《核》命题报告

重庆市巴蜀中学 常瑞年

Contents

1 题面 2
1.1 题目描述 2
1.2 限制与约定 2

2 题解 2
2.1 算法一 2
2.2 算法二 2
2.3 算法三 3
2.4 算法四 3
2.5 算法五 4
2.6 一些细节 4

3 总结与作者的话 5

4 致谢 5

5 参考资料 5

1 题面

1.1 题目描述

给定形如 $AB \equiv A \pmod q$ 的方程, 定义 $f(B)$ 为满足方程的 A 的解数, 求所有非奇异矩阵 B 的 $3^{f(B)}$ 的和

1.2 限制与约定

对于所有测试点, 有 $10^8 \leqslant mod \leqslant 10^9 + 7, 2 \leqslant q < mod$ 且满足 q, mod 为素数

本题采用子任务捆绑测试, 子任务描述及具体分值如下:

子任务	分值	n	q	mod
1	10	$\leqslant 3$	$\leqslant 3$	
2	20	$\leqslant 10^2$		
3	10	$\leqslant 3 \cdot 10^3$		
4	20	$\leqslant 10^6$		$=998244353$
5	10	$\leqslant 10^7$		$= q + 2$
6	30	$\leqslant 10^7$		

2 题解

2.1 算法一

暴力搜索所有的 A, B, 并注意到 A 的行之间无关, 只需枚举一行, 这样做可以通过子任务 1, 获得 5 分

2.2 算法二

为了方便, 接下来我们约定一些记号

记 $[n]_q = \frac{1-q^n}{1-q}, [n!]_q = [1]_q \cdot [2]_q \cdot \ldots \cdot [n]_q, \binom{n}{m}_q = \frac{[n!]_q}{[m!]_q[(n-m)!]_q}$

$\{n\}_q = (q^n - 1)(q^n - q)...(q^n - q^{n-1})$
$\{n, m\}_q = q = (q^m - q^{m-n})(q^m - q^{m-n+1})...(q^m - q^{m-1})$
$(\omega; q)_n = (1 - \omega)(1 - \omega q)(1 - \omega q^2)...(1 - \omega q^{n-1})$, 特别地,$(\omega; q)_0 = 1$
则 $\binom{n}{m}_q$ 可以写作 $\frac{(q;q)_n}{(q;q)_m (q;q)_{n-m}}$, 我们称作 q-binomial[1]

考虑令 a 为行向量, 则同算法一,$aB \equiv a \pmod q$ 的解数的 n 次方就是 $f(B)$

这等价于说求解非奇异线性变换 B 的 $1-$ 特征子空间[2]维数 (这是作者已经熟悉的语言, 读者也可以从解方程高斯消元的角度进行思考), 不妨设为 d, 则 $f(B) = q^d$

那么我们考虑求解所有非奇异且其 $1-$ 特征子空间维数为 d 的线性变换数量, 最后使用快速幂求解 $3^{q^{dn}}$

不妨设 n 维空间中已经确定了一个 $n - d$ 维子空间当作 $1-$ 特征子空间, 剩下的 d 维中无 $1-$ 特征子空间并且确定 B 维一非奇异线性变换的方案数为 g_d

则:

$$g_d = \{d, n\}_q - \sum_{1 \leqslant k \leqslant d} \binom{d}{k}_q g_{d-k}$$

这是说, 首先我们为剩下的空间 (的基) 确定一个非奇异的线性变换 (其方案数是 $\{d, n\}_q$), 但是这会导致 $1-$ 特征子空间的维度变高, 于是我们枚举变高的维度 k 并容斥

暴力做是 $O(n^2)$ 的, 可以通过子任务 $1, 2, 3$, 可以获得 25 分

2.3 算法三

注意到将式子移项之后拆开 $q - binomial$ 可以写成卷积, 于是求逆可以得到时间复杂度 $O(n \log n)$, 可以通过子任务 $1, 2, 3, 4$, 获得 45 分

2.4 算法四

其实我们可以推导一个不需要求逆的算法, 为了遵循传统, 这里我们把 $q - binomial$ 用 $(q; q)_n$ 的方式表示出来

[1] https://en.wikipedia.org/wiki/Gaussian_binomial_coefficient
[2] 可见https://en.wikipedia.org/wiki/Vector_space#Eigenvalues_and_eigenvectors

因此考虑生成函数 $\zeta(x)=\sum_n \frac{x^n}{(q;q)_n}$ 的逆
注意到 $\zeta(x)-\zeta(qx)=\zeta(x)x$, 即 $(1-x)\zeta(x)=\zeta(qx)$
那么 $\zeta^{-1}(x)=(1-x)\zeta^{-1}(qx)$ 两边取 $[x^n]$ 即可递推求得 $\zeta^{-1}(x)$
于是我们用递推代替了求逆, 不过还是需要 NTT, 与算法三得到相同的分数

2.5 算法五

使用生成函数的想法非常不错, 干脆直接求出答案的递推式
我们定义 q-GF 为形如 $\sum_n \frac{f_n x^n}{(q;q)_n}$ 的生成函数
令 $C(x)=\sum_n \frac{\{n,m\}_q x^n}{(q;q)_n}$, 这里把 m 作为原题目中的 n,n 作为下标比较美观
则我们相当于要求 $C(x)\zeta^{-1}(x)$
考虑 $C(x)$ 满足的方程:

$$C(x)-C(qx)=q^mC(x)-q^{m+1}C(q^{-1}x)$$

两边乘以 $\zeta^{-1}(x)$ 得:

$$(1-q^m)C(x)\zeta^{-1}(x)+q^{m+1}C(q^{-1}x)\zeta^{-1}(x)=C(qx)\zeta^{-1}(x)$$

注意到 $\zeta^{-1}(qx)=\frac{\zeta^{-1}(x)}{1-x}$,$\zeta^{-1}(q^{-1}x)=(1-q^{-1}x)\zeta^{-1}(x)$
并设 $D(x)=C(x)\zeta^{-1}(x)$ 为我们要求的目标, 则代入整理得:

$$(1-q^m)D(x)+\frac{q^{m+1}D(q^{-1}x)}{1-q^{-1}x}=D(qx)(1-x)$$

代入 $x\to qx$ 即:

$$(1-x)(1-q^m)D(qx)+q^{m+1}D(x)=D(q^2x)(1-x)(1-qx)$$

两边取 $[x^n]$ 递推即可, 可以通过所有子任务, 得到满分

2.6 一些细节

容易发现, 在 d 小的时候, 递推式并不起作用, 因此我们直接使用 $O(n^2)$ 的部分

3 总结与作者的话

作者命此题主要有两个目的, 一是微小的扩充生成函数的用途, 当我们拥有了 EGF,OGF,BGF,DGF,GGF, 等等, 我们仍然可以考虑使用同样的形式进行扩展, 比较狭窄地想, 这只是 q-analogue 罢了, 不过我们仍然可以赋予其人为构造的意义, 另一方面, 作者的意图在于让大家熟悉 q, 而 q 多半就与某种特定的数学对象有关, 尤其是线性代数, 群论

这里考察的内容在这样的扩充中是较为基础的, 仅拼凑了矩阵可逆的限制与特征子空间的限制, 把一个一维的问题变得稍微复杂, 其实我们可以扩展出去, 考察幂零矩阵, 幂等矩阵, 辛酉矩阵, 正交矩阵相关的计数, 直至群到一般线性群的同态计数, 甚至有没有可能群表示计数 (这一个是作者的胡思乱想), 能够考察的东西非常多, 但是由于重点在于考察 q 的相关推导及计算, 作者挑了一个简单而稍有代表性的, 而把更多的可能性留给之后的选手考察 (可以拿去出题)

可是当我们对这样的组合计数, 以及其衍生进行考察时, 我们仍然灰心的认为, 做和出这样的题目, 也许会有一时的满足, 但是其功能上来说不过等同于玩具, 再过复杂和技巧性的推导其实从一开始就是没有意义的

哦对了, 你还可以把整式递推的方法弄上来把这题出道 $9e8$

4 致谢

感谢 EI, 子空间反演真好玩

5 参考资料

[1] 李白天.https://www.luogu.com.cn/blog/EntropyIncreaser/subspace-inversion