

## Задача А. Обратный элемент по модулю

Имя входного файла: `inv.in`  
Имя выходного файла: `inv.out`  
Ограничение по времени: 1 секунда  
Ограничение по памяти: 64 мегабайта

Обратным элементом к  $n$  в кольце вычетов по модулю  $m$  называется такой элемент  $x$ , что выполняется равенство  $nx \equiv 1 \pmod{m}$ .

### Формат входных данных

Входной файл содержит два целых числа  $n$  и  $m$  ( $1 \leq n, m \leq 10^9$ ).

### Формат выходных данных

В выходной файл выведите обратный элемент к  $n$  в кольце вычетов по модулю  $m$ . Если этого элемента не существует, то выведите  $-1$ .

### Примеры

<code>inv.in</code>	<code>inv.out</code>
1 2	1
1 5	1
2 4	-1

## Задача В. Диофантово уравнение

Имя входного файла: dioph.in  
Имя выходного файла: dioph.out  
Ограничение по времени: 1 секунда  
Ограничение по памяти: 256 мегабайта

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 входных данных

Входной файл содержит три целых числа  $a$  и  $b$  и  $c$  ( $1 \leq a, b, c \leq 10^9$ ).

### Формат выходных данных

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

### Примеры

dioph.in	dioph.out
1 2 3	1 1

## Задача С. Китайская теорема

Имя входного файла: `chine.in`  
Имя выходного файла: `chine.out`  
Ограничение по времени: 1 секунда  
Ограничение по памяти: 64 мегабайта

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 входных данных

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

### Формат выходных данных

В выходной файл выведите искомое наименьшее неотрицательное число  $x$ .

### Примеры

<code>chine.in</code>	<code>chine.out</code>
1 0 2 3	3
3 2 5 9	38

## Задача D. Проверка на простоту

Имя входного файла: prime.in  
Имя выходного файла: prime.out  
Ограничение по времени: 1 секунда  
Ограничение по памяти: 256 мегабайт

Дано натуральное число  $N$ . Определите, является ли оно простым.

### Формат входных данных

Программа получает на вход одно целое число  $N$ ,  $2 \leq N \leq 10^{18}$ .

### Формат выходных данных

Если число  $N$  простое, программа должна вывести YES, для составного числа программа должна вывести NO.

### Примеры

prime.in	prime.out
3	YES
4	NO

## Задача Е. Разложение на множители

Имя входного файла: `factor.in`  
Имя выходного файла: `factor.out`  
Ограничение по времени: 2 секунды  
Ограничение по памяти: 256 мегабайт

Дано натуральное число  $N$ . Известно, что оно является произведением двух простых чисел. Разложите его на множители.

### Формат входных данных

Программа получает на вход одно целое число  $N$ ,  $4 \leq N \leq 10^{18}$ .

### Формат выходных данных

Программа должна вывести два простых делителя числа  $N$  в порядке неубывания.

### Примеры

<code>factor.in</code>	<code>factor.out</code>
15	3 5

## Задача F. Вычислите функции

Имя входного файла: `func.in`  
Имя выходного файла: `func.out`  
Ограничение по времени: 2 секунды  
Ограничение по памяти: 64 мегабайта

Дано число  $N$ . Требуется вычислить следующие функции для него:

$\varphi(N)$  = количество взаимно простых с  $N$  чисел среди  $1, 2, \dots, N$

$\tau(N)$  = количество делителей числа  $N$

$\sigma(N)$  = сумма всех делителей числа  $N$

### Формат входных данных

Во входном файле содержится единственное число  $1 \leq N \leq 10^9$ .

### Формат выходных данных

В единственную строку выходного файла выведите через пробел три числа — значения  $\varphi(N)$ ,  $\tau(N)$ ,  $\sigma(N)$ .

### Примеры

<code>func.in</code>	<code>func.out</code>
2	1 2 3

## Задача G. RSA. Взлом RSA

Имя входного файла: `rsa.in`  
Имя выходного файла: `rsa.out`  
Ограничение по времени: 2 секунды  
Ограничение по памяти: 64 мегабайта

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  $C = M^e \pmod n$  (для этого необходимо только знание открытого ключа). Полученное зашифрованное сообщение  $C$  передается по каналу связи. Для его расшифровки необходимо вычислить значение  $M = C^d \pmod n$ , 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 входных данных

Программа получает на вход три натуральных числа:  $n$ ,  $e$ ,  $C$ ,  $n \leq 10^9$ ,  $e \leq 10^9$ ,  $C < n$ . 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 выходных данных

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

### Примеры

<code>rsa.in</code>	<code>rsa.out</code>
143 113 41	123
9173503 3 4051753	111111

## Задача Н. Простая задача

Имя входного файла:            `prosto.in`  
Имя выходного файла:           `prosto.out`  
Ограничение по времени:       2 секунды  
Ограничение по памяти:         256 мегабайт

Найдите количество натуральных чисел на данном отрезке от  $a$  до  $b$  включительно, не делящихся нацело ни на одно из заданных различных простых чисел  $p_i$ .

### Формат входных данных

В первой строке входного файла заданы два числа  $a$  и  $b$  — границы отрезка ( $1 \leq a \leq b \leq 10^{18}$ ). Во второй строке задано количество простых чисел  $n$  ( $1 \leq n \leq 9$ ). В третьей строке перечислены сами простые числа  $p_i$ . Все числа  $p_i$  различны и не превосходят 100.

### Формат выходных данных

Ответ должен содержать единственное целое число — ответ на задачу.

### Примеры

<code>prosto.in</code>	<code>prosto.out</code>
5 10 2 2 3	2
20 40 2 3 7	12