

4 - Продвинутая теория чисел

A. Первообразный корень по простому модулю

2 секунды, 256 мегабайт

Дано простое нечётное число p . Требуется найти минимальный первообразный корень по модулю p .

Входные данные

Первая строка входного файла содержит простое число p ($3 \leq p \leq 10^9$).

Выходные данные

Выведите ответ на поставленную задачу.

входные данные
3
выходные данные
2

входные данные
239
выходные данные
7

входные данные
127
выходные данные
3

B. Дискретное логарифмирование

3 секунды, 256 мегабайт

Даны натуральные числа a , b , и простое число n . Требуется найти дискретный логарифм b по основанию a по модулю n , то есть такое число x ($0 \leq x < n$), что $a^x \equiv b \pmod n$.

Входные данные

В первой строке заданы через пробел три целых числа a , b и n ($0 \leq a, b < n \leq 10^{12}$), Число n простое.

Выходные данные

В первой строке выведите -1 , если дискретного логарифма не существует. Иначе следует вывести его значение.

Если ответ неоднозначен, разрешается выводить любой.

входные данные
2 4 7
выходные данные
2

входные данные
41 145 239
выходные данные
116

C. Корень по модулю

4 секунды, 256 мегабайт

Даны числа a , b и m , ($1 \leq a, b < m \leq 10^9$), m — простое. Требуется найти корень степени b из a по модулю m .

Входные данные

Входной файл состоит из одного или нескольких тестов. Количество тестов $T \leq 300$ задано в первой строке.

В T последующих строках заданы по три числа в каждой — a , b и m .

Выходные данные

Для каждого из тестов выведите какой-либо из корней степени b из a по модулю m , либо -1 , если искомого корня не существует. Выводимое число должно быть в пределах от -1 до $m - 1$.

входные данные
2 4 3 5 1 3 7
выходные данные
4 1

D. Проверка на простоту

1 секунда, 256 мегабайт

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

E. Факторизация

3 секунды, 256 мегабайт

Дано натуральное число. Факторизуйте его, то есть представьте в виде произведения набора простых чисел. Число p называется простым, если имеет ровно два различных натуральных делителя: 1 и p .

Входные данные

В единственной строке записано единственное натуральное число N . $2 \leq N \leq 9 \cdot 10^{18}$.

Выходные данные

Выведите в неубывающем порядке одно или несколько простых чисел, произведение которых равно N .

входные данные
6
выходные данные
2 3

входные данные
7

выходные данные
7

[Codeforces](#) (c) Copyright 2010-2020 Михаил Мирзаянов
Соревнования по программированию 2.0