

# Лабораторная работа №6

## Разложение чисел на множители

Кузнецов Юрий Владимирович

# Содержание I

- 1 Введение
- 2 Метод Полларда
- 3 Заключение

# Section 1

## Введение

# Введение

В данной презентации будет представлена реализация разложения чисел на множители

# Основные темы

- Метод Полларда

## Section 2

# Метод Полларда

# Метод Полларда

```
1 function binary_gcd(x, y)
2   if x == 0
3     return 0
4   end
5
6   x = abs(x)
7   y = abs(y)
8
9   if x == y
10    return x
11  end
12
13  multiplier = 1
14
15  while x > 0
16    if x % 2 == 0 && y % 2 == 0
17      multiplier *= 2
18      x = x / 2
19      y = y / 2
20    elseif x % 2 == 0
21      x = x / 2
22    elseif y % 2 == 0
23      y = y / 2
24    elseif x > y
25      x = x - y
26    else
27      y = y - x
28    end
29  end
30
31  return multiplier * y
32 end
33
34 function pollard_factorization(number, seed, transformation::Function)
35   if number % 2 == 0
36     return 2, number / 2
37   end
38
39   value1 = seed
40   value2 = seed
41   iteration = 0
42   factor = 0
43
44   while factor == 0 && iteration < 100
45     value1 = transformation(value1)
46     value2 = transformation(transformation(value2))
47     gcd = binary_gcd(value1 - value2, number)
48
49     if gcd > 1
50       return gcd, number / gcd
51     end
52     iteration += 1
53   end
54
55   return "No factor found"
56 end
57
58 num1 = 12345623
59 seed1 = 1
```

## Section 3

Заключение



# Заключение

В ходе выполнения лабораторной работы, было изучено и запрограммировано разложение чисел на множители