3 - Базовая теория чисел

A. Массовое разложение на множители

1.0 с, 64 мегабайта

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

Входные данные
В первой строке задано число n ($2 \le n \le 300000$). В следующих n строках заданы числа a_i ($2 \le a_i \le 10^6$), 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

B. Просеивай!

2 секунды, 512 мегабайт

Для положительного целого n определим функции:

- $d(n)$ — минимальный делитель n, больший 1, по определению положим $d(1) = 0$.
- $s_0(n)$ — количество различных делителей n.
- $s_1(n)$ — сумма всех делителей n.
- $\varphi(n)$ — функция Эйлера, количество целых чисел k, таких что $1 \le k \le n$ и $GCD(n, k) = 1$.

По данному числу n вычислите $\sum_{k=1}^{n} d(k)$, $\sum_{k=1}^{n} s_0(k)$, $\sum_{k=1}^{n} s_1(k)$ и $\sum_{k=1}^{n} \varphi(k)$.

Входные данные
В единственной строке записано число n ($1 \le n \le 10^7$).

Выходные данные
Выведите четыре числа: $\sum_{k=1}^{n} d(k)$, $\sum_{k=1}^{n} s_0(k)$, $\sum_{k=1}^{n} s_1(k)$ и $\sum_{k=1}^{n} \varphi(k)$.

входные данные
10
выходные данные
28 27 87 32

C. 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

D. Прямая

1 second, 256 megabytes

Своим уравнением $Ax + By + C = 0$ задана прямая на плоскости. Требуется найти любую принадлежащую этой прямой точку, координаты которой — целые числа от $-5 \cdot 10^{18}$ до $5 \cdot 10^{18}$ включительно, или выяснить что таких точек нет.

Входные данные
В первой строке содержатся три целых числа A, B и C ($-2 \cdot 10^9 \le A, B, C \le 2 \cdot 10^9$) — соответствующие коэффициенты уравнения прямой. Гарантируется, что $A^2 + B^2 > 0$.

Выходные данные
Если искомая точка существует, выведите ее координаты, иначе выведите единственное число `-1`.

входные данные
2 5 3
выходные данные
6 -3

E. Китайская теорема

1 секунда, 256 мегабайт

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.

Входные данные

Первая строка входных данных содержит число N, $1 \le N \le 10^4$, — количество тестов, для которых нужно решить задачу.

Следующие N строк содержат по четыре целых числа a_i, b_i, n_i и m_i ($1 \le n_i, m_i \le 10^9$, $0 \le a_i < n_i$, $0 \le b_i < m_i$).

Выходные данные

Для каждого из тестов выведите искомое наименьшее неотрицательное число x_i.

входные данные
2 1 0 2 3 3 2 5 9
выходные данные
3 38