

Разложение чисел на множители

Драммех Мариама

7 ноября, 2024, Москва, Россия

Российский Университет Дружбы Народов

Цели и задачи

Цель лабораторной работы

Изучение задачи разложения на множители, изучение p -алгоритма Поллрада.

Выполнение лабораторной работы

Задача разложения на простые множители

Разложение на множители — предмет непрерывного исследования в прошлом; и такие же исследования, вероятно, продолжатся в будущем. Разложение на множители играет очень важную роль в безопасности некоторых криптосистем с открытым ключом.

р-алгоритм Поллрада

- Вход. Число n , начальное значение c , функция f , обладающая сжимающими свойствами.
 - Выход. Нетривиальный делитель числа n .
1. Положить $a = c, b = c$
 2. Вычислить $a = f(a)(\text{mod } n), b = f(b)(\text{mod } n)$
 3. Найти $d = \text{GCD}(a - b, n)$
 4. Если $1 < d < n$, то положить $p = d$ и результат: p . При $d = n$ результат: ДЕЛИТЕЛЬ НЕ НАЙДЕН. При $d = 1$ вернуться на шаг 2.

Сложность. Заметим, что этот метод требует сделать $B-1$ операций возведения в степень $a = a^e \bmod n$. Есть быстрый алгоритм возведения в степень, который выполняет это за $2 * \log_2 B$ операций. Метод также использует вычисления НОД, который требует n^3 операций. Мы можем сказать, что сложность — так или иначе больше, чем $O(B)$ или $O(2^n)$, где n_b — число битов в B . Другая проблема — этот алгоритм может заканчиваться сигналом об ошибке. Вероятность успеха очень мала, если B имеет значение, не очень близкое к величине \sqrt{n} .

Пример работы алгоритма

```
In [1]: 1 from math import gcd
2
3 def f(x, n):
4     return (x*x+5)%n
5
6 def fu(n, a, b, d):
7     a = f(a, n)
8     b = f(f(b, n), n)
9     d = gcd(a-b, n)
10    if 1<d<n:
11        print(d)
12        exit()
13    if d == n:
14        print("not found")
15    if d == 1:
16        fu(n, a, b, d)
17
18 def main():
19     n = 1359331
20     c = 1
21     a = f(c, n)
22     b = f(a, n)
23     d = gcd(a-b, n)
24     if 1< d < n:
25         print(d)
26         exit()
27     if d == n:
28         pass
29     if d == 1:
30         fu(n, a, b, d)
```

```
In [2]: 1 main()
```


Выводы

Изучили задачу разложения на множители и р-алгоритм Поллрада.