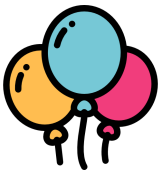


第三題：橢圓曲線 (C_Elliptic)

建議印出題本或開兩份以上題本頁面來模擬實際比賽翻頁體驗

問題敘述

小明想報名參加 WOW (Worst Of Worst) 程式選拔賽，最近在準備的過程中看了許多數學書，其中一題看到了跟模逆元相關的東西。他發現在模 p 底下，每個**不是 0** 的餘數 a，都存在另一個餘數 b，使得 $ab \equiv 1 \pmod{p}$。這個數字被稱為 a 的模逆元，記為 $b = a^{-1}$。他又發現根據費馬小定理 $a^{-1} \equiv a^{p-2} \pmod{p}$，因為 $a \cdot a^{p-2} \equiv a^{p-1} \equiv 1 \pmod{p}$。

小明後來又看到一題跟橢圓曲線有關的題目。橢圓曲線指的一條光滑、射影、虧格為 1 的代數曲線，以及曲線上的一個有理點。書上寫道，根據 *Riemann-Roch* 定理，這些曲線都會是三次曲線（請見下方的橢圓曲線小教室），亦即形如

$$Ax^3 + Bx^2y + Cxy^2 + Dy^3 + Ex^2 + Fxy + Gy^2 + Hx + Iy + J = 0$$

若將那個有理點設為坐標原點，則 $J = 0$。

小明現在想要知道這條曲線在 F_p 中有哪些點，也就是有多少 $0 \le x, y < p$ 滿足

$$Ax^3 + Bx^2y + Cxy^2 + Dy^3 + Ex^2 + Fxy + Gy^2 + Hx + Iy \equiv 0 \pmod{p}$$

小明發現如果 $y \neq 0$，做 $x \equiv wz^{-1} \pmod{p}$，$y \equiv z^{-1} \pmod{p}$ 的變數代換（$w \equiv xy^{-1} \pmod{p}$，$z \equiv y^{-1} \pmod{p}$），並將兩邊同乘 z^3，會得到

$$Aw^3 + Bw^2 + Cw + D + Ew^2z + Fwz + Gz + Hwz^2 + Iz^2 \equiv 0 \pmod{p}$$

整理一下就會是

$$(Hw + I)z^2 + (Ew^2 + Fw + G)z + (Aw^3 + Bw^2 + Cw + D) \equiv 0 \pmod{p}$$

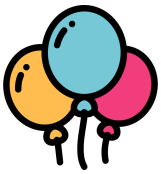
小明只需要枚舉 w，方程式就變成一個 z 的二次方程式了！不過小明開始煩惱，現在給定一個二次方程式

$$az^2 + bz + c \equiv 0 \pmod{p}$$

要如何去解他呢？他想起國中時老師教的配方法，得到

$$(2az + b)^2 \equiv b^2 - 4ac \pmod{p}$$

小明發現**在 $a = 0$ 或 $a = b = 0$ 或 $a = b = c = 0$ 的時候都有特別的情況要處理**，而在 $a \neq 0$ 時他只要處理好模 p 的每個餘數是否可以開根號就好，也就是把所有



$0^2 \bmod p, 1^2 \bmod p, 2^2 \bmod p, \ldots, (p-1)^2 \bmod p$ 存起來，再檢查 $b^2 - 4ac$ 是哪些數的平方即可。

開完根號後會得到

$$2az + b \equiv d \pmod{p}$$

解就會是 $z \equiv (2a)^{-1}(d-b) \pmod{p}$。

小明於是拿 $x^3 + 2xy^2 + 2y^3 + xy + y^2 + y \equiv 0 \pmod{3}$ 試了一遍。

在模三底下，我們有

	0	1	2
根號	0	1, 2	無
逆元	無	1	2

若 $y = 0$，則 $x^3 \equiv 0 \pmod{3}$，枚舉以後發現解只有 $x = 0$。

若 $y \neq 0$，則用一樣的變數代換可以得到

$$z^2 + (w+1)z + (w^3 + 2w + 2) \equiv 0 \pmod{3}$$

$w = 0$ 時 $z^2 + z + 2 \equiv 0 \pmod{3}$，亦即 $(2z+1)^2 \equiv 2 \pmod{3}$。但是 2 不能開根號，因此無解。

$w = 1$ 時 $z^2 + 2z + 2 \equiv 0 \pmod{3}$，亦即 $(z+1)^2 \equiv 2 \pmod{3}$。但是 2 不能開根號，因此無解。

$w = 2$ 時 $z^2 + 2 \equiv 0 \pmod{3}$，亦即 $z^2 \equiv 1 \pmod{3}$。此時 $z = 1, 2$。推回得到 $(x, y) = (2 \cdot 1^{-1}, 1^{-1}), (2 \cdot 2^{-1}, 2^{-1}) = (2, 1), (1, 2)$。

故所有解只有 $(0, 0), (1, 2), (2, 1)$。

請你幫助小明撰寫一個程式解決上述問題吧！

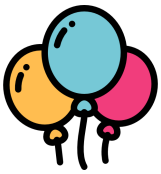
橢圓曲線小教室

以下簡述為何橢圓曲線都是三次曲線。

首先是名詞定義：

- 體：一個可以做加減乘除的結構。例如有理數、複數、文中提到的 F_p（模 p 底下的整數）。

  以下假定給定一個體 F。



- n 維射影空間（$\mathbb{FP}^n$, *projective space*）：你可以想像為 F^n 加上了每個方向的無窮遠形成的空間（注意：往上和往下視為同一個方向，因為他們平行。例如往上和往左就是不同的方向）。數學上來說，是將 $F^{n+1} - \{0\}$ 中，將相對原點同樣方向的點視為同一個點形成的集合。

  例如在 $\mathbb{RP}^2$ 中 $(1, -2, 0)$ 與 $(-2, 4, 0)$ 是同一個點。
- （射影）代數集合（*projective algebraic set*）：一些 n 元齊次（每一項的次方和相同）多項式（係數在 F 中）在 $\mathbb{FP}^n$ 中的零點（根）集合。

  例如 $\{(x, 0, 1)|x \in \mathbb{R}\} \cup \{(0, y, 1)|y \in \mathbb{R}\} \cup \{(0, 1, 0), (1, 0, 0)\}$ 就是一個在 $\mathbb{RP}^2$ 的代數集合，因為他是 $P(x, y, z) = xy = 0$ 的集合。

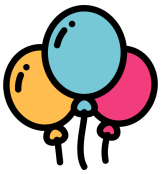
  又或著每個點 $p = (p_1, \ldots, p_{n+1}) \in \mathbb{FP}^n$ 都是一個代數集合，因為他是滿足所有 $P_{i,j}(x_1, \ldots, x_{n+1}) = p_i x_j - p_j x_i = 0$ 的集合。

  要求齊次的原因是我們定義射影空間時，要求同樣方向的點要是同一個點，因此當 $(x_1, \ldots x_{n+1})$ 是一組解時，$(kx_1, \ldots, kx_{n+1})$ 也要是一組解。
- 可約的（代數集合）（*reducible*）：可以表示成兩個代數（嚴格子）集合的聯集的代數集合。

  例如 $\{(x, 0)|x \in \mathbb{R}\} \cup \{(0, y)|y \in \mathbb{R}\}$ 是可約的，因為他可以表示成 x 軸和 y 軸的聯集。
- （射影）代數簇（*algebraic variety*）：一個不可約代數集合。
- （代數簇的）維度（dim, *dimension*）：一條遞降的代數簇鍊指的是 $X_0 \supsetneq X_1 \supsetneq \cdots \supsetneq X_n$。$n$ 稱為這條鏈的長度。一個代數簇的維度是所有從他開始的遞降的代數簇鍊中最長的那條的長度。

  直觀上來看，一個曲面包含一個曲線，一個曲線包含一個點，這條鏈的長度是 2，因此一個曲面的維度是 2。這應該跟一般對維度的想像很類似。
- 代數曲線（*algebraic curve*）：一維的代數簇。
- 奇異點（*singular point*）：比較不可微的點。嚴格來說是雅可比矩陣的零化度（*nullity*）大於代數簇的維度的點。例如自交的地方或尖點就是奇異點。
- 光滑（*smooth*, *non-singular*）：沒有奇異點的代數簇。
- 微分形式 (*differential form*)：在這裡我們只考慮一維的情形，亦即 differential 1-form。一個 differential 1-form 是一個路徑打到純量的線性函數。例如在 $\mathbb{R}^2$ 中，$\gamma \mapsto \int_\gamma \mathrm{d}x$ 是一個 differential 1-form，記為 $\mathrm{d}x$。又或者 $xy\mathrm{d}x + y^2\mathrm{d}y$ 也是一個 differential 1-form，因為他可以把 $\gamma \mapsto \int_\gamma xy\mathrm{d}x + y^2\mathrm{d}y$。

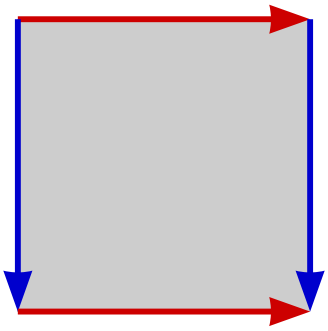
  給定局部的一個座標 $(x_1, \ldots, x_n)$，一個 1-form 長得像 $f_1(x_1, \ldots, x_n)\mathrm{d}x_1 + \ldots + f_n(x_1, \ldots, x_n)\mathrm{d}x_n$。如果每個 f_i 都是全純的，則將這個形式稱為全純形式 (*holomorphic 1-form*)。
- 虧格（*genus*）：你們可能在拓樸或哪裡聽過這個名字。基本上指的是一個表面有幾個「洞」，例如球面有零個，甜甜圈有一個。數學上來說，如果底下的體是 $\mathbb{C}$ 且 $n = \dim X$，那 $g(X) = \dim H^0(X, \Omega^n)$，亦即所有 global holomorphic n-form 形成的線性空間的維度。這可以利用 *Kähler differential* 推廣到在任何代數封閉體上面的代數簇的虧格，或是任何體上的代數曲線的虧格，變成 $g = \dim \Gamma(X, \Omega^1_X)$。
- 橢圓曲線（*elliptic curve*）：光滑、射影、虧格為 1 的代數曲線，以及其上的一個點。



於是我們終於解釋完橢圓曲線的定義了。

我們終於可以來介紹橢圓曲線了。先從最簡單的 $\mathbb{C}$ 上開始。

一個 $\mathbb{C}$ 上的橢圓曲線就是一個甜甜圈（他相對實數是二維的，但相對複數是一維的，因此是曲線），也就是把一個正方形的上緣跟下緣（A）用同樣方向黏住，左緣跟右緣（B）用同樣方向黏住，如下圖。



於是這等價於 $\mathbb{C}/\Lambda$，其中 Λ 是一個網格（$\Lambda = \mathbb{Z}w_1 + \mathbb{Z}w_2$）。這上面的 holomorphic 1-form 一定是 $f\,\mathrm{d}z$，其中 f 是 $\mathbb{C}/\Lambda$ 上的全純函數（*holomorphic function*）。但這上面的全純函數（會是有界的，根據劉維爾定理）一定是常數函數。因此所有 holomorphic 1-form 一定是常數乘上 $\mathrm{d}z$，故的確 $g = \dim H^0(X, \Omega^1) = 1$。

接著考慮這上面的亞純函數（*meromorphic function*），亦即所有全純的 $\mathbb{C}/\Lambda \to \mathbb{CP}^1$。Weierstrass 給出了一個亞純函數

$$\wp(z) = \frac{1}{z^2} + \sum_{w \in \Lambda \setminus \{0\}} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2} \right)$$

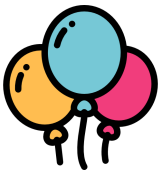
這個函數是雅可比橢圓函數的特例，而雅可比橢圓函數是橢圓積分的反函數，也因此這個函數 $\wp$ 被稱為 *Weierstrass's elliptic function*。這也是為什麼橢圓曲線叫橢圓曲線（對，歷史脈絡事實上是反過來的）。注意到 $\wp$ 在 0 有一個二階極點（pole of order 2，亦即在 0 的泰勒（其實是 Laurent）展開有一個 z^{-2} 的項）。而且 $\wp$ 是無限次可微的，而 $\wp'(z)$ 在 0 有一個三階極點。

一個曲線 X 上的除子（*(Weil) divisor*）指的是曲線上的點的形式線性組合（*formal linear combination*, i.e. free abelian group），亦即所有長得像 $\sum_{finite} a_i P_i$ 的東西，其中 P_i 是 X 上的點。

每個 X 上的函數都可以對應到一個除子，定義為

$$(f) = \sum_{P \in X} \mathrm{ord}_f(P) P$$

其中 ord 指的是 P 的泰勒（Laurent）展開的第一個非零項的次數。例如 $f : \mathbb{CP}^1 \to \mathbb{CP}^1, f(z) = z - 1/z$ 的除子就是 $(f) = 1 \cdot (-1) - 1 \cdot (0) + 1 \cdot (1) - 1 \cdot (\infty)$。另外，若一個除子的所有係數都非負，則稱這個除子為有效除子（*effective divisor*, ≥ 0），而一個除子的度數（*degree*, deg）指的是他的係數和。



給定一個除子 D，我們就可以定義他對應的一個函數的空間

$$\mathscr{L}(D) = \{f : X \to \mathbb{CP}^1 | (f) - D \geq 0\}$$

他其實就是在取所有極點不比 D 還差的函數集合。

這會是一個線性空間，因此我們可以定義他的維度 $\ell(D) = \dim \mathscr{L}(D)$。

這時 Riemann-Roch 終於出場了。定理告訴我們

$$\ell(D) - \ell(K - D) = \deg(D) - g + 1$$

其中 K 是任意一個 global holomorphic 1-form 的除子。

在 $\mathbb{C}/\Lambda$ 的情形，我們剛剛已經提到 global holomorphic 1-form 是常數函數，因此 $K = 0$。

現在考慮原點 P，我們有 $\ell(nP) - \ell(-nP) = \deg(nP) - g + 1 = n$。

如果 $n = 0$，則 $\ell(nP) = \ell(0) + n = 1$。否則 $nP > 0$，此時 $\ell(-nP) = 0$（只有 0 函數具有零點但不具極點，故 $\mathscr{L}(-nP) = \{0\}$）。因此此時 $\ell(nP) = n$。

取差分，這告訴我們只在原點恰好有一個 n 階極點的亞純函數（在縮放以後）只有一個，除了 $n = 1$ 的時候沒有（不存在 $n = 1$ 的情況也可以很直接地透過留數定理看出）。

$n = 0$ 時是 $f(z) = 1$；

$n = 2$ 時是 $\wp$；

$n = 3$ 時是 $\wp'$；

$n = 4$ 時有 $\wp^2$；

$n = 5$ 時有 $\wp\wp'$；

$n = 6$ 時有 $\wp^3, \wp'^2$，因此我們有 $\wp'^2 = a\wp^3 + c\wp\wp' + d\wp^2 + e\wp' + f\wp + g$。（事實上 $\wp'^2 = 4\wp^3 - g2\wp - g_3$）。

因此我們可以考慮一個全純映射 $f : \mathbb{C}/\Lambda \to \mathbb{CP}^2, z \mapsto (\wp(z), \wp'(z))$，他的軌跡會是一個三次曲線（想想看為什麼他會單/滿射）。

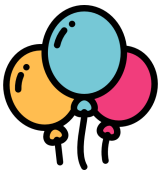
事實上任何橢圓曲線 X 都可以透過一樣的方式取一個有二階極點的函數 $x : X \to \mathbb{CP}^1, x \in \mathscr{L}(2P)$ 與有三階極點的函數 $y : X \to \mathbb{CP}^1, y \in \mathscr{L}(3P)$，並取映射 $f : X \to \mathbb{CP}^2, z \mapsto (x(z), y(z))$，他也會是一條三次曲線。

至此，我們已經（很不嚴謹的）證明所有橢圓曲線都可以被視為平面上的三次曲線。

至於 Riemann-Roch 的證明需要用到更高深的數學概念，有興趣的讀者可以自行上網尋找相關書籍與資料來閱讀。

輸入格式

每筆測資的輸入只有一行，包含用空白隔開的十個整數 $A, B, C, D, E, F, G, H, I, p$，意義如題目所示。



輸出格式

若

$$\begin{cases} Ax^3 + Bx^2y + Cxy^2 + Dy^3 + Ex^2 + Fxy + Gy^2 + Hx + Iy \equiv 0 \pmod{p} \\ 0 \le x, y < p \end{cases}$$

有 k 組解，請輸出 k 行，每行有兩個以空白隔開的整數 x, y，滿足以上的方程式。

注意解的順序必須按照 x 的大小排序。若兩組解有相同的 x，請先輸出較小 y 的那組。

測資限制

- $p \le 5 \times 10^5$。
- p 是質數。
- $0 \le A, B, C, D, E, F, G, H, I < p$。
- $A, B, C, D, E, F, G, H, I$ 至少有一個數字非 0。

輸入範例 1

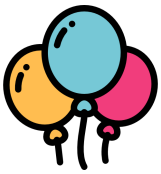
```
1 0 2 2 0 1 1 0 1 3
```

輸出範例 1

```
0 0
1 2
2 1
```

輸入範例 2

```
1 1 1 1 1 1 1 1 1 7
```



輸出範例 2

```
0 0
0 2
0 4
2 0
2 4
3 5
4 0
4 2
5 3
```

評分說明

本題共有 3 組測試題組，條件限制如下所示。每一組可有一或多筆測試資料，該組所有測試資料皆需答對才會獲得該組分數。

子任務	分數	額外輸入限制
1	7	$p = 2$。
2	22	$3 \leq p < 10^3$。
3	71	無額外限制。