

SGU 106 解题手记

解 $ax+by=c$ 这样的不定方程。首先要求得一组 $|a|x+|b|y=|c|$ 的整数解 (x',y') 。

$$\begin{aligned} |a|x'+|b|y' &= |c| \\ y' &= \frac{|c|-|a|x'}{|b|} \in \mathbb{Z} \end{aligned}$$

可以看出, x' 是同余方程 $|a|x \equiv |c| \pmod{|b|}$ 的一个根。为了解这个同余方程, 需要知道一些同余和同余方程的基本概念及定理。

同余的定义: 若 $m|a-b$, 则说“ a 与 b 关于 m 同余”, 表示为 $a \equiv b \pmod{m}$ 。反之, 若 $m \nmid a-b$, 则说“ a 与 b 关于 m 不同余”。

同余的性质: 若 $a \equiv b \pmod{m}$, 则 $m|(a-b)$ 。

剩余类: 关于 m 同余的整数的集合。

完全剩余系: 从模 m 的每一个剩余类中任意挑出一个整数, 则这 m 个整数就称为关于 m 的一个完全剩余系。

同余方程的解: 同余方程 $ax \equiv b \pmod{m}$ 的一个解 $x=k$ 并不是一个数, 而是关于 m 的一个剩余类。即, 凡关于 m 同余的数, 算作一个解, 只有关于 m 不同余的数, 才是不同的解。

定理 1 若 $(a,m)=1$, 则同余方程 $ax \equiv b \pmod{m}$ 有且只有一解。

证明: 设 $1,2,3,\dots,m$ 是关于 m 的一个完全剩余系, $(a,m)=1$, 所以 $a,2a,\dots,ma$ 也是关于 m 的一个完全剩余系 (可用反证法证明), 其中有一数, 设为 ak , 满足 $ak \equiv b \pmod{m}$, 则 $x=k$ 就是 $ax \equiv b \pmod{m}$ 的唯一解。

定理 2 设 $(a,m)=d>1$, 同余方程 $ax \equiv b \pmod{m}$ 有解的充分必要条件是 $d|b$ 。

证明: 必要性 (“ \Rightarrow ”): 设同余方程 $ax \equiv b \pmod{m}$ 有解 x_0 , 则 $m|ax_0-b$, $d|m$, $d|a$, 故 $d|b$ 。

充分性 (“ \Leftarrow ”): 如果 $d|b$, 则由 $(\frac{a}{d}, \frac{m}{d})=1$, 可知同余方程 $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$ 有一解, 此解即 $ax \equiv b \pmod{m}$ 的一个解。

定理 3 设 $(a,m)=d$, $d|b$, 则同余方程 $ax \equiv b \pmod{m}$ 有 d 个解, 且

$$x_i = x_0 + i \frac{m}{d} \quad (1 \leq i \leq d-1)。$$

证明: 当 $d=1$ 时, 根据定理 1, 定理 3 成立。

当 $d>1$ 时, 则由 $(\frac{a}{d}, \frac{m}{d})=1$, 可知同余方程 $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$ 有一解 $x=x_0$, x_0 ,

$x_i = x_0 + i \frac{m}{d} \quad (1 \leq i \leq d-1)$ 均为 $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$ 的根, 而 $x_i \quad (0 \leq i \leq d-1)$ 关于 m 不同余。故 $x=x_i \quad (0 \leq i \leq d-1)$ 是 $ax \equiv b \pmod{m}$ 的 d 个解。

同余方程的解法: 同余方程 $ax \equiv b \pmod{m}$ 的解法。

若 $(a,m)=1$, 首先用 `extended_euclid` 算法得到满足 $ax'+my'=1$ 的 (x',y') , 则 $ax' \equiv 1 \pmod{m}$, 即 $x=bx'$ 是同余方程 $ax \equiv b \pmod{m}$ 的解。

若 $(a,m)=d>1$, 且 $d|b$, 则用 `extended_euclid` 算法得到满足 $ax'+my'=d$ 的 (x',y') , $x=x_0 = \frac{b}{d}x'$ 是同余方程 $ax \equiv b \pmod{m}$ 的一个解, 然后由定理 3 可得其它解。

extended_euclid 算法:

```

Algorithm extended_euclid(a,b)
  if b=0 then
    extended_euclid←a
    x'←1
    y'←0
  else
    extended_euclid←extended_euclid(b,a mod b)
    t←y'
    y'←x'−⌊ $\frac{a}{b}$ ⌋·y'
    x'←t

```

在得到的 $|a|x+|b|y=|c|$ 一组整数解 (x',y') 后, 根据 $|a|x+|b|y=|c|$ 与 $ax+by=c$ 的系数关系, 得到 $ax+by=c$ 的一组解 (x_0,y_0) 。再设 $d=(|a|,|b|)$, 则 $ax+by=c$ 的解可以表示为 $(x_0 + \frac{i \cdot b}{d}, y_0 - \frac{i \cdot a}{d})$ 。满足 $x_1 \leq x \leq x_2, y_1 \leq y \leq y_2$ 的解的个数, 由不等式组:

$$\begin{cases} x_1 - x_0 \leq \frac{i \cdot b}{d} \leq x_2 - x_0 \\ y_0 - y_2 \leq \frac{i \cdot a}{d} \leq y_0 - y_1 \end{cases} \text{ 决定。}$$

Submit 1: WA on 2. FT.....把要解的方程看错了。虽然看错, 但程序中又写错一次, 正好错回来。少判断了 $a=0$ 和 $b=0$ 的情况, 不过这跟 WA 无关。

最后求整解个数的地方有问题: 假设 $\frac{b}{d} > 0$, 那么, $x_1 - x_0 \leq \frac{i \cdot b}{d} \leq x_2 - x_0$ 等价于

$$\left\lfloor \frac{x_1 - x_0}{\frac{b}{d}} \right\rfloor \leq i \leq \left\lfloor \frac{x_2 - x_0}{\frac{b}{d}} \right\rfloor, \text{ 而我在程序里写成了 } \left\lfloor \frac{x_1 - x_0}{\frac{b}{d}} \right\rfloor \leq i \leq \left\lceil \frac{x_2 - x_0}{\frac{b}{d}} \right\rceil。$$

Submit 2: WA on 3. 有一个错误没发现, 程序里写的全是 $\left\lfloor \frac{x_1 - x_0}{\frac{b}{d}} \right\rfloor \leq i \leq \left\lceil \frac{x_2 - x_0}{\frac{b}{d}} \right\rceil \dots\dots$

Submit 3: AC.