

Binomial解题报告

长沙市雅礼中学 伍一鸣

Contents

1	问题简述	2
1.1	题目大意	2
1.2	数据规模	2
2	关键词	2
3	算法一	3
4	算法二	3
5	算法三	3
5.1	Lucas定理	3
5.2	具体算法	3
6	算法四	4
7	算法五	4
8	知识点补充	5
8.1	逆元素	5
8.2	原根	5
8.3	离散对数	5

1 问题简述

1.1 题目大意

给定 n 和 p ，对于所有的 $0 \leq x < p \mid x \in \mathbb{N}$ ，求满足 $C_n^m \equiv x \pmod{p}$ 的 m 的个数，输出答案在29进制下的最后一位。

1.2 数据规模

5%的数据： $n < 2000$

30%的数据： $n < 10^8$

50%的数据： $n < p^5, p \leq 5000$

85%的数据： $n < p^5, p \leq 2^{16}$

100%的数据： $n < p^{10}, p \leq 2^{16}$ (p 为质数)

2 关键词

数论知识, FFT, 动态规划

3 算法一

直接用 $C_n^m = C_{n-1}^m + C_{n-1}^{m-1}$ 这个递推式进行计算。

时间复杂度: $O(n^2)$

期望得分: 10分

4 算法二

我们有这样一个递推式 $C_n^m = C_n^{m-1} \times \frac{n-m+1}{m}$

由于 p 是质数, 对于除法可以用乘法逆元来解决。但是若计算到某一项时 C_n^m 我们就没有办法继续递推下去了, 为了让递推能够进行下去我们需要记录 C_n^m 中 p 的次数。若 p 的次数为 0 则当前余数即为答案, 否则当前的答案为 0。

一些常数优化:

- 预处理逆元
- 利用组合数的对称性少算一半

时间复杂度: $O(n)$

期望得分: 30分

5 算法三

5.1 Lucas定理

$$C_n^m \equiv \prod_{i=0}^k C_{n_i}^{m_i} \pmod{p}$$
$$n = \sum_{i=0}^k n_i \cdot p^i, m = \sum_{i=0}^k m_i \cdot p^i$$

推论: $C_n^m \equiv 0 \pmod{p} \iff \exists i, m_i > n_i$

由上述推论, 我们只需考虑 $x \neq 0$ 的情况

5.2 具体算法

我们令 $f_{i,j}$ 表示考虑了连乘式的前 i 项之后, 当前对于 p 的余数为 j 的方案数, 设 $b_{i,j}$ 为满足 $C_{n_i}^{m_i} \equiv j \pmod{p}$ 的 m_i 的个数, 我们只要套用算法二, 对于一个 i 可在 $O(n_i)$ 的时间计算出 $b_{i,j}$ 。转移的时候: $f_{i,j} \times b_{i,k} \rightarrow f_{i+1, j \times k \pmod{p}}$

时间复杂度: $O(p^2 \cdot \log n)$

期望得分: 50分

6 算法四

我们继续算法三的思路：要优化算法三无非是两条路：减少阶段数，减少每阶段转移的时间。阶段数是很难减少的，所以我们尝试减少每阶段转移的时间。我们取 p 的一个原根 g_0 ，将算法三中所有的 j 和 k 转成以 g_0 为底数， $\text{mod } p$ 意义下的离散对数。做完这一步的转化之后，我们可以发现相邻两阶段之间的转移就是一次多项式乘法了。对于多项式乘法我们可以使用FFT来优化。（关于FFT的介绍可以参见《算法导论》的相关章节。）使用FFT优化了之后，每个阶段的转移只需要 $O(p \log p)$ 的时间了。但是我们为了保证精度每次都需要逆FFT再让系数对29取余，再加上使用了大量复数运算，所以这个算法的常数巨大无比。

时间复杂度： $O(p \cdot \log p \cdot \log n)$

期望得分：85分

7 算法五

算法四的FFT中由于复数运算较大的常数，不一定能够拿到满分，我们还需要继续优化。再次阅读题目，我们对于答案只需输出 $\text{mod } 29$ 后的值这点的利用还不够。我们一直都没有利用到 $(29-1)^2 \times p \ll 2^{31}$ 这条性质。仔细研究了复根的相关性质我们发现，FFT中复根所需要的性质，原根都有，复根是可以原根来代替的。选取一个大质数 Q ，设 $Q-1 = 2^t \times c$ ，要求满足： $2^t \geq \text{len}$ (len 为作为结果的多项式的次数)，且结果中的系数都小于 Q ，这里的 Q 可以取 $479 \times 2^{21} + 1$ 。求出 Q 的一个原根 g ，用 $g^{\frac{Q-1}{c}}$ 代替1的单位复根作为FFT中的旋转因子。这样我们就只要在 $\text{mod } Q$ 的剩余系下来做FFT了。省掉了复数运算，常数大大减小。

时间复杂度： $O(p \cdot \log p \cdot \log n)$

期望得分：100分

8 知识点补充

8.1 逆元素

设 S 为一有二元运算 $*$ 的集合。若 e 为 $(S, *)$ 的单位元且 $a * b = e$ ，则 a 称为 b 的左逆元素且 b 称为 a 的右逆元素。

扩展欧几里得算法求解不定方程 $ax + bp = 1$ ，即可求得乘法逆元。

8.2 原根

设 m 是正整数， a 是整数，若 a 模 m 的阶等于 $\varphi(m)$ ，则称 a 为模 m 的一个原根。

目前没有什么特别好的算法求解原根， a 只能从2开始枚举，然后验证一下 $\varphi(m)$ 的所有真约数是不是 a 模 m 的阶。若都不是那么 a 为模 m 的一个原根。

8.3 离散对数

当模 m 有原根时，设 a 为模 m 的一个原根，则当 $x \equiv a^k \pmod{p}$ 时： $Ind_a x \equiv k \pmod{\varphi(m)}$ ，此处的 $Ind_a x$ 为 x 以整数 a 为底，模 $\varphi(m)$ 时的离散对数值。

本题中需要对于给定的 m 求解 $[1, m - 1]$ 的离散对数，这个可以按照 k 的大小逐个 $O(1)$ 求解。