D. Discrete Logarithm Problem

PROBLEM DESCRIPTION

$a^x \equiv b \ (mod\ p)$

離散對數，給 p、a、b 求 x。

SOLUTION TECHINQUES

暴力 / Baby-step giant-step

SOLUTION SKETCHES

(當時我在賽場回想了好一陣子才想起 Baby-step giant-step 怎麼做… orz)

裸離散對數，不過這題其實不需要 Baby-step giant-step，測資筆數只有幾十筆。

一個數字的次方(取 p 餘數)最終必然會有循環，我們可以很簡單推論這個循環長度不會超過 p (不會經過 p 個以上的數字)，所以我們只要暴力計算 $a^{\{0,1,2,\dots,p-1\}}$ (mod p)有沒有出現 b 即可，並記錄次方數 x。

TIME COMPLEXITY

每筆測資 O(p)

SOLUTION PROGRAM FOR REFERENCE

None due to live contest.