

## Лабораторная работа 2-6. Математика

### А. Массовая проверка простоты

ограничение по времени на тест: 1.5 секунд

ограничение по памяти на тест: 256 мегабайт

ввод: стандартный ввод

вывод: стандартный вывод

Целое число  $p \geq 2$  является простым, если у него нет делителей кроме 1 и  $p$ . Необходимо для всех чисел во входном файле проверить простые они или нет.

#### Входные данные

В первой строке задано число  $n$  ( $2 \leq n \leq 500\,000$ ). В следующих  $n$  строках заданы числа  $a_i$  ( $2 \leq a_i \leq 2 \cdot 10^7$ ), которые нужно проверить на простоту

#### Выходные данные

Для каждого числа во входном файле выведите на отдельной строке «YES» или «NO» в зависимости от того, простое оно или нет.

#### Пример

входные данные	Скопировать
4 60 14 3 55	
выходные данные	Скопировать
NO NO	

YES  
NO

## В. Массовое разложение на множители

ограничение по времени на тест: 0.5 секунд  
ограничение по памяти на тест: 64 мегабайта  
ввод: стандартный ввод  
вывод: стандартный вывод

Дано много чисел. Требуется разложить их все на простые множители.

### Входные данные

В первой строке задано число  $n$  ( $2 \leq n \leq 300000$ ). В следующих  $n$  строках заданы числа  $a_i$  ( $2 \leq a_i \leq 10^6$ ), которые нужно разложить на множители.

### Выходные данные

Для каждого числа выведите в отдельной строке разложение на простые множители в порядке возрастания множителей.

### Пример

входные данные

Скопировать

4  
60  
14  
3  
55

выходные данные

Скопировать

2 2 3 5  
2 7  
3  
5 11

## С. Большая проверка на простоту

ограничение по времени на тест: 2 секунды

ограничение по памяти на тест: 64 мегабайта

ввод: стандартный ввод

вывод: стандартный вывод

Дано  $n$  натуральных чисел  $a_i$ . Определите для каждого числа, является ли оно простым.

### Входные данные

Программа получает на вход число  $n$ ,  $1 \leq n \leq 1000$  и далее  $n$  чисел  $a_i$ ,  $1 \leq a_i \leq 10^{18}$ .

### Выходные данные

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

### Пример

входные данные	Скопировать
4 1 5 10 239	
выходные данные	Скопировать
NO YES NO YES	

## D. Китайская теорема

ограничение по времени на тест: 2 секунды

ограничение по памяти на тест: 64 мегабайта

ввод: стандартный ввод

вывод: стандартный вывод

Решите в целых числах систему уравнений

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

Гарантируется, что  $n$  и  $m$  взаимно просты. Среди решений следует выбрать наименьшее неотрицательное число.

### Входные данные

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

### Выходные данные

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

### Примеры

<b>входные данные</b>	Скопировать
1 0 2 3	
<b>выходные данные</b>	Скопировать
3	

  

<b>входные данные</b>	Скопировать
3 2 5 9	
<b>выходные данные</b>	Скопировать
38	

## Е. Взлом RSA

ограничение по времени на тест: 2 секунды

ограничение по памяти на тест: 64 мегабайта

ввод: стандартный ввод

вывод: стандартный вывод

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.

### Входные данные

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  $M$ .

### Выходные данные

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

### Примеры

<b>входные данные</b>	Скопировать
143 113 41	
<b>выходные данные</b>	Скопировать
123	

  

<b>входные данные</b>	Скопировать
9173503 3 4051753	
<b>выходные данные</b>	Скопировать
111111	

## Г. Задача для второклассника

ограничение по времени на тест: 2 секунды  
ограничение по памяти на тест: 256 мегабайт

ввод: стандартный ввод  
вывод: стандартный вывод

Вам даны два числа. Необходимо найти их произведение.

### Входные данные

Входные данные состоят из двух строк, на каждой из которых находится целое одно **целое** число, длина которого не превосходит двухсот пятидесяти тысяч символов.

### Выходные данные

Выведите произведение данных чисел.

### Примеры

<b>входные данные</b>	Скопировать
2 2	
<b>выходные данные</b>	Скопировать
4	
<b>входные данные</b>	Скопировать
1 -1	
<b>выходные данные</b>	Скопировать
-1	

---

[Codeforces](#) (c) Copyright 2010-2019 Михаил Мирзаянов  
Соревнования по программированию 2.0

