ЛАБОРАТОРНАЯ РАБОТА №6

Разложение чисел на множители

Кузнецов Юрий Владимирович

# Введение

В данном отчёте будет представлена реализация разложения чисел на множители

# Основное содержание

## Разложение чисел на множители

* Метод Полларда

# Кодовая реализация

## Метод Полларда

function binary\_gcd(x, y)  
 if x == 0  
 return 0  
 end  
  
 x = abs(x)  
 y = abs(y)  
  
 if x == y  
 return x  
 end  
  
 multiplier = 1  
  
 while x > 0  
 if x % 2 == 0 && y % 2 == 0  
 multiplier \*= 2  
 x ÷= 2  
 y ÷= 2  
 elseif x % 2 == 0  
 x ÷= 2  
 elseif y % 2 == 0  
 y ÷= 2  
 elseif x >= y  
 x -= y  
 else  
 y -= x  
 end  
 end  
  
 return multiplier \* y  
end

## Метод Полларда

function pollard\_factorization(number, seed, transformation::Function)  
 if number % 2 == 0  
 return 2, number ÷ 2  
 end  
  
 value1 = seed  
 value2 = seed  
 iteration = 0  
 factor = 0  
  
 while factor == 0 && iteration < 100  
 value1 = transformation(value1)  
 value2 = transformation(transformation(value2))  
 gcd = binary\_gcd(value1 - value2, number)  
  
 if gcd > 1  
 return gcd, number ÷ gcd  
 end  
 iteration += 1  
 end  
  
 return "No factor found"  
end  
  
num1 = 12342523  
seed1 = 1  
println(pollard\_factorization(num1, seed1, x -> (x^2 + 5) % num1))  
  
num2 = 1432432  
seed2 = 1  
println(pollard\_factorization(num2, seed2, x -> (x^2 + 13) % num2))

# Заключение

В данной лабораторной работе представлена реализация разложения чисел на множители