



# **ИНСТИТУТ ИНТЕЛЛЕКТУАЛЬНЫХ КИБЕРНЕТИЧЕСКИХ СИСТЕМ**

**Кафедра  
«Криптология и кибербезопасность»**

---

## **ОТЧЕТ о лабораторной работе №3**

Выполнил студент  
группы Б20-505  
Соколов Александр Дмитриевич

---

**Москва – 2023**

---

## Лабораторная работа №3 Факторизация

### Разложить числа методом Ферма

Дано число  $n = p * q$ , где  $p$  и  $q$  - простые числа. Причем разность  $|p - q|$  не очень большая.

Допустим  $p > q$

#### Алгоритм

Пусть существуют такие два числа  $u$  и  $v$ , что  $n = u^2 - v^2$ . Тогда:

$$p * q = u^2 - v^2 = (u - v) * (u + v)$$

Возможны два случая:

- $p = u + v, q = u - v$
- $u - v = 1, u + v = n$ . Этот случай нам не подходит, однако он возможен только в случае, когда  $v = \frac{n-1}{2}$ , но в первом случае  $v = \frac{p-q}{2} < \frac{n-1}{2}$ . Таким образом до этого случая мы просто не дойдем по ходу работы программы.

Начиная с числа  $v = 1$  увеличиваем  $v$  до тех пор, пока  $n + v^2$  не станет квадратом целого числа.

#### Проверка числа на “квадратность”

Пусть у нас есть простое число  $p$ . Рассмотрим группу чисел по модулю  $p$ .

$$0, 1, 2, 3, 4, 5, \dots, \frac{p-1}{2}, \frac{p+1}{2} = p - \frac{p-1}{2}, \dots, p - 5, p - 4, p - 3, p - 2, p - 1$$

Пусть у нас есть два числа  $x, y$ , такие что:

$$x^2 = b(mod\ p)$$

$$y^2 = b(mod\ p)$$

Тогда

$$x^2 - y^2 = (x - y) * (x + y) = 0(mod\ p)$$

Так как  $p$  - простое, то либо

$$x = y(mod\ p)$$

либо

$$x = -y(mod\ p)$$

Таким образом квадратов по модулю  $p$ :  $\frac{p-1}{2} + 1$  (Учитывая 0);

Чтобы проверить, что число является квадратом по модулю простого числа  $p$  можно воспользоваться символом Лежандра, который в случае простого числа вычисляется следующим образом:

$$x = \left(\frac{b}{p}\right) = b^{\frac{p-1}{2}} \pmod{p}$$

Если  $x = 1$ , то число  $a$  - квадрат по модулю  $p$ .

Если  $x = p - 1$ , то число  $a$  - не является квадратом.

Если  $x = 0$ , то число  $a$  - делится на  $p$ .

Пусть у нас есть число  $b = a^2$  в целых числах. Тогда оно так же будет являться квадратом по модулю  $p$ .

Вероятность того, что случайное число является квадратом по модулю  $p$  примерно 0.5. Если проверить его таким способом для  $m$  простых чисел, получим вероятность ошибки работы алгоритма  $\frac{1}{2^m}$ .

### База простых чисел

Я использовал первые 45 простых чисел

3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73

79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157

163, 167, 173, 179, 181, 191, 193, 197, 199

### Результаты счета для заданных чисел

Вариант 10:

$$n_1 = 240316062981161$$

$$u = 15502131$$

$$v = 1600$$

$$p = 15503731$$

$$q = 15500531$$

---


$$n_2 = 240317584752391$$

$$u = 15502180$$

$$v = 3$$

$$p = 15502183$$

$$q = 15502177$$

## Разложить числа ро-методом Полларда

### Алгоритм

Пусть у нас есть функция  $f : Z_n \rightarrow Z_n$  и последовательность  $x_1 \rightarrow f(x_1) \rightarrow f(f(x_1)) \rightarrow \dots \rightarrow f^m(x)$

Вероятность того, что все числа в этой последовательности разные:

$$P = \frac{n}{n} * \frac{n-1}{n} * \frac{n-2}{n} * \dots * \frac{n-m+1}{n} = (1 - \frac{1}{n}) * (1 - \frac{2}{n}) * \dots * (1 - \frac{m-1}{n}) \approx e^{-\frac{1}{n} * \sum_{i=1}^{m-1} i} = e^{-\frac{m*(m-1)}{2*n}} \approx e^{-\frac{m^2}{2*n}}$$

Тогда при  $m \approx \lambda * \sqrt{n}$ ,  $\lambda \geq 1$  вероятность будет  $P \approx e^{-\frac{\lambda^2}{2}}$

И вероятность того, что будет хотя бы одно повторение:

$$P' = 1 - P \approx 1 - e^{-\frac{\lambda^2}{2}}$$

### Многочлены

Пусть  $f(x) = Poly(x)(mod n)$

Тогда, если  $f(x_i) = f(x_j)$ , тогда  $x_{i+1} = x_{j+1}$ , а также все  $x_{i+1+k} = x_{j+1+k}$

Линейный случай нам не подходит, так как в его случае период  $f$  будет  $p$ .

Я использовал многочлен  $f(x) = x^2 + 7(mod n)$

### Факторизация

Так как мы ищем множители числа  $n$  и функция задана по модулю  $n$ , тогда функция будет работать и по модулю  $q$ , а следовательно вероятность того, что получится найти два одинаковых числа в последовательности длины  $m$  по модулю  $q$ :

$$P \approx 1 - e^{-\frac{m^2}{2*p}}, \text{ а если период } f \text{ меньше } p \text{ то еще больше.}$$

Таким образом мы начинаем со случайного числа  $x_1, y_1 = x_1$

Затем последовательно считаем два новых числа:

$$x_i = f(x_{i-1})$$

$$y_i = f(f(y_{i-1}))$$

И считаем  $gcd(y_i - x_i, n)$  пока он не перестанет быть 1.

### Результаты счета для заданных чисел n

Вариант 10

$$n_1 = 22122335181319$$

$$q = 1427047 \ p = 15502177$$

$$\text{длина} = 2401$$

---

$$n_2 = 22341667061281$$

$$q = 1441051$$

$$p = 15503731$$

$$\text{длина} = 837$$