水题选讲

mcfx

March 15, 2017

sro 各位大佬 orz

我等下讲的题各位大佬应该有做过的，那么可以开始冬眠了。
如果觉得我太菜不想听的，也可以冬眠了。
还有那个叫 *WXH* 的大佬，也可以冬眠了。

一道水题

$F(0)=0, F(1)=1, F(n)=(F(n-1)+F(n-2))mod\ P$
其实就是斐波那契数列
给一个 y，求出一个 x，满足 $F(x)=y$
原题的范围是 $P=10^k, k\leq 18$
各位大佬可以想一下 P 为任意数怎么做
（假）提示：BSGS

一道水题

$F(0)=0, F(1)=1, F(n)=(F(n-1)+F(n-2)) mod\ P$
其实就是斐波那契数列
给一个 y，求出一个 x，满足 $F(x)=y$
原题的范围是 $P=10^k, k \leq 18$
各位大佬可以想一下 P 为任意数怎么做
（假）提示：BSGS
如果用BSGS，那么每次需要给出一个矩阵 A，然后判断集合中是否存在一个矩阵 B，使 $A \cdot B$ 的某一项为 y
如果有哪位大佬知道这么一种数据结构，那么还是非常资辞的

两个结论

对于 $P = p^y (a > 0, p\ is\ prime)$，如果 F 有一个循环节为 x，那么对于 $P = p^{y+1}$，$x \cdot p$一定为一个循环节
还有一个比较显然的结论，存在一个循环节是一个积性函数（不一定最小）
大概也算提示吧

证明

考虑一个矩阵 $A=\begin{bmatrix}1 & 1\\ 1 & 0\end{bmatrix}$，那么 A^x 在 $mod\ P$ 意义下是 $\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$

在 $mod\ P\cdot p$ 意义下是 $\begin{bmatrix}a\cdot P+1 & b\cdot P\\ b\cdot P & c\cdot P+1\end{bmatrix}$

由于 $\begin{bmatrix}a_1\cdot P+1 & b_1\cdot P\\ b_1\cdot P & c_1\cdot P+1\end{bmatrix}\cdot\begin{bmatrix}a_2\cdot P+1 & b_2\cdot P\\ b_2\cdot P & c_2\cdot P+1\end{bmatrix}=$

$\begin{bmatrix}(a_1+a_2)\cdot P+1 & (b_1+b_2)\cdot P\\ (b_1+b_2)\cdot P & (c_1+c_2)\cdot P+1\end{bmatrix}(mod\ P\cdot p)$

那么 $A^{x\cdot p}=\begin{bmatrix}a\cdot P\cdot p+1 & b\cdot P\cdot p\\ b\cdot P\cdot p & c\cdot P\cdot p+1\end{bmatrix}=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}(mod\ P\cdot p)$

即对于 $P=p^{y+1}$，$x\cdot p$ 为一个循环节

题解

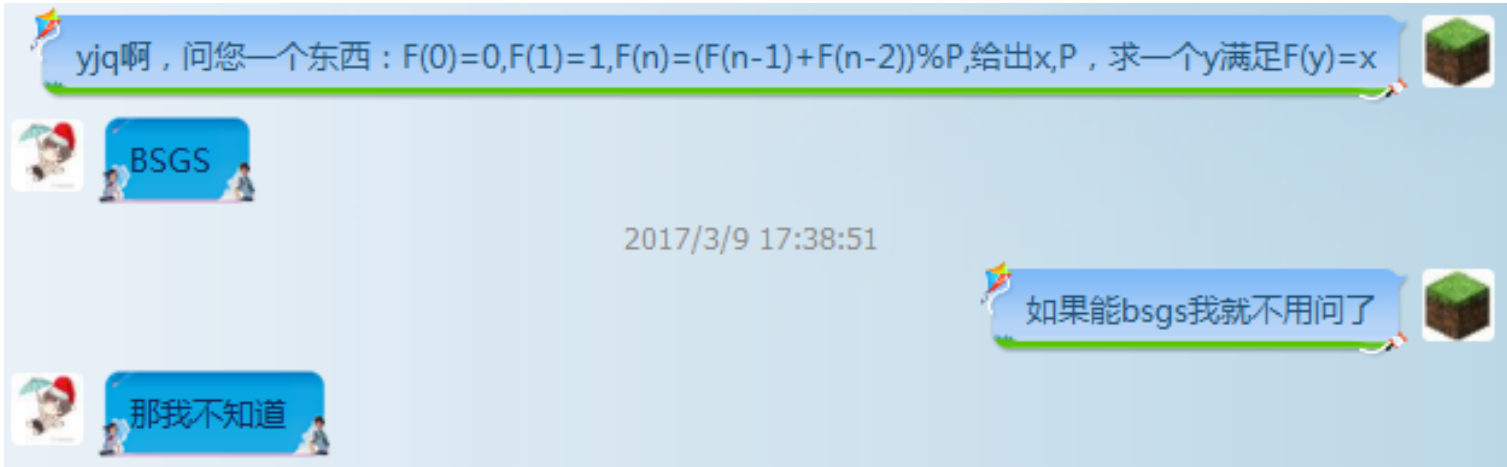
假设 $P = 2^k$,那么 $3 \cdot P$ 一定是 F 的循环节
题目是给一个 y，求出一个 x，满足 $F(x) = y$

题解

假设 $P = 2^k$,那么 $3 \cdot P$ 一定是 F 的循环节
题目是给一个 y，求出一个 x，满足 $F(x) = y$
考虑搜索
每个状态保存当前的 P, x ，那么对于当前不合法的 x ，可以不用继续搜索
会搜索到的状态不会很多

题解

假设 $P = 2^k$,那么 $3 \cdot P$ 一定是 F 的循环节
题目是给一个 y，求出一个 x，满足 $F(x) = y$
考虑搜索
每个状态保存当前的 P, x ，那么对于当前不合法的 x ，可以不用继续搜索
会搜索到的状态不会很多
题目里 $P = 10^k$ ，可以分解质因数做，也可以直接用循环节搜索
同样的做法在 P 是一些较小质数的乘积时也可以使用
所以如果 $P = 10^9 + 7$ ，各位大佬有没有做法啊？（YJQ 说她不会）



又一道水题

给一个长为 n 的置换 B，求出一个置换 A，满足 $A^k = B$

$n \leq 10^6$

又一道水题

给一个长为 n 的置换 B，求出一个置换 A，满足 $A^k = B$

$n \leq 10^6$

王修涵大概已经秒了这个题了吧

题解

考虑 A 中的一个长为 L 的循环 S，如果 $gcd(L,k)=1$，那么在 B 中 S 的长度仍为 L
如果 $gcd(L,k)$ 不为 1，那么在 B 中 S 被分为 $gcd(L,k)$ 个长度为 $\frac{L}{gcd(L,k)}$ 的循环

题解

考虑 A 中的一个长为 L 的循环 S，如果 $gcd(L,k)=1$，那么在 B 中 S 的长度仍为 L

如果 $gcd(L,k)$ 不为 1，那么在 B 中 S 被分为 $gcd(L,k)$ 个长度为 $\frac{L}{gcd(L,k)}$ 的循环

考虑 B 中的一个长为 L_2 的循环 S，如果 $gcd(L_2,k)=1$，那么在 A 中 S 可以是一个长度仍为 L_2 的循环

否则要在 A 中找到一个长为 L_1 的循环，使 $gcd(L_1,k)\cdot L_2=L_1$

题解

考虑 A 中的一个长为 L 的循环 S，如果 $gcd(L,k)=1$，那么在 B 中 S 的长度仍为 L

如果 $gcd(L,k)$ 不为 1，那么在 B 中 S 被分为 $gcd(L,k)$ 个长度为 $\frac{L}{gcd(L,k)}$ 的循环

考虑 B 中的一个长为 L_2 的循环 S，如果 $gcd(L_2,k)=1$，那么在 A 中 S 可以是一个长度仍为 L_2 的循环

否则要在 A 中找到一个长为 L_1 的循环，使 $gcd(L_1,k)\cdot L_2=L_1$

设 $t=gcd(L_1,k)$，那么 $t=gcd(t\cdot L_2,k)$，即 $gcd(L_2,\frac{k}{t})=1$

显然，t 一定是 $gcd(L_2,k)$ 的倍数，也一定是 $gcd(L_2,\frac{k}{gcd(L_2,k)})$ 的倍数……

如此重复，直到 gcd 为 1 时就求出了一个 t 的最小值

把这 t 个循环接在一起就得到了答案

sro 各位大佬 orz

谢谢各位大佬！