Лабораторная работа №6

Математические основы защиты информации и информационной безопасности

Данилова Анастасия Сергеевна

Содержание

Цель работы

Изучить методы разложения чисел на множители и реализовать их программно на языке программмирования Julia.

Задание

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

Теоретическое введение

Р-метод Полларда

Ро-алгоритм — предложенный Джоном Поллардом в 1975 году алгоритм, служащий для факторизации (разложения на множители) целых чисел. Данный алгоритм основывается на алгоритме Флойда поиска длины цикла в последовательности и некоторых следствиях из парадокса дней рождения. Алгоритм наиболее эффективен при факторизации составных чисел с достаточно малыми множителями в разложении.

Метод Квадратов(теорема Ферма о 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. Это понимание имеет широкие применения в различных теоретических и практических аспектах математического анализа.

Для каждого нечетного числа мы можем найти пары (s, t), которые позволяют записать число как разность квадратов двух других целых чисел. Метод квадратов показывают, что существуют различные способы представления каждого положительного нечетного числа в виде разности квадратов, что делает этот метод полезным в различных задачах теории чисел.

Выполнение лабораторной работы

```
using Random
function pollard(n, c)
    f(x) = (x^2 + 5) % n

    a = c
    b = c
    d = 1

    while d == 1
        a = f(a) % n
        b = f(f(b)) % n
        d = gcd(abs(a - b), n)

        if d == n
            return "Делитель не найден"
        end
    end
    return d
end
println("Введите n")
n = parse(Int, readline())
println("Введите c")
c = parse(Int, readline())

result = pollard(n, c)
println("Нетривиальный делитель ", result)
```

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.
```

Результат 1

```
  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.
```

Результат 2

```julia
function square_method(n)
    divisors = []
    sqrt_n = floor(Int, sqrt(n))

    for i in 1:sqrt_n
        if n % i == 0
            push!(divisors, (i, n / i))
        end
    end
    return divisors
end

println("Введите число n")
n = parse(Int, readline())
divisors = square_method(n)

for (p, q) in divisors
    s = (p + q) / 2
    t = (q - p) / 2

    if (p + q) % 2 == 0 && (q - p) % 2 == 0
        println("$n = $p * $q, откуда s = $s, t = $t и n = $s^2 - $t^2")
    end
end
```

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.
```

Результат

Выводы

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

Список литературы

1. Mathematics // Julia URL: https://docs.julialang.org/en/v1/base/math/