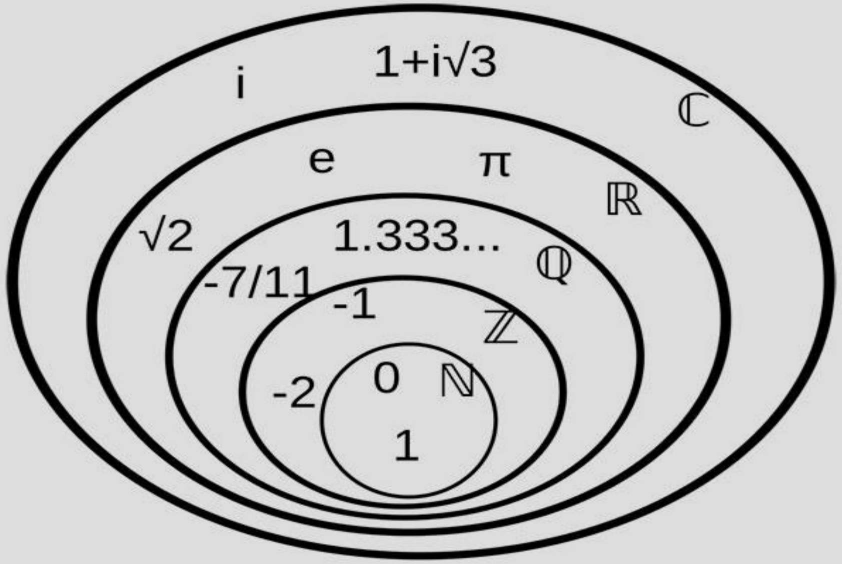

第1.4节 求解同余方程

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$a_1 \equiv a_2 \equiv \ldots \equiv a_k\ (mod\ m)$.
- 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$sa + tm \equiv 1 \pmod m$.
  - 因为$tm \equiv 0 \pmod m$，所以有$sa \equiv 1 \pmod m$.
  - 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$3x \equiv 4(mod\ 7)$. 【备注:前面例中已经知道-2是3模7的逆】
- 解:
  - 已知-2是3模7的逆. 在方程的两边同时乘以-2得到$-2 \cdot 3x \equiv -2 \cdot 4(mod\ 7)$. （备注性质1：若$a \equiv b(mod\ m)$, $c \equiv d(mod\ m)$, 则$ac \equiv bd(mod\ m)$）
  - 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, ...

华中科技大学 计算机科学与技术学院 School of Computer Science &Technology, HUST

- 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$x \equiv \bar{a}b(\bmod m)$.