Задача A. Решето Эратосфена за линейное время

Имя входного файла:	`стандартный ввод`
Имя выходного файла:	`стандартный вывод`
Ограничение по времени:	6 секунд
Ограничение по памяти:	1024 мегабайта

Для целого $x \geqslant 2$ обозначим $MinPrime(x)$ функцию, возвращающую наименьший простой делитель числа x. Найдите сумму $MinPrime(x)$ по всем x в пределах от L до R.

Формат входных данных

В единственной строке находятся два целых числа L и R — границы отрезка натурального ряда ($2 \leqslant L \leqslant R \leqslant 10^8$).

Формат выходных данных

Выведите одно число — искомую сумму.

Примеры

стандартный ввод	стандартный вывод
2 2	2
3 3	3
4 4	2
5 5	5
6 6	2
7 7	7
2 7	21
2 100000000	279218813374515

Задача B. Диофантово уравнение

Имя входного файла:	`stdin`
Имя выходного файла:	`stdout`
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 ($1 \leqslant a, b, c \leqslant 10^9$).

Формат выходных данных

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

Примеры

stdin	stdout
1 2 3	1 1

Задача C. Обратное по модулю

Имя входного файла:	`стандартный ввод`
Имя выходного файла:	`стандартный вывод`
Ограничение по времени:	2 секунды
Ограничение по памяти:	256 мегабайт

Даны два целых числа — a, m ($0 \leqslant a < m$). Нужно найти такое целое x, что $a \cdot x \equiv 1 \pmod{m}$.

Формат входных данных

На первой строке два целых числа — a, m ($0 \leqslant a \leqslant 10^{18}$, $1 < m \leqslant 10^{18}$, $a < m$).

Формат выходных данных

Если такого x не существует, выведите -1. Иначе выведите целое x ($0 \leqslant x < m$). Если ответов несколько, выведите любой.

Примеры

стандартный ввод	стандартный вывод
7 30	13

Задача D. Китайская теорема

Имя входного файла:	`stdin`
Имя выходного файла:	`stdout`
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 ($1 \leqslant n, m \leqslant 10^6$, $0 \leqslant a < n$, $0 \leqslant b < m$).

Формат выходных данных

В выходной файл выведите искомое наименьшее неотрицательное число x.

Примеры

stdin	stdout
1 0 2 3	3
3 2 5 9	38

Задача E. Простые сложности

Имя входного файла:	`again.in`
Имя выходного файла:	`again.out`
Ограничение по времени:	5 секунды
Ограничение по памяти:	256 мегабайта

В этой жизни не всё так просто. Особенно числа. Вам дан набор чисел. Необходимо для каждого из них определить, является ли оно простым.

Формат входных данных

В первой строке входных данных содержится единственное число $1 \leqslant T \leqslant 5\,000$ — количество чисел, которые необходимо проверить на простоту. Далее содержится T целых положительных чисел, не превосходящих 10^{18}.

Формат выходных данных

В i-й строке выходных данных должно быть записано «`YES`», если i-е число является простым, и «`NO`» в противном случае.

Примеры

again.in	again.out
2 3 4	YES NO

Задача F. Факторизация

Имя входного файла:	`pollard.in`
Имя выходного файла:	`pollard.out`
Ограничение по времени:	3 секунды
Ограничение по памяти:	256 мегабайт

Дано натуральное число. Факторизуйте его, то есть представьте в виде произведения набора простых чисел. Число p называется простым, если имеет ровно два различных натуральных делителя: 1 и p.

Формат входных данных

В единственной строке записано единственное натуральное число N. $2 \leqslant N \leqslant 9 \cdot 10^{18}$.

Формат выходных данных

Выведите в неубывающем порядке одно или несколько простых чисел, произведение которых равно N.

Примеры

pollard.in	pollard.out
6	2 3
7	7

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 $C = M^e \bmod n$ (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 входных данных

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 выходных данных

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

Примеры

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