y2018-4-4. Математика, криптография

A. Массовая проверка простоты

1.5 секунд, 256 мегабайт

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.

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

B. Массовое разложение на множители

2 секунды, 256 мегабайт

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.

входные данные
4 60 14 3 55
выходные данные
2 2 3 5 2 7 3 5 11

C. Большая проверка на простоту

2 секунды, 64 мегабайта

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.

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

D. Китайская теорема

2 секунды, 64 мегабайта

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.

входные данные
1 0 2 3
выходные данные
3

входные данные
3 2 5 9
выходные данные
38

E. Взлом RSA

2 секунды, 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 $\{ed \equiv 1 \pm od\{(p-1)(q-1)\}\}$ (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.

Входные данные
Программа получает на вход три натуральных числа: n, e, C, $n \le 10^9$, $e \le 10^9$, $C < n$. 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 ($0 \le M < n$), которое было зашифровано такой криптосхемой.

входные данные
143 113 41
выходные данные
123

входные данные
9173503 3 4051753
выходные данные
111111

F. Задача для второклассника

2 секунды, 256 мегабайт

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.

входные данные
2 2
выходные данные
4

входные данные
1 -1
выходные данные
-1

G. Дуэль

2 секунды, 256 мегабайт

Двое дуэлянтов решили выбрать в качестве места проведения поединка тёмную аллею. Вдоль этой аллеи растёт n деревьев и кустов. Расстояние между соседними объектами равно одному метру. Дуэль решили проводить по следующим правилам. Некоторое дерево выбирается в качестве стартовой точки. Затем два дерева, находящихся на одинаковом расстоянии от исходного, отмечаются как места для стрельбы. Дуэлянты начинают движение от стартовой точки в противоположных направлениях. Когда соперники достигают отмеченных деревьев, они разворачиваются и начинают стрелять друг в друга.

Дана схема расположения деревьев вдоль аллеи. Требуется определить количество способов выбрать стартовую точку и места для стрельбы согласно правилам дуэли.

Входные данные
Во входном файле содержится одна строка, состоящая из символов '0' и '1' — схема аллеи. Деревья обозначаются символом '1', кусты — символом '0'. Длина строки не превосходит 100000 символов.

Выходные данные
Выведите количество способов выбрать стартовую точку и места для стрельбы согласно правилам дуэли.

входные данные
101010101
выходные данные
4

входные данные
101001
выходные данные
0

В первом примере возможны следующие конфигурации дуэли (стартовое дерево и деревья для стрельбы выделены жирным шрифтом): **1**0**1**0**1**0101, 10**1**0**1**0**1**01, 1010**1**0**1**0**1** и **1**010**1**0**1**0**1**.