一次同余方程

1. 同余方程的解

通常记为x ≡ a（mod m）

2. 求解方法1（暴力遍历）

若同余方程有解，则遍历模 的一个完全剩余系，就能找到其所有的解，通常选择遍历模的最小非负完全剩余系，这种方法适合模数较小的情形.

3. 例题1

【例3.1.1】 求解同余方程$5x \equiv 3 (\mathrm{mod}\ 7)$.

解: 将模7的一个完全剩余系中的剩余代入方程中，这里选择最小非负完全剩余系{0, 1, 2, 3, 4, 5, 6}. 因 $5\times2\equiv10\equiv3(\mathrm{mod}\ 7)$, 故 $x \equiv 2(\mathrm{mod}\ 7)$ 为同余方程的所有解.

【例3.1.2】 求解同余方程$4x \equiv 2(\mathrm{mod}\ 6)$.

解: 将模6的一个完全剩余系中的剩余代入方程中，这里选择最小非负完全剩余系{0, 1, 2, 3, 4, 5}. 因

$$4\times2\equiv8\equiv2(\mathrm{mod}\ 6),\ 4\times5\equiv20\equiv2(\mathrm{mod}\ 6),$$

故$x \equiv 2(\mathrm{mod}\ 6), x \equiv 5(\mathrm{mod}\ 6)$为同余方程的所有解.

4. 求解方法2 （欧几里得算法）

设a为整数，m为正整数，若（a，m）= 1，则同余方程 ax ≡ 1（mod m）有唯一解

因为利用欧几里得算法，可以得到 sa + tm = 1这类等式，等式两端mod m，可以得到as ≡ 1（mod m）则x ≡ s（mod m）即为解

5. 例题2（欧几里得）

【例3.1.5】 解同余方程$15x \equiv 1 \pmod{28}$.

解: 由于(15,28)=1,方程有唯一解.

由欧几里德算法

28=15+13　15=13+2　13=6×2+1

1=13-6×2　这步重点

=13-6×(15-13)=13×7-6×15

=(28-15)×7-6×15=28×7-13×15　得到结果

即: 1=28×7-13×15

等式两端模28得15×(-13)≡1(mod 28).

故 x≡-13≡15(mod 28)　此15非上面15，是负变正

6. 求解方法3 （欧几里得变式）

设a为整数，m为正整数，若（a，m）= 1，则同余方程 ax ≡ b（mod m）有唯一解

且解为 x ≡ bx0 (mod m)，x0为 ax ≡ 1（mod m）的解

7. 例题3（欧几里得变式）

【例3.1.6】 求解同余方程$15x \equiv 3 \pmod{28}$.

解: 由【例3.1.5】知, $15x \equiv 1 \pmod{28}$的解为

$$x \equiv 15 \pmod{28}.$$

故同余方程$15x \equiv 3 \pmod{28}$的解为

$$x \equiv 3 \times 15 \equiv 45 \equiv 17 \pmod{28}.$$

8. **通用求解方法**

一次同余方程-求解步骤

故解同余方程$ax \equiv b \pmod m$的步骤如下:

(1) 判断方程是否有解. 即判断(a,m)是否整除b.

(2) 计算$\frac{\mathrm{a}}{(\mathrm{a,m})}x \equiv 1\left(\mathrm{mod}\,\frac{\mathrm{m}}{(\mathrm{a,m})}\right)$的解. 运用欧几里德算法求解. 设求得的解为$x \equiv x_0\left(\mathrm{mod}\,\frac{m}{(a,m)}\right)$.

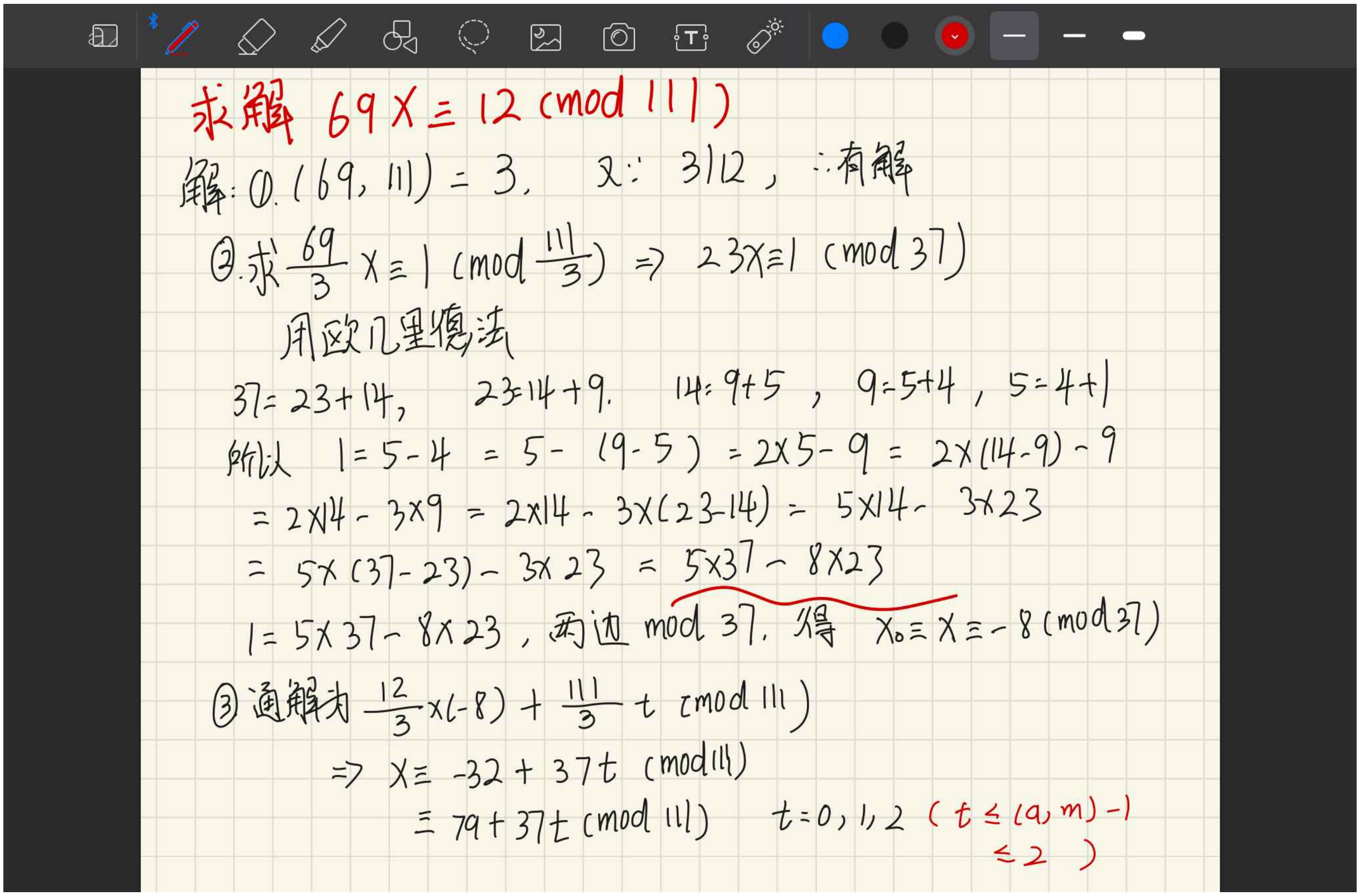
(3) 写出方程$\frac{a}{(a,m)}x \equiv \frac{b}{(a,m)}\left(\mathrm{mod}\,\frac{m}{(a,m)}\right)$的解为

$$x \equiv \frac{b}{(a,m)}x_0\left(\mathrm{mod}\,\frac{m}{(a,m)}\right).$$

(4) 写出方程$ax \equiv b \pmod m$的全部解为

$$x \equiv \frac{b}{(a,m)}x_0 + \frac{m}{(a,m)}t\,(mod\, m),\ t = 0,1,2,\dots,(a,m)-1.$$

9. 例题4（通用解法）



求解 $69x \equiv 12 \pmod{111}$

解：① $(69,111)=3$，又∵ $3 \mid 12$，∴有解

② 求 $\frac{69}{3}x \equiv 1 \pmod{\frac{111}{3}} \Rightarrow 23x \equiv 1 \pmod{37}$

用欧几里德法

$37=23+14$，$23=14+9$，$14=9+5$，$9=5+4$，$5=4+1$

所以 $1=5-4=5-(9-5)=2\times5-9=2\times(14-9)-9$

$=2\times14-3\times9=2\times14-3\times(23-14)=5\times14-3\times23$

$=5\times(37-23)-3\times23=5\times37-8\times23$

$1=5\times37-8\times23$，两边 mod 37，得 $x_0 \equiv x \equiv -8 \pmod{37}$

③ 通解为 $\frac{12}{3}\times(-8)+\frac{111}{3}t \pmod{111}$

$\Rightarrow x \equiv -32+37t \pmod{111}$

$\equiv 79+37t \pmod{111}$　$t=0,1,2$　$(t \le (a,m)-1 \le 2)$

10. 逆元

1. 为什么要求逆元

我们先来看一道简单的数学问题： 12/4mod7=? 很显然，答案等于3.但要是a和b很大很大，我们又应该怎么求得答案

这个时候，我们就要把除法转化为乘法

> 逆元在这时就能发挥作用了。根据我们刚才的定义，设 $4x\equiv1(\text{mod}7)$，易得 x=2。此时x就是一个逆元。我们在原方程两边乘以x，问题就转化成了：12∗2mod7=?。我们发现，答案依然等于3. 因此，乘法逆元可以在模运算下把除法转化为乘法，wonderful！

2. 怎么求逆元

使用扩展欧几里得。求解逆元本身就是解线性同余方程，使用exgcd算出即可

> 用上面例子来说，4x ≡ 1 (mod 7)，用gcd => 7 = 4 + 3；4 = 3 + 1

> 所以1 = 4 - 3；1 = 4 -（7 - 4）= 2 * 4 - 7；两边同时除7，可得x ≡ 2 (mod 7)，即2是逆元