ЛАБОРАТОРНАЯ РАБОТА №7

Дискретное логарифмирование в конечном поле

Кузнецов Юрий Владимирович

# Введение

В данном отчёте будет представлена реализация дискретного логарифмирования в конечном поле

# Основное содержание

## Основной метод

* р-метод Полларда для задач дискретного логарифмирования

# Кодовая реализация

## Метод Полларда

function find\_gamma(a\_diff, b\_diff, prime\_modulus)  
 for gamma in 1:prime\_modulus  
 if (b\_diff \* gamma) % prime\_modulus == a\_diff  
 return gamma  
 end  
 end  
end  
  
function update\_xab(x, a, b, prime\_modulus, alpha, beta)  
 if x % 3 == 0  
 return mod(x^2, prime\_modulus), mod(a \* 2, prime\_modulus - 1), mod(b \* 2, prime\_modulus - 1)  
 elseif x % 3 == 1  
 return mod(x \* alpha, prime\_modulus), mod(a + 1, prime\_modulus - 1), b  
 else  
 return mod(x \* beta, prime\_modulus), a, mod(b + 1, prime\_modulus - 1)  
 end  
end  
  
function pollard\_rho\_log(prime\_modulus, alpha, beta)  
 if prime\_modulus % 2 == 0  
 return "Invalid"  
 end

## Метод Полларда

a1, b1, x1 = 0, 0, 1  
 a2, b2, x2 = 0, 0, 1  
 iteration\_limit = 1000  
  
  
 trace1 = zeros(Int64, 3, iteration\_limit)  
 trace2 = zeros(Int64, 3, iteration\_limit)  
  
 for iteration in 1:iteration\_limit  
  
 x1, a1, b1 = update\_xab(x1, a1, b1, prime\_modulus, alpha, beta)  
 trace1[:, iteration] = [x1, a1, b1]  
  
  
 x2, a2, b2 = update\_xab(x2, a2, b2, prime\_modulus, alpha, beta)  
 x2, a2, b2 = update\_xab(x2, a2, b2, prime\_modulus, alpha, beta)  
 trace2[:, iteration] = [x2, a2, b2]  
  
 if x1 == x2  
 display(trace1[:, 1:iteration])  
 display(trace2[:, 1:iteration])  
  
 diff\_b = b2 - b1  
 if diff\_b == 0  
 return "Not found"  
 else  
 return find\_gamma(a1 - a2, diff\_b, prime\_modulus)  
 end  
 end  
 end

## Метод Полларда

return "Invalid"  
end  
  
prime1 = 2341  
alpha1 = 4  
beta1 = 86  
println(pollard\_rho\_log(prime1, alpha1, beta1))  
  
prime2 = 1234  
alpha2 = 3  
beta2 = 4  
println(pollard\_rho\_log(prime2, alpha2, beta2))

# Заключение

В данной лабораторной работе представлена реализация дискретного логарифмирования в конечном поле