

## B. BSGS-數學天才的難關

### Description

很久以前在某所冠地名高中有一名天才學生黃瓜，他可以用七天讀完國中會考，用一個月讀完高中學測，而這樣的他尤其擅長數學，常常無師自通超前學習，也因為他什麼都會，考試都考超過一百分，所以常常數學課上不聽數學老師上課，由於他這樣不專心聽課的態度讓數學老師很生氣。

於是乎數學老師心生一計，有一天老師在上課前對他說：「現在老師跟你打一個賭，只要老師出了一個問題他回答的出來，就送給他一台 PS6，但如果他回答不出來，他之後就得乖乖上課。」黃瓜本來信心滿滿，但是這次他失算了，因為老師要求他計算出符合下方同餘方程式的答案  $x$ 。

$$a^x \equiv b \pmod{p}$$

由於老師給出的數字很大，已經超出人類的能力範圍，就算是天才也是人類也是有極限的，於是他偷偷傳訊息來拜託你用程式的能力來幫助他順利回答出正確答案，並且答應你會讓你一起跟他玩 PS6。

請你根據題目給定的解法和步驟，設計出能快速解開這個方程式的程式，幫助他度過這個難關，讓你跟他能一起開心地玩免錢的 PS6。

### 同餘方程式說明

同餘：當兩個整數  $x, y$  除以同一個正整數  $m$ ，若得相同餘數，則稱二整數  $a, b$  對於模數  $m$  同餘，記為

$$a \equiv b \pmod{m}$$

同餘方程式，顧名思義就是餘數相同的方程式，以下列方程式舉例，此方程式的含意就是利用 2 對 3, 5 取餘數的結果相同 ( $3\%2 = 5\%2 = 1$ )

$$3 \equiv 5 \pmod{2}$$

### 算法說明

根據歐拉定理，若解存在，則  $x$  有無限多組解，且必定存在一解在區間  $[0, p-1]$  之間，所以可以嘗試枚舉區間內的所有  $x$  來計算答案。但是還有一個夠快速的做法，就是 BSGS (BABY-STEP GIANT-STEP) 算法，首先我們可以令  $x = m * i - j$ ，而  $m$  為  $\sqrt{p}$  的向上取整，並將方程式改寫為下方形式

$$a^{m*i-j} \equiv b \pmod{p}$$

接下來我們將  $a$  的  $-j$  次方進行移項就能得到下方的方程式

$$a^{m*i} \equiv b \times a^j \pmod{p}$$

經過計算，我們可以知道  $i$  的範圍介於 1 到  $m$ ，而  $j$  的範圍介於 0 到  $m - 1$  之間，接著我們枚舉右側的所有  $j$  並把結果儲存起來。若對於一個  $i$  存在一個  $j$  使得兩者同餘，表示  $(i, j)$  會符合方程式，最後再使用  $(i, j)$  轉換出  $x$  並輸出答案。

## Input

第一行為三個正整數  $a, b, p$ ，代表上述同餘方程式左側的底數、方程式右側的數字和模數。

各變數範圍如下：

- $1 \leq a, b, p \leq 10^9$
- 保證  $a$  和  $p$  互質
- 保證此題目在  $[0, p]$  區間內有至少一解

## Output

請輸出一個整數代表  $x$  使得方程式成立。

### Sample 1

Input	Output
3 5 2	1

### Sample 2

Input	Output
7 3 10	3

### Sample 3

Input	Output
7 4 17	4

## 配分

在一個子任務的「測試資料範圍」的敘述中，如果存在沒有提到範圍的變數，則此變數的範圍為 Input 所描述的範圍。

子任務編號	子任務配分	測試資料範圍
0	0%	範例測資
1	8%	$a \leq 100, p \leq 100$
2	21%	$a \leq 10^5, p \leq 1000$
3	24%	$p \leq 10^5$
4	47%	無額外限制

## Hint

Sample3 的實際做法如下：

已知  $a = 7, b = 4, p = 17, m = \sqrt{p} = 4.1231 \dots$ ，向上取整可得  $m = 5$ ，接著我們枚舉  $j$  的範圍並記錄  $4 \times 7^j \pmod{17}$  的答案，並且枚舉  $i$  並計算  $7^{5 \times i} \pmod{17}$  的結果。

$$\begin{array}{ll}
 \underline{j = 0, 4 \times 7^0 \pmod{17} = 4} & \underline{i = 1, 7^{5 \times 1} \pmod{17} = 11} \\
 \underline{j = 1, 4 \times 7^1 \pmod{17} = 11} & i = 2, 7^{5 \times 2} \pmod{17} = 2 \\
 \underline{j = 2, 4 \times 7^2 \pmod{17} = 9} & i = 3, 7^{5 \times 3} \pmod{17} = 5 \\
 \underline{j = 3, 4 \times 7^3 \pmod{17} = 12} & \underline{i = 4, 7^{5 \times 4} \pmod{17} = 4} \\
 j = 4, 4 \times 7^4 \pmod{17} = 16 & i = 5, 7^{5 \times 5} \pmod{17} = 10
 \end{array}$$

可以看到當  $i = 1$  時與  $j = 1$  的結果相同所以可以反推得出有一個  $x = 5 \times 1 - 1 = 4, 7^4 = 2401 \equiv 4 \pmod{17}$ 。

而當  $i = 4, j = 0$  時可得  $x = 5 \times 4 - 0 = 20$  為此方程式的另一個解。