

Разложение чисел на множители

Лабораторная работа №6

Данилова А.С.

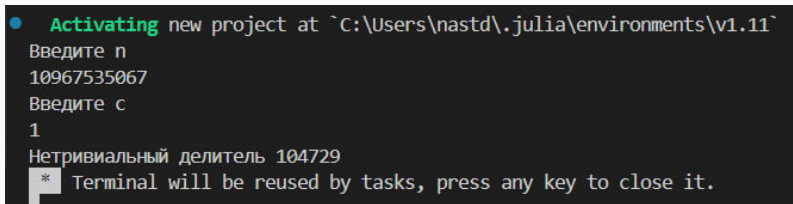
- Изучить теоретическую часть об алгоритме, который реализует метод Полларда;
- Изучить метод разложения квадратов на множители(теорема Ферма о разложении);
- Реализовать оба метода программно.

Po-алгоритм — предложенный Джоном Поллардом в 1975 году алгоритм, служащий для факторизации (разложения на множители) целых чисел. Алгоритм наиболее эффективен при факторизации составных чисел с достаточно малыми множителями в разложении.

Метод квадратов, связанный с теоремой Ферма о разложении, представляет собой эффективный способ работы с целыми числами и обнаружения свойств связи между делителями и квадратами чисел. Для каждого нечетного числа мы можем найти пары (s, t) , которые позволяют записать число как разность квадратов двух других целых чисел.

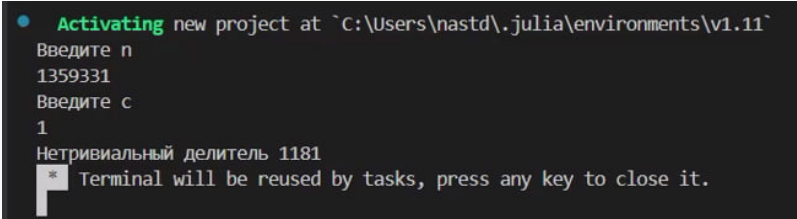
```
1  using Random
2  function pollard(n, c)
3      f(x) = (x^2 + 5) % n
4
5      a = c
6      b = c
7      d = 1
8
9      while d == 1
10         a = f(a) % n
11         b = f(f(b)) % n
12         d = gcd(abs(a - b), n)
13
14         if d == n
15             return "Делитель не найден"
16         end
17     end
18     return d
19 end
20 println("Введите n")
21 n = parse{Int, readline()}
22 println("Введите c")
23 c = parse{Int, readline()}
24
25 result = pollard(n, c)
26 println("Нетривиальный делитель ", result)
```

Рис. 1: Р-метод Полларда



```
● Activating new project at `C:\Users\nastd\.julia\environments\v1.11`  
Введите n  
10967535067  
Введите c  
1  
Нетривиальный делитель 104729  
* Terminal will be reused by tasks, press any key to close it.
```

Рис. 2: Результат



```
• Activating new project at `C:\Users\nastd\.julia\environments\v1.11`  
Введите n  
1359331  
Введите c  
1  
Нетривиальный делитель 1181  
* Terminal will be reused by tasks, press any key to close it.
```

Рис. 3: Результат

```
1 function square_method(n)
2     divisors = []
3     sqrt_n = floor(Int, sqrt(n))
4
5     for i in 1:sqrt_n
6         if n % i == 0
7             push!(divisors, (i, n / i))
8         end
9     end
10    return divisors
11 end
12
13 println("Введите число n")
14 n = parse{Int, readline()}
15 divisors = square_method(n)
16
17 for (p, q) in divisors
18     s = (p + q) / 2
19     t = (q - p) / 2
20
21     if (p + q) % 2 == 0 && (q - p) % 2 == 0
22         println("$n = $p * $q, откуда s = $s, t = $t и n = $s^2 - $t^2")
23     end
24 end
```

Рис. 4: Метод квадратов


```
● Activating new project at `C:\Users\nastd\.julia\environments\v1.11`  
Введите число n (целое положительное):  
15  
15 = 1 * 15, откуда s = 8, t = 7 и 15 = 8^2 - 7^2  
15 = 3 * 5, откуда s = 4, t = 1 и 15 = 4^2 - 1^2  
* Terminal will be reused by tasks, press any key to close it.
```

Рис. 5: Результат

Мы изучили методы разложения чисел на множители и реализовали их программно на языке программирования Julia.