Dioph. Диофантово уравнение

Имя входного файла: `dioph.in`
Имя выходного файла: `dioph.out`

Даны натуральные числа a, b и c. Решите в целых числах уравнение $ax + by = c$. Среди множества решений следует выбрать такое, где x имеет наименьшее неотрицательное значение.

Формат входного файла

Входной файл содержит три целых числа a, b, c ($1 \leqslant a, b, c \leqslant 10^4$).

Формат выходного файла

В выходной файл выведите искомые x и y через пробел. Если решения не существует, выведите одну строку «Impossible».

Пример

dioph.in	dioph.out
1 2 3	1 1
10 6 8	2 -2

Inv. Обратный элемент

Имя входного файла: `inv.in`
Имя выходного файла: `inv.out`

Обратным элементом к a в кольце вычетов по модулю m называется такой элемент x, что выполняется равенство $ax \equiv 1 \pmod m$.

Формат входного файла

Входной файл содержит два целых числа a и m ($1 \leqslant a < m \leqslant 10^9$).

Формат выходного файла

В выходной файл выведите обратный элемент к a в кольце вычетов по модулю m. Если такого элемента не существует, выведите 0.

Пример

inv.in	inv.out
2 3	2
5 25	0

Chine. Китайская теорема

Имя входного файла: `chine.in`
Имя выходного файла: `chine.out`

Решите в целых числах систему уравнений

$$\begin{cases} x \equiv a \pmod n \\ x \equiv b \pmod m, \end{cases}$$

где n и m взаимно просты. Среди решений следует выбрать наименьшее неотрицательное число.

Формат входного файла

Входной файл содержит четыре целых числа a, b, n и m ($1 \leqslant n, m \leqslant 10^6$, $0 \leqslant a < n$, $0 \leqslant b < m$).

Формат выходного файла

В выходной файл выведите искомое наименьшее неотрицательное число x.

Пример

chine.in	chine.out
1 0 2 3	3
3 2 5 9	38

RSA. Взлом RSA

Имя входного файла: `rsa.in`
Имя выходного файла: `rsa.out`

В 1977 году Ronald Linn Rivest, Adi Shamir и Leonard Adleman предложили новую криптографическую схему RSA, используемую до сих пор. RSA является криптосистемой с открытым ключом: зашифровать сообщение может кто угодно, знающий общеизвестный открытый ключ, а расшифровать сообщение — только тот, кто знает специальный секретный ключ.

Желающий использовать систему RSA для получения сообщений должен сгенерировать два простых числа p и q, вычислить $n = pq$ и сгенерировать два числа e и d такие, что $ed \equiv 1 \pmod{(p-1)(q-1)}$ (заметим, что $(p-1)(q-1) = \varphi(n)$). Числа n и e составляют открытый ключ и являются общеизвестными. Число d является секретным ключом, также необходимо хранить в тайне и разложение числа n на простые множители, так как это позволяет вычислить секретный ключ d.

Сообщениями в системе RSA являются числа из $\mathbb{Z}_n$. Пусть M — исходное сообщение. Для его шифрования вычисляется значение $C = M^e \bmod n$ (для этого необходимо только знание открытого ключа). Полученное зашифрованное сообщение C передается по каналу связи. Для его расшифровки необходимо вычислить значение $M = C^d \bmod n$, а для этого необходимо знание секретного ключа.

Вы перехватили зашифрованное сообщение C и знаете только открытый ключ: числа n и e. "Взломайте" RSA — расшифруйте сообщение на основе только этих данных.

Формат входного файла

Программа получает на вход три натуральных числа: n, e, C, $n \leqslant 10^9$, $e \leqslant 10^9$, $C < n$. Числа n и e являются частью какой-то реальной схемы RSA, т.е. n является произведением двух простых и e взаимно просто с $\varphi(n)$. Число C является результатом шифрования некоторого сообщения M.

Формат выходного файла

Выведите одно число M $(0 \leqslant M < n)$, которое было зашифровано такой криптосхемой.

Пример

rsa.in	rsa.out
143 113 41	123
9173503 3 4051753	111111

Поставленная задача ничем не отличается от реальной криптосистемы RSA, только используются существенно более длинные числа, разложение которых на простые множители, а, значит, и криптоанализ RSA, является практически невыполнимой вычислительной задачей.