逆来求解. 但 gcd(35,15)=5|10, 因此方程有解.
  - 注意到35, 10, 15存在公约数5. 因此可以化解为$7x \equiv 2\ (mod\ 3)$
  - 求解可得$x \equiv 2(mod\ 3)$的所有整数x. 因此$x = 3t + 2$, t为整数.
  - 这其中小于15的正整数分别有2($t = 0$时), 5($t = 1$时), 8($t = 2$时),11($t = 3$时),14($t = 4$时)
  - 因此, 该同余方程的解是满足$x \equiv 2, 5, 8, 11, 14(mod\ 15)$的所有整数$x$, 比如2,5,8,11,14,…及-1,-4, -7,…

【基础知识:设$d \geq 1$, 则$a \equiv b(mod\ m) \Leftrightarrow da \equiv db(mod\ dm)$】

1.4.1 求解线性同余方程

- 例: 求解线性同余方程$6x \equiv 3 (\mathrm{mod}\ 9)$.
- 解:
  - gcd(6,9)=3|3, 方程有解.
  - 注意到6, 3, 9存在公约数3. 因此可以化解为$2x \equiv 1\ (mod\ 3)$
  - 求解可得$x \equiv 2 (mod\ 3)$的所有整数x. 因此$x = 3t + 2$, t为整数.
  - 这其中小于9的正整数分别有2($t = 0$时), 5($t = 1$时), 8($t = 2$时)
  - 因此，该同余方程的解是满足$x \equiv 2, 5, 8\ (mod\ 9)$的所有整数$x$，比如2,5,8,…及-1,-4, -7,…

1.4.2 中国剩余定理

- 在古代中国, 数学家孙子问道:
  - 有物不知其数, 三分之余二, 五分之余三, 七分之余二, 此物几何?
- 翻译过来就是下列**同余方程组**的解是什么:
  - $x \equiv 2\ (mod\ 3)$,
  - $x \equiv 3\ (mod\ 5)$,
  - $x \equiv 2\ (mod\ 7)$?
- 中国剩余定理、反向替换等方法都可以来求解该问题.

1.4.2 中国剩余定理

- 例:求解孙子的提问, $x\equiv 2\ (mod\ 3)$, $x\equiv 3\ (mod\ 5)$, $x\equiv 2\ (mod\ 7)$
- 【解法编成歌诀：“三人同行七十稀，五树梅花廿一支，七子团圆正半月，除百零五便得知”】
  - 三人同行七十稀: 把除以3所得的余数用70乘
  - 五树梅花日一枝:把除以5所得的余数用21乘
  - 七子团圆正半月:把除以7所得的余数用15乘
  - 除百零五便得知:把上述三个积加起来，减去105的倍数(其中105=3*5*7)，所得的差即为所求
  - 因此列式为2×70＋3×21＋2×15=233，233-105×2=23

1.4.2 中国剩余定理

- **中国剩余定理**(Chinese remainder theorem, CRT), 又称为孙子定理(实际上是秦九韶发现的).
- 【中国剩余定理】：令m_1，m_2,…，m_n为大于1的两两互素的正整数, 而a_1, a_2,…, a_n是任意整数, 则同余方程
  - $x \equiv a_1 \pmod{m_1}$
  - $x \equiv a_2 \pmod{m_2}$
  - …
  - $x \equiv a_n \pmod{m_n}$

  存在着唯一的解$\boldsymbol{x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_n M_n y_n}$，这其中 $m = m_1 m_2 \ldots m_n$, $M_i = \frac{\boldsymbol{m}}{\boldsymbol{m_i}}$，由于$gcd(M_i, m_i) = 1$，必存在整数$y_i$使得 $M_i y_i \equiv 1 \pmod{m_i}$，$i = 1,2,\cdots,n$.

1.4.2 中国剩余定理

- 例:求解孙子的提问, $x \equiv 2\ (mod\ 3)$, $x \equiv 3\ (mod\ 5)$, $x \equiv 2\ (mod\ 7)$
- 解:
  - 令m=3· 5 ·7=105, $M_1=m/3=35$, $M_2=m/5=21$, $M_3=m/7=15$.
  - 可以算出, $y_1=2$是$M_1=35$模3的逆, 因为$35 \cdot 2 \equiv 2 \cdot 2 \equiv 1\ (mod\ 3)$; $y_2=1$是$M_2=21$模5的逆, 因为$21 \equiv 1\ (mod\ 5)$; $y_3=1$是$M_3=15$模7的逆, 因为$15 \equiv 1\ (mod\ 7)$
  - 因此, $x = a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3 = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233 \equiv 23\ (mod\ 105)$
  - 从而, 我们得出23是方程组的一个最小的正整数解.

1.4.2 反向替换方法

- 在中国剩余定理中要求m_1，m_2,…，m_n是两两互素的正整数．但实际中可能并不一定满足．因此，我们还可以用一种称为**反向替换**的方法来更容易的求解同余方程组.

- 例:利用反向替换的方法求解孙子的提问, $x \equiv 2 \ (mod\ 3)$, $x \equiv 3 \ (mod\ 5)$, $x \equiv 2 \ (mod\ 7)$
- 解:
  - 第一个同余方程可以重写为$x = 3t + 2$, 其中t是整数.
  - 将它放入第二个同余方程可得$3t + 2 \equiv 3 \ (mod\ 5)$.
  - 解它可得$t \equiv 2 \ (mod\ 5)$.
  - 第二个同余方程可以重写为$t = 5u + 2$, 其中u是整数.

1.4.2 反向替换方法

- 解(续):
  - 将它放入刚才的等式$x = 3t + 2$，可得$x = 3(5u + 2) + 2 = 15u + 8$.
  - 再将它放入第三个同余方程可得$15u + 8 \equiv 2 (mod\ 7)$.
  - 解它可得$u \equiv 1\ (mod\ 7)$.
  - 第三个同余方程可以重写为$u = 7v + 1$, 其中v是整数.
  - 将它放入刚才的等式$x = 15u + 8$，可得$x = 15(7v + 1) + 8 = 105v + 23$.
  - 将这个转换为一个同余式，就能找到同余方程组的解，$x \equiv 23\ (mod\ 105)$.

1.4.2 反向替换方法

- 例: 韩信点兵问题. 一队士兵已知少于105人, 排成每行3人余2人, 每行5人余1人, 每行7人余6人. 问这队士兵至少有多少人?
- 解:易知等价求满足如下三个同余方程组的最小正整数:

$$x \equiv 2 \pmod 3$$
$$x \equiv 1 \pmod 5$$
$$x \equiv 6 \pmod 7$$

  - 由第一个同余式，存在整数k使得$x=3k+2$，代入第二个同余式得$3k+2\equiv 1 \pmod 5$，即$3k\equiv 4 \pmod 5$．它有唯一解$k\equiv 3 \pmod 5$．故存在整数r使得$k=5r+3$,
  - 从而$x=3(5r+3)+2=15r+11$，代入第三个同余式得$15r+11 \equiv 6 \pmod 7$，即$15r\equiv 2 \pmod 7$. 它有唯一解$r\equiv 2 \pmod 7$. 故存在整数s使得$r=7s+2$,
  - 从而$x=15(7s+2)+11=105s+41$，即要求的解为41．将这个转换为一个同余式, 就能找到同余方程组的解, $x \equiv 41 \pmod{105}$. 因此士兵为41人.

1.4.3 大整数的计算机算术

- 假定$m_1, m_2, \ldots, m_n$是两两互素的模数, 并令m为其乘积. 根据中国剩余定理可以证明满足$0 \le a < m$的整数a可以唯一地表示为一个n元祖, 其元素由a除以m_i的余数组成, $i = 1,2, \ldots, n$. 即a可以唯一地表示为

$$(a \ \textbf{mod} \ m_1, a \ \textbf{mod} \ m_2, \ldots, a \ \textbf{mod} \ m_n)$$

- 证明略.

1.4.3 大整数的计算机算术

- 例: 当整数用二元祖表示, 其中第一个元素是该整数除以3的余数, 第二个元素是该整数除以4的余数. 那么分别写出小于12的非负整数的二元组表示.
- 解:根据题目要求分别求解 (a **mod** 3, a **mod** 4), $0 \le a < 12$. 因此:

0=(0,0)	1=(1,1)	2=(2,2)	3=(0,3)
4=(1,0)	5=(2,1)	6=(0,2)	7=(1,3)
8=(2,0)	9=(0,1)	10=(1,2)	11=(2,3)

1.4.3 大整数的计算机算术

- 假定在某台计算机上做小于100的整数算术运算比做大整数算术快. 如果我们将整数表示为除以100以内的两两互素的模的余数，那么可以将计算限制在100以内的整数中.
- 例:在计算机中将整数表示为除以99, 98, 97, 95(它们是两两互素)的4元组. 那么计算123684和413456之和.
- 解:
  - 整数123684=(33, 8, 9, 89), 413456=(32, 92, 42, 16)
  - 为了计算和的结果，我们不是直接将这两个整数做求和运算. 我们是将四元组的对应分量相加，再按相应的结果进行各自的除以对应模的余数降低四元组分量的结果. 即
  - 123684+ 413456 =(33, 8, 9, 89)+(32, 92, 42, 16)=(65 **mod** 99, 100 **mod** 98, 51 **mod** 97, 105 **mod** 95) =(65, 2, 51, 10)

1.4.3 大整数的计算机算术

- 如果需要找出(65,2,51,10)所表示的整数, 那么需要求解同余方程组

$$x \equiv 65\ (mod\ 99)$$

$$x \equiv 2\ (mod\ 98)$$

$$x \equiv 51\ (mod\ 97)$$

$$x \equiv 10\ (mod\ 95)$$

- 使用前述方法可以求解得到该方程组唯一小于$99 * 98 * 97 * 95 = 89403930$的解是537140. 计算可知$123684 + 413456 = 537140$确实是这两个整数的和.
- 总结: 只有当我们需要恢复(65,2,51,10)所表示的整数, 那么我们不得不做一次大于100的整数算术运算.