random

April 27, 2014

题目简述

M_0是一个$[0, 2^m)$之间的整数。
定义：

$$M_n = \begin{cases} 2M_{n-1} & ,2M_{n-1} < 2^m \\ (2M_{n-1} - 2^m) \oplus x & ,2M_{n-1} \geq 2^m \end{cases}$$

我们有两类问题：
第一类：给定M_0, x, k，求出M_k。
第二类：给定$M_0, x, l, M_{k'}$，求出M_k使得$M_{k \cdot 2^l} = M_{k'}$。

数据范围

测试点编号	m	k	l	$type$	x是否为“好的”
1	≤ 10	$\leq 10^9$	N/A	0	是
2	≤ 10	$\leq 10^9$	≤ 10	1	是
3	≤ 100	$\leq 10^9$	N/A	0	是
4	≤ 100	$\leq 10^9$	N/A	0	是
5	≤ 100	$\leq 10^9$	N/A	0	是
6	≤ 100	$\leq 10^5$	$= 1$	1	是
7	≤ 100	$\leq 10^9$	≤ 10	1	是
8	≤ 100	$\leq 10^9$	≤ 10	1	是
9	≤ 100	$\leq 10^9$	≤ 10	1	是
10	≤ 1000	$\leq 10^{18}$	≤ 10	1	是
11	≤ 1000	$\leq 10^{18}$	≤ 10	1	是
12	≤ 1000	$\leq 10^{18}$	≤ 10	1	是
13	≤ 2000	$\leq 10^{18}$	N/A	0	是
14	≤ 2000	$\leq 10^{18}$	N/A	0	是
15	≤ 500000	$\leq 10^6$	N/A	0	否
16	≤ 500000	$\leq 10^6$	N/A	0	否
17	≤ 1000000	$\leq 10^6$	N/A	0	否
18	≤ 1000000	$\leq 10^6$	N/A	0	否
19	≤ 1000000	$\leq 10^6$	N/A	0	否
20	≤ 1000000	$\leq 10^6$	N/A	0	否

问题分析

考虑将x看成一个GF(2)中的一个多项式，那么每次操作就相当于：

$$M = x \cdot M \bmod (X + x^m).$$

令$MOD = X + x^m$.
那么考虑第一类问题，等价于求$ax^k \bmod (MOD)$.
考虑第二类问题，就是个顶ax^{k*2^l}的情况下求出ax^k.

第一类问题

主要问题在于快速的进行多项式乘法和多项式取模。
由于在GF(2)上进行操作，所以可以2进制压位。

数据1, 3, 4, 5, 13, 14

如果我们使用二进制压位来进行多项式乘法和多项式取模，复杂度都是$O(n^2/32)$。
那么使用快速幂计算出$x^k \pmod{MOD}$即可。

多项式快速乘法

很简单的我们可以使用FFT进行多项式快速乘法。
复杂度$O(n \log n)$。

多项式快速除法

我们可以考虑将多项式快速除法转换为快速乘法。
考虑$f(x) = q(x)g(x) + r(x)$，期中$degf = n, degg = m, degr < m$，其中$g$是一个首一多项式。
我们只需要求出q即可。
注意到$f(1/x) = q(1/x)g(1/x) + r(1/x)$。两边同乘$x^n$, 得到:

$$x^n f(1/x) = x^{n-m} q(1/x) x^m g(1/x) + x^{n-m+1} x^{m-1} r(1/x).$$

令$x^n(1/x) = F(x)$, $G(x)$与$Q(x), R(x)$同理。
那么

$$F(x) = Q(x)G(x) + x^{n-m+1}R(x)$$
$$F(x) = Q(x)G(x) \pmod{x^{n-m+1}}$$
$$F(x)G(x)^{-1} = Q(x) \pmod{x^{n-m+1}}$$

多项式快速除法

故只要求出$G(x)^{-1} \pmod{x^{n-m+1}}$即可。
如何求出一个多项式关于x^n的逆元。
考虑倍增构造，令$h_0 = 1$，那么易知$h_0 G = 1 \pmod{x^1}$。
若$h_i G = 1 \pmod{x^{2^i}}$。
不妨令$h_{i+1} = 2h_i - Gh_i^2$。
那么可以看出$h_{i+1} G = 1 \pmod{x^{2^{i+1}}}$。
重复$\log n$次就能得出需要的逆元。
有了逆元只有就能把除法变成乘法了。

第二类数据

首先我们注意到，数据是好的意味着它近似于等概率的分布，而给定当前的数值，下一个值是唯一的，那么实际上我们会走出一个环，如果这个环没有包含$[0, 2^m - 1]$中所有的数，那么某些数就永远不会被选到，这也就意味着他们肯定不是好的。
而这意味着，$x^{2^m} = x$。
那么我们就立刻知道$x^{2^{m-l} \cdot 2^l} = x$。
那么在给定了ax^k的情况下，我们先求出a的逆元a^{2^m-2}，然后左乘它得到x^k，然后计算$(x^k)^{2^{m-l}}$，再左乘回a即可。