# A. Разложение на множители

2 секунды, 256 мегабайт

Дано число. Требуется разложить его на простые множители.

### Входные данные
Вводится число $n$ ($2 \le n \le 10^9$).

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

| входные данные |
|---|
| 17 |
| **выходные данные** |
| 17 |

| входные данные |
|---|
| 60 |
| **выходные данные** |
| 2 2 3 5 |

# B. Большая проверка на простоту больших чисел

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 $n$, $1 \le n \le 5000$ и далее $n$ чисел $a_i$, $1 \le a_i \le 10^{18}$.

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

| входные данные |
|---|
| 4<br>1<br>5<br>10<br>239 |
| **выходные данные** |
| NO<br>YES<br>NO<br>YES |

# C. 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 $m$ ($1 \le n, m \le 10^6$, $0 \le a < n$, $0 \le b < m$).

### 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 |

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

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

| входные данные |
| --- |
| 143<br>113<br>41 |
| **выходные данные** |
| 123 |

| входные данные |
| --- |
| 9173503<br>3<br>4051753 |
| **выходные данные** |
| 111111 |

## E. Перемножение полиномов

1 секунда, 256 мегабайт

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

### Входные данные

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

### Выходные данные

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

| входные данные |
| --- |
| 2<br>1 4 2<br>2 5 6 |
| **выходные данные** |
| 2 13 30 34 12 |

## F. 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**0101010**1**.