

《六元不定方程》解题报告

题目大意

给定整数 N, r , 求有多少六元有序数组 (a, b, c, a', b', c') 满足同余方程 $ab + a'b' \equiv bc + b'c' \equiv ca + c'a' \equiv r \pmod{N}$ 。其中 $a, b, c, a', b', c' \in \{0, 1, \dots, N-1\}$ 。

保证 $\mu(N) \neq 0$, 即 N 所有素因数的次数都为 1。

数据范围

对于所有数据, 保证 $0 \leq r < N \leq 10^{18}, N \geq 2, \mu(N) \neq 0$ 。

子任务编号	分值	$N \leq$	特殊限制
1	7	50	
2	8	500	
3	15	10^7	
4	20	10^{10}	$r = 0$
5	20	10^{10}	$r = 1$
6	10	10^{18}	N 为素数
7	20	10^{18}	

解题过程

考虑对于每个素因数 p 算出答案, 由中国剩余定理, N 的答案即为每个素因数答案之积。

[1] $r = 0$

先特判 (a, a') 或 (b, b') 全为 0 的情况, 简单分类讨论可得共有 $2p^3 + p^2 - 2p$ 种方案。

下面考虑 $(a, a'), (b, b')$ 均不全为 0 的情况。

固定 $a, a', (b, b')$ 共有 $p-1$ 组解, 此时 (c, c') 只需满足方程组 $\begin{cases} ac + a'c' \equiv 0 \\ bc + b'c' \equiv 0 \end{cases}$ 。

若 $ab' \not\equiv a'b$, 则该方程组有唯一解。否则 $(b, b') \equiv k(a, a')$, 容易发现 (c, c') 有 p 组解, 此时 $ka^2 + ka'^2 \equiv 0$, 即 $a^2 + a'^2 \equiv 0$ 。

记 $x^2 + y^2 \equiv r$ 的解数为 C_r , 则共有 $(C_0 - 1)(p-1)p + ((p^2 - 1)(p-1) - (C_0 - 1)(p-1)) = (C_0 - 1)(p-1)^2 + p^3 - p^2 - p + 1$ 种方案。

故共有 $3p^3 - p^2 - p + C_0(p-1)^2$ 种方案。

[2] $r \neq 0$

注意到 $(a, a'), (b, b'), (c, c')$ 均不能全为 0。

固定 $a, a', (b, b')$ 共有 p 组解, 此时 (c, c') 只需满足方程组 $\begin{cases} ac + a'c' \equiv r \\ bc + b'c' \equiv r \end{cases}$

若 $ab' \not\equiv a'b$, 则该方程组有唯一解。否则 $(b, b') \equiv k(a, a')$, 可以发现 $k = 1$, 此时 $a^2 + a'^2 \equiv r$, (c, c') 有 p 组解。

$ab' \equiv a'b$ 的方案数为 $\sum_{k=1}^{p-1} (k(a^2 + a'^2) \equiv r \text{ 的方案数})$, 即 $\sum_{k=1}^{p-1} C_{rk^{-1}} = p^2 - C_0$ 。

故有 $C_r p + ((p^2 - 1)p - (p^2 - C_0)) = p^3 - p^2 - p + C_0 + C_r p$ 种方案。

所以只需计算出 C_0, C_r 。

记 Legendre 符号为 $\left(\frac{a}{p}\right)$, 则 $x^2 \equiv a \pmod{p}$ 的解数为 $\left(\frac{a}{p}\right) + 1$, 故

$$\begin{aligned} C_r &= \sum_{i=0}^{p-1} \left(\left(\frac{i}{p} \right) + 1 \right) \left(\left(\frac{r-i}{p} \right) + 1 \right) \\ &= \sum_{i=0}^{p-1} \left(\frac{i(r-i)}{p} \right) + 2 \sum_{i=0}^{p-1} \left(\frac{i}{p} \right) + p \\ &= \sum_{i=1}^{p-1} \left(\frac{\frac{r}{i} - 1}{p} \right) + p \end{aligned}$$

当 $r = 0$ 时, $C_r = (p-1) \left(\frac{-1}{p} \right) + p$ 。

当 $r \neq 0$ 时, $C_r = \sum_{i=0}^{p-2} \left(\frac{i}{p} \right) + p = p - \left(\frac{-1}{p} \right)$ 。

计算答案时, 用 Pollard-Rho 分解素因数即可。

参考资料

[1] <https://oi-wiki.org/math/number-theory/pollard-rho/>

[2] <https://oi-wiki.org/math/number-theory/crt/>

[3] <https://oi-wiki.org/math/number-theory/quad-residue/>