Лабораторная работа №6

Разложение чисел на множители

Выполнила:

Манаева Варвара Евгеньевна, НФИмд-01-24, 1132249514

Для проверки будем использовать число 221

1. Алгоритм, реализующий p-метод Полларда

In [1]:
```
function evklidBin(a, b)
    if a == 0 || b == 0
        return 0
    elseif a == b
        return a
    elseif a < 0
        a *= -1
    elseif b < 0
        b *= -1
    end
    g = 1
    u = a; v = b
    while u > 0
        if u % 2 == 0 && v % 2 == 0
            g *= 2
            u = round(Int, u/2)
            v = round(Int, v/2)
        elseif u % 2 == 0
            u = round(Int, u/2)
        elseif v % 2 == 0
            v = round(Int, v/2)
        elseif u >= v
            u = u - v
        else
            v = v - u
        end
    end
    g *= v
    return g
end
```

Out[1]:
```
evklidBin (generic function with 1 method)
```

In [8]:
```
function metodPollarda(n, c, any_func::Function)
    if n % 2 == 0
        return 2, round(Int, n/2)
    end
    a = c; b = c
    i = 0
```

```
    p = 0
    while p == 0 && i < 100
        a = any_func(a)
        b = any_func(any_func(b))
        d = evklidBin(a-b, n)
        if d > 1
            return d, round(Int, n/d)
        end
        i += 1
    end
    return "Делитель не найден"
end
```

Out[8]: metodPollarda (generic function with 1 method)

In [3]:
```
n = 1359331
c = 1
metodPollarda(n, c, x -> (x^2 + 5) % n)
```

```
6       41      1
41      123939  1
1686    391594  1
123939  438157  1
435426  582738  1
391594  1144026 1
1090062 885749  1181
```

Out[3]: (1181, 1151)

In [9]:
```
n = 135956347
c = 1
metodPollarda(n, c, x -> (x^2 + 13) % n)
```

Out[9]: (5591, 24317)