

# Разложение чисел на множители

---

Нкуранга Джуниор НФИмд 02-21

28 января, 2022, 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

```
24
25 def main():
26     n = 1359331
27     c = 1
28     a = c
29     b = c
30     a = f(a, n) % n
31     b = f(a,n) % n
32     d = gcd(a-b, n)
33     if 1<d<n:
34         p = d
35         print(p)
36         exit()
37     if d == n:
38         pass
39     if d == 1:
40         fu(n, a, b, d)
```

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

```
1181
```

**Figure 1:** Работа алгоритма



## **Выводы**

---

Изучили задачу разложения на множители и р-алгоритм Поллрада.