Факторизация методом квадратичного решета

ИУ8-115
Леус А.А.
Лобусов И.С
Романчук Ю.В

Алгоритм

Шаг 1

$$L = e^{\sqrt{\ln(N) ln(ln(N))}}$$

$$B \approx L^{\frac{1}{\sqrt{2}}}$$

$N = 87463$, we calculate $B \approx 42$

Шаг 2

$$F(T) = T^2 - N$$

We start with a T which is $ceil(\sqrt{N})$

$$F(a) = 296^2 - N = 153, F(a+1) = 297^2 - N = 746, F(a+2) = 298^2 - N = 1341$$

$LS = \{153, 746, 1341, 1938, 2537, 3138, 3741, \ldots.\}$

$\sqrt{87463} = 295.74$. So we start with a = 296.

Шаг 3. Факторная база

{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41 ,43}

If $N^{\frac{p-1}{2}} \mod p \neq 1$, then N is not a QR for that odd prime

$FB = \{2, 3, 13, 17, 19, 29, 41, 43\}$

Шаг 4. Разложение LS по FB

$LS = 153, 746, 1341, 1938, 2537, 3138, 3741, \ldots .$

$FB = \{2, 3, 13, 17, 19, 29, 41, 43\}$

$153 = 3^2 \text{ x } 17$

$F(a) = 296^2 - N = 153$

1. $296^2 \mod 87463 \equiv 153$ and $153 = 3^2 \text{ x } 17$
2. $299^2 \mod 87463 \equiv 1938$ and $1938 = 2 \text{ x } 3 \text{ x } 17 \text{ x } 19$
3. $302^2 \mod 87463 \equiv 3741$ and $3741 = 3 \text{ x } 29 \text{ x } 43$
4. $307^2 \mod 87463 \equiv 6786$ and $6786 = 2 \text{ x } 3^2 \text{ x } 13 \text{ x } 29$
5. $316^2 \mod 87463 \equiv 12393$ and $12393 = 3^6 \text{ x } 17$
6. $343^2 \mod 87463 \equiv 30186$ and $30186 = 2 \text{ x } 3^3 \text{ x } 13 \text{ x } 43$
7. $347^2 \mod 87463 \equiv 32946$ and $32946 = 2 \text{ x } 3 \text{ x } 17^2 \text{ x } 19$

Шаг 5. Построение матрицы

$$6786 = 2 \times 3^2 \times 13 \times 29$$

$$6786 = 2^1 \times 3^2 \times 13^1 \times 17^0 \times 19^0 \times 21^0 \times 29^1$$

$$v(6786) = \{1\ 2\ 1\ 0\ 0\ 0\ 1\ 0\ 0\}$$

$$A^T = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Шаг 6. Поиск ядра матрицы

```
sage: R = Zmod(2)
sage: A = matrix(R, [
....: [0, 0, 0, 1, 0, 0, 0, 0, 0],
....: [1, 1, 0, 1, 1, 0, 0, 0, 0],
....: [0, 1, 0, 0, 0, 0, 1, 0, 1],
....: [1, 0, 1, 0, 0, 0, 1, 0, 0],
....: [0, 0, 0, 1, 0, 0, 0, 0, 0],
....: [1, 1, 1, 0, 0, 0, 0, 0, 1],
....: [1, 1, 0, 0, 1, 0, 0, 0, 0]])
sage: A.kernel()
Vector space of degree 7 and dimension 3 over Ring of integers modulo 2
Basis matrix:
[1 0 0 0 1 0 0]
[0 1 0 0 1 0 1]
[0 0 1 1 0 1 0]
```

Шаг 7.

$v1 = [1\,0\,0\,0\,1\,0\,0]$ (i.e. multiply the squares of 1st & 5th Number to get a Zero exponent vector - $296^2 \times 316^2$)

$$296^2 \times 316^2 \equiv (3^2 \times 17)(3^6 \times 17) \bmod 87463$$

$$= (3^4 \quad X \quad 17)^2$$

$$gcd(N, (296 \times 316) - (3^4 \times 17)) = 587$$

$$87463 = 587 \times 149$$

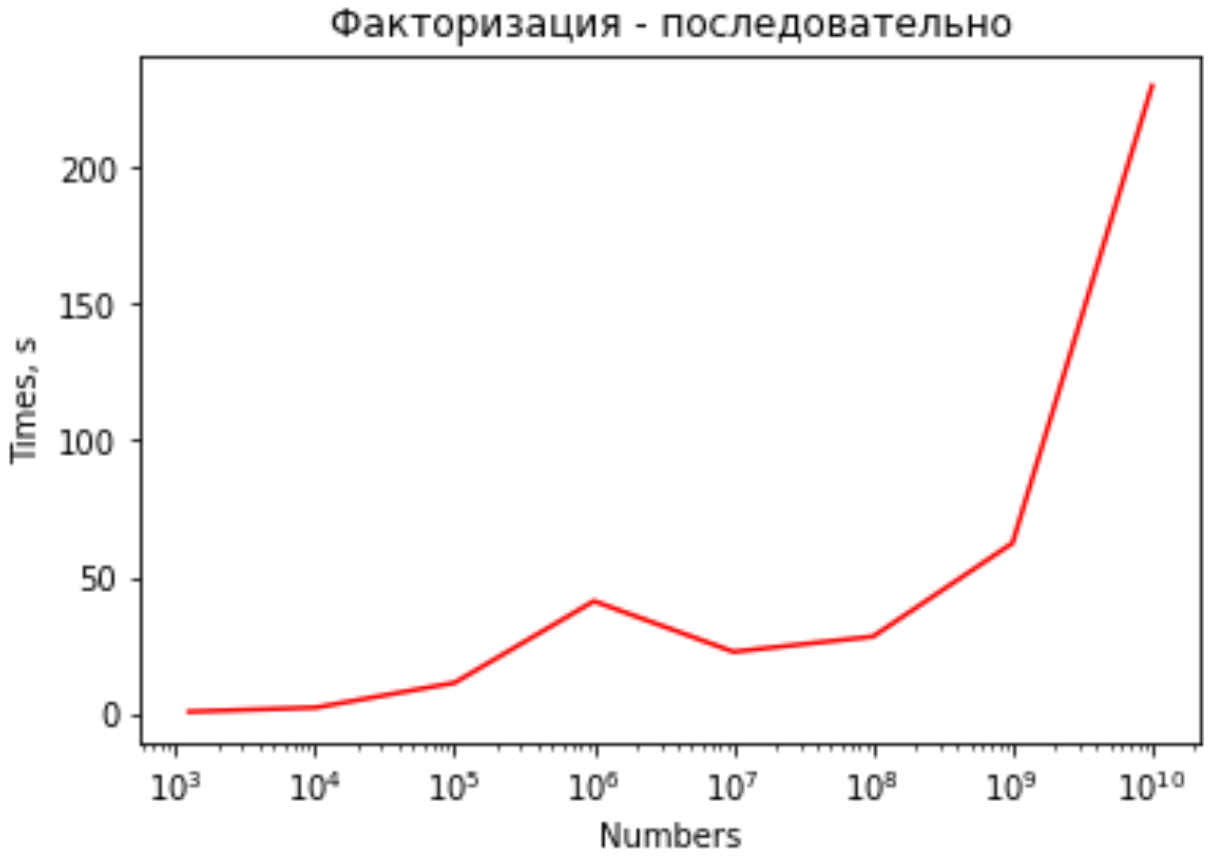
1. $296^2 \bmod 87463$
2. $299^2 \bmod 87463$
3. $302^2 \bmod 87463$
4. $307^2 \bmod 87463$
5. $316^2 \bmod 87463$
6. $343^2 \bmod 87463$
7. $347^2 \bmod 87463$

Параллельная реализация

- Вычисление LS
- Сокращение факторной базы
- Разложение LS по FB
- Вычисление ядра

Результаты

n = 1251 = 3 * 417
n = 10173 = 3 * 3391
n = 100247 = 7 * 14321
n = 1000225 = 5 * 200045
n = 10000188 = 4 * 2500047
n = 100000185 = 3 * 33333395
n = 1000000179 = 3 * 333333393
n = 10000000177 = 1787 * 5595971



n = 1251 = 9 * 139
n = 10173 = 3 * 3391
n = 100247 = 7 * 14321
n = 1000225 = 25 * 40009
n = 10000188 = 3 * 3333396
n = 100000185 = 3 * 33333395
n = 1000000179 = 3 * 333333393
n = 10000000177 = 1787 * 5595971