线性同余方程

主讲人：邓哲也

线性同余方程

设 x 是未知整数，形如

$$ax \equiv b \pmod{m}$$

的同余式成为一元线性同余方程。

线性同余方程

【定理】

设 a，b 和 m 是整数，$m > 0$，$(a, m) = d$.

若 $d \nmid b$，则 $ax \equiv b \pmod{m}$ 无解。

若 $d \mid b$，则 $ax \equiv b \pmod{m}$ 恰好有 d 个模 m 不同余的解。

线性同余方程

【例】找出 $9x \equiv 12 \pmod{15}$ 的解。

因为 $(9,15)=3$ 且 $3 \mid 12$，所以恰好有 3 个不同余的解。

求解 $9x - 15y = 12$，由扩展欧几里得算法得：

$$15 = 9 * 1 + 6$$

$$9 = 6 * 1 + 3$$

$$6 = 3 * 2$$

所以 $3 = 9 - 6 * 1 = 9 - (15 - 9 * 1) * 1 = 9 * 2 - 15$

求出一组特解 $x=2*4=8$，$y=1*4=4$

线性同余方程

【例】找出 $9x \equiv 12 \pmod{15}$ 的解。

求出特解 $x=8, y=4$，即 $9 * 8 - 4 * 15 = 12$

所以 $x_1 \equiv 8$，$x_2 \equiv 8+5 \equiv 13$，$x_3 \equiv 8+5+5 \equiv 3 \pmod{15}$.

模的逆

【模的逆】 $ax \equiv 1 \pmod{m}$ 的解称为 a 模 m 的逆。

如 $7x \equiv 1 \pmod{31}$ 的解满足 $x \equiv 9 \pmod{31}$

用模的逆来解线性同余方程

【模的逆】 $ax \equiv 1 \pmod{m}$ 的解称为 a 模 m 的逆。设 a 模 m 的一个逆为 k，即 $ak \equiv 1 \pmod{m}$

对于 $ax \equiv b \pmod{m}$，两边同乘以 k，得到 $akx \equiv bk \pmod{m}$

也即 $x \equiv bk \pmod{m}$

模的逆

【定理】设 p 是素数，正整数 a 是其自身模 p 的逆，当且仅当 $a \equiv 1 \pmod p$ 或 $a \equiv -1 \pmod p$

证明：若$a \equiv 1 \pmod p$ 或 $a \equiv -1 \pmod p$，则$a^2 \equiv 1 \pmod p$，所以a其自身模p的逆。反过来，若a是其自身模p的逆，则$a^2=a \cdot a \equiv 1 \pmod p$。因此，$p \mid (a^2-1)$。又因为$a^2-1=(a-1)(a+1)$，所以$p \mid (a-1)$或$p \mid (a+1)$。因此，或者$a \equiv 1 \pmod p$，或者$a \equiv -1 \pmod p$

费马小定理

【定理】假如 p 是质数，且 (a, p)=1，那么

$$a^{p-1} \equiv 1 \pmod{p}$$

因此可以得到，$a * a^{p-2} \equiv 1 \pmod{p}$

所以 a^{p-2} 是 a 模 p 的一个逆。

可以用快速幂加速计算。

NOIP 2012 Day2 T1 同余方程

求关于 x 同余方程 $ax \equiv 1 \pmod{b}$ 的最小正整数解。

样例输入：3 10

样例输出：7

数据范围：2 <= a, b <= 2,000,000,000

下节课再见