

Разложение чисел на множители

Шевляков Илья Николаевич НФИмд-01-21

24 декабря, 2021, Москва, Россия

Российский Университет Дружбы Народов

Цели и задачи

Цель лабораторной работы

Изучение задачи дискретного логарифмирования.

Выполнение лабораторной работы

Задача дискретного логарифмирования

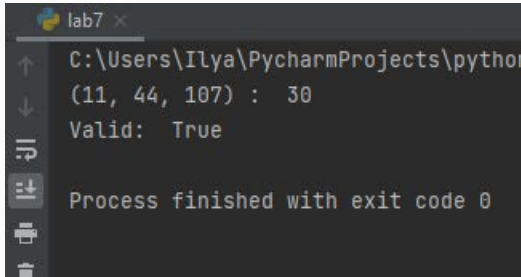
Решение задачи дискретного логарифмирования состоит в нахождении некоторого целого неотрицательного числа x , удовлетворяющего уравнению. Если оно разрешимо, у него должно быть хотя бы одно натуральное решение, не превышающее порядок группы.

р-алгоритм Поллрада

- Вход. Простое число p , число a порядка r по модулю p , целое число b $1 < b < p$; отображение f , обладающее сжимающими свойствами и сохраняющее вычислимость логарифма.
 - Выход. показатель x , для которого $a^x = b \pmod{p}$, если такой показатель существует.
1. Выбрать произвольные целые числа u, v и положить $c = a^u \pmod{p}$, $d = c$
 2. Выполнять условия, вычисляя при этом логарифмы для c и d как линейные функции от x по модулю r , до получения равенства $c = d \pmod{p}$
 3. Приняв логарифмы для c и d , вычислить логарифм x решением сравнения по модулю r . Результат x или РЕШЕНИЯ НЕТ.

Алгоритм полного перебора нашёл бы решение за число шагов не выше порядка данной группы.

Пример работы алгоритма



The image shows a terminal window titled 'lab7' with a Python icon. The terminal output is as follows:

```
C:\Users\Ilya\PycharmProjects\python  
(11, 44, 107) : 30  
Valid: True  
  
Process finished with exit code 0
```

On the left side of the terminal, there is a vertical toolbar with icons for navigating between files, running the program, and other development actions.

Figure 1: Работа алгоритма

Выводы

Изучили задачу дискретного логарифмирования.