Цель работы

Основной целью работы является реализовать алгоритм разложение чисел на множители.

Выполнение лабораторной работы

Алгоритм, реализующий p-метод Полларда

[17]:
```
using Printf
function fermat_factor(n::Int)
    if n % 2 == 0
        return (2, n ÷ 2)
    end
    x = ceil(Int, sqrt(n))
    y2 = x*x - n
    while true
        y = isqrt(y2)
        if y*y == y2
            return (x - y, x + y)
        end
        x += 1
        y2 = x*x - n
    end
end
n = 1359331
p, q = fermat_factor(n)
@printf("Факторизация числа %d методом Ферма: %d x %d\n", n, p, q)
```

```
Факторизация числа 1359331 методом Ферма: 1151 x 1181
```

Разложение на множители число

[15]:
```
using Random
function pollard_rho(n::Int; c::Int=1, max_iter::Int=10^6)
    if n % 2 == 0
        return 2
    end
    f(x) = (x * x + c) % n
    x, y, d = 2, 2, 1
    for _ in 1:max_iter
        x = f(x)
        y = f(f(y))
        d = gcd(abs(x - y), n)
        if d == n
            return n  # неудача, стоит попробовать другое c
        elseif d > 1
            return d  # найден делитель
        end
    end
    return n  # ничего не нашли в пределах max_iter
end
n = 456
println("Факторизация $n при помощи Pollard's Rho:")
d = pollard_rho(n, c=1)
if d != n
    println("Найден делитель d = $d, второй = $(n ÷ d)")
else
    println("Не удалось найти делитель, попробуйте другой c")
end
```

```
Факторизация 456 при помощи Pollard's Rho:
Найден делитель d = 2, второй = 228
```

Вывод

В ходе выполнения лабораторной работы был реализован алгоритм разложение чисел на множители.