

問題 17 – 電熊的 $a+b$ 問題 (bear)

(25 分)

問題敘述

這世界上有一隻凌駕於人類智商的熊，牠就是電熊，平時會電電別人當有趣。如果不想被電，那就只能餵他吃蜂蜜，或是解出一道電熊出的 $a+b$ 問題！

現在，你在路上遭遇了電熊，手邊沒有蜂蜜，但又不想被電的你，自然只剩解出題目這一條路了！電熊會給你若干個資訊，只要你能夠回答出 $a+b$ ，你就可以免於攻擊。這些資訊及變數的定義如下：

1. p, q 為兩個質數，且 p, q 不相等。
2. $n = pq$, $g = n + 1$, $\lambda = (p - 1)(q - 1)$ 。
3. a, b, r_a, r_b 為四個整數。
4. $c_a \equiv g^a r_a^n \pmod{n^2}$, $c_b \equiv g^b r_b^n \pmod{n^2}$ 。

現在給你 $c_a c_b \pmod{n^2}$, λ, n 這三個數字，你能夠告訴電熊 $a+b$ 的最小可能值是多少嗎？

輸入格式

每個輸入只有一行，包含三個整數，分別是 $c_a c_b \pmod{n^2}$, λ, n 。
這三個數字中間以空白隔開。

輸出格式

請輸出一行整數，也就是 $a+b$ 的最小可能值為多少。

資料範圍

- $1 \leq p, q \leq 256$ ，其中 p, q 是質數。
- $1 \leq a + b < n$
- $1 \leq r_a, r_b < n$
- $1 \leq c_a c_b < n^2$

資料範例

輸入範例 1

503160642 32760 33127

輸出範例 1

3498

範例解釋 1

在這個範例中，電熊心中所想的 $a = 348$, $b = 3150$, $r_a = 12745$, $r_b = 3536$ 。

所以答案是 $348 + 3150 = 3498$ 。

而 $c_a c_b$ 是透過下面式子得出來的結果：

$$(33127 + 1)^{348} (12745)^{33127} (33127 + 1)^{3150} (3536)^{33127} \equiv 503160642 \pmod{33127^2}$$

輸入範例 2

838515010 29548 29893

輸出範例 2

7414

範例解釋 2

在這個範例中，電熊心中所想的 $a = 7171$, $b = 246$, $r_a = 20971$, $r_b = 8718$ 。

所以答案是 $7171 + 246 = 7414$ 。

而 $c_a c_b$ 是透過下面式子得出來的結果：

$$(29893 + 1)^{7171} (20971)^{29893} (29893 + 1)^{246} (8718)^{29893} \equiv 838515010 \pmod{29893^2}$$

輸入範例 3

144104393 39508 39913

輸出範例 3

32277

範例解釋 3

在這個範例中，電熊心中所想的 $a = 14836$, $b = 17441$, $r_a = 8125$, $r_b = 38352$ 。

所以答案是 $14836 + 17441 = 32277$ 。

而 $c_a c_b$ 是透過下面式子得出來的結果：

$$(39913 + 1)^{14836} (8125)^{39913} (39913 + 1)^{17441} (38352)^{39913} \equiv 144104393 \pmod{39913^2}$$

符號意思以及可能有用的提示

- $a \equiv b \pmod{c}$ 的意思是 $a \% c = b \% c$ ，其中 $\%$ 是取餘數的意思。例如 $5 \% 2 = 1$ 。
歐拉定理和二項式定理可能會對你有幫助。