

у2020-4-4. Математика, криптография

А. Разложение на множители

ограничение по времени на тест: 2 секунды  
ограничение по памяти на тест: 256 мегабайт  
ввод: стандартный ввод  
вывод: стандартный вывод

Дано число. Требуется разложить его на простые множители.

Входные данные

Вводится число  $n$  ( $2 \leq n \leq 10^9$ ).

Выходные данные

Выведите через пробел разложение на простые множители в порядке неубывания множителей.

Примеры

<b>входные данные</b>	Скопировать
17	
<b>выходные данные</b>	Скопировать
17	
<b>входные данные</b>	Скопировать
60	
<b>выходные данные</b>	Скопировать
2 2 3 5	

В. Большая проверка на простоту больших чисел

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  $n$ ,  $1 \leq n \leq 5000$  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

<b>входные данные</b>	Скопировать
4 1 5 10 239	
<b>выходные данные</b>	Скопировать
NO YES NO YES	

С. 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	

D. 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  $ed \bmod (p-1)(q-1) = 1$  (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:  $n, e, C$ ,  $n \leq 10^9$ ,  $e \leq 10^9$ ,  $C < n$ . 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	

Е. Перемножение полиномов

ограничение по времени на тест: 1 секунда  
ограничение по памяти на тест: 256 мегабайт  
ввод: стандартный ввод  
вывод: стандартный вывод

Даны два полинома  $A(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$  и  $B(x) = b_0 + b_1x + b_2x^2 + \dots + b_nx^n$ . Найдите их произведение в виде  $C(x) = c_0 + c_1x + c_2x^2 + \dots + c_{2n}x^{2n}$ .

Входные данные

Первая строка содержит число  $n$  ( $1 \leq n \leq 10^5$ ). Вторая строка содержит  $n + 1$  число —  $a_0, a_1, \dots, a_n$ , третья строка содержит  $n + 1$  целое число —  $b_0, b_1, \dots, b_n$  ( $0 \leq a_i, b_i \leq 100$ ).

Выходные данные

Выведите  $2n + 1$  число —  $c_0, c_1, \dots, c_{2n}$ .

Пример

<b>входные данные</b>	Скопировать
2 1 4 2 2 5 6	
<b>выходные данные</b>	Скопировать
2 13 30 34 12	

Ф. Дуэль

ограничение по времени на тест: 2 секунды  
ограничение по памяти на тест: 256 мегабайт  
ввод: стандартный ввод  
вывод: стандартный вывод

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.

Примеры

<b>входные данные</b>	Скопировать
101010101	
<b>выходные данные</b>	Скопировать
4	
<b>входные данные</b>	Скопировать
101001	
<b>выходные данные</b>	Скопировать
0	

Примечание

В первом примере возможны следующие конфигурации дуэли (стартовое дерево и деревья для стрельбы выделены жирным шрифтом): 101010101, 101010101, 101010101 и 101010101.