Codechef DEC12 Quasi-Polynomial Sum
解题报告

镇海中学 邹逍遥

1 试题来源

Codechef DEC12 QPOLYSUM

2 问题简述

给定一个D次多项式$P(x)$的前$(D+1)$项$P(0) \mod M, P(1) \mod M, \cdots, P(D) \mod M$分别为$A_0, A_1, \cdots, A_D$，非负整数Q，正整数M,N，求$(P(0) \times Q^0 + P(1) \times Q^1 + \cdots + P(N-1) \times Q^{N-1}) \mod M$ 的值。

3 数据范围

1 $\leq$数据组数≤ 5000

$1 < M < 10^{18}$

$0 \leq Q < M$

$1 \leq N < 10^{100000}$

$0 \leq D < 20000$

$0 \le A_i < M$

所有数据中$D+1$的和不超过20000

所有数据中N的位数和不超过10^5

M不能被2至$D+14$中的任意一个数整除

4 解答

令$G(n) = \Sigma_{i=0}^{n-1} P(i)Q^i$，通过数学归纳法可以得出$G(n) = Q^n F(n) - F(0)$，其中$F(x)$为一个次数为D的多项式。

证明：

当$D=0$时这就是一个等比数列求和公式，显然成立。

假设当$D=k$时成立，那么当$D=k+1$时，令$S_d(n) = \Sigma_{i=0}^{n-1} P(i)Q^i$，那么$QS_d(n) = \Sigma_{i=0}^{n-1} P(i)Q^{i+1} = \Sigma_{i=1}^{n} P(i-1)Q^i$

于是$(Q-1)S_d(n) = \Sigma_{i=0}^{n-1}(P(i-1)-P(i))Q^{i+1} + P(n-1)Q^n - P(-1)$。

由于$P(i-1)-P(i)$是一个次数为$D-1$的多项式，那么根据假设，$\Sigma_{i=0}^{n-1}(P(i-1) - P(i))Q^i$能被表示成$Q^n f(x) - f(0)$。

于是$S_d(n)$能被表示成$\frac{Q^n F(n)}{Q-1} - c$，其中$F(n) = (f(n) + P(n-1))$，c为常数。

当$n=0$时可以得出$S_d(n) = 0 = F(0) - c$，所以$c = F(0)$，即$S_d(n) = Q^n F(n) - F(0)$。

证毕。

由$G(n) = Q^n F(n) - F(0)$得出$G(n+1) - G(n) = P(n)Q^n = Q^{n+1}F(n+1) - Q^n F(n)$，即$P(n) = QF(n+1) - F(n)$，$F(n+1) = \frac{F(n)+P(n)}{Q}$。这样就得到了$F(n)$的递推式。

虽然我们不知道$F(n)$任意一项的值，但是可以根据递推式把$F(1), F(2), \cdots, F(d+$

1)表示成关于$F(0)$的一次函数。

由于$F(n)$是一个次数为D的多项式，那么就满足$\Sigma_{i=0}^{d+1}(-1)^i\binom{d+1}{i}F(i)=0$，于是利用这个方程就得到了一个关于$F(0)$的一次函数，解出$F(0)$即可。之后利用拉格朗日插值法即可算出$F(n)$。那么到现在为止问题看起来已经解决了。

4.1 没有逆元的情况

但是注意到在递推和解方程的过程中会涉及除法运算，但在模M的情况下不一定有逆元。

最后方程中$F(0)$的系数为$\Sigma_{i=0}^{d+1}(-1)^i\binom{d+1}{i}Q^{-i}=(1-Q^{-1})^{d+1}$，所以需要用到$Q-1$的逆元。同时在递推式中也需要用到$Q$的逆元。那么假如在模$M$下没有$Q$或$Q-1$的逆元就会无法处理。

4.2 $Q=0$和$Q=1$时

为了解决这个问题，首先需要处理掉$Q=0$和$Q=1$的情况。

当$Q=0$时，答案就是$P(0)$。

当$Q=1$时，先利用插值算出$P(D+1)$，令$S(n)=\Sigma_{i=0}^{n}P(i)$，那么$S(n)$显然是一个$D+1$次多项式。通过$S(n)$的前$D+1$项就可以算出$S(n)$的值。

4.3 $Q\geq 2$时

容易想到可以将模数拆成几个小模数分别计算然后利用中国剩余定理合并。

那么令$M=m_1m_2m_3$，其中$(m_2m_3,Q)=1,m_1|Q^u,(m_1m_3,Q-1)=1,m_2|(Q-1)^v$，$u,v$是满足条件的最小自然数。

那么对于三个模数分别解决。由于$(m_3, Q) = (m_3, Q-1) = 1$，所以模$m_3$的答案可以用上述做法算出。

4.3.1 模m1的解法

由于$m_1 | Q^u$，当$i \geq u$时，$P(i)Q^i \equiv 0 \pmod{Q^u}$，不需要计算。所以可以通过前几项直接算出。

4.3.2 模m2的解法

设$m_2 = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$，容易看出$v \leq \max(a_1, a_2, \cdots, a_k)$。

根据题目条件M与$2, 3, \cdots, d+1$互质，所以M的最小素因子不会小于17。

因为$17^{14} > 10^{18}$，所以$v \leq \max(a_i) \leq 14$，即M与$2, 3, \cdots, d+v$互质。

$P(i)Q^i = P(i)((Q-1)+1)^i = P(i)\Sigma_{j=0}^{i}\binom{i}{j}(Q-1)^j$

当$j \geq v$时，$(Q-1)^j \equiv 0 \pmod{(Q-1)^v}$，可以忽略。所以

$\Sigma_{i=0}^{n-1} P(i)Q^i = \Sigma_{j=0}^{v-1}(Q-1)^j \Sigma_{i=0}^{n-1} P(i)\binom{i}{j}$

其中$\binom{i}{j}$是一个关于i的j次多项式。所以$\Sigma_{i=0}^{n-1} P(i)Q^i$是一个次数不超过$d+v$的多项式

令$G(n) = \Sigma_{i=0}^{n-1} P(i)Q^i$，可以暴力算出$G(0), G(1), \cdots, G(d+v)$，由于$M$与$2, 3, \cdots, d+v$互质，所以可以算出$G(n) \bmod m_2$的值。

4.4 算法效率

时间复杂度：$O(D + \log n)$

空间复杂度：$O(D)$