

```

1 #Лабораторная работа №7
2 #Тема: Дискретное логарифмирование в конечном поле
3 #Выполнила: Исламова Сания
4 #Группа НПИмд-01-24
5
6 # Заголовок программы
7 println("ρ-метод Полларда для дискретного логарифмирования")
8 # Бесконечный цикл для многократного использования программы
9 while true
10    # Запрос ввода данных от пользователя
11    println("\nВведите p a b r через пробел (или 'выход' для завершения):")
12    # Чтение введенной строки с клавиатуры
13    input = readline()
14    # Проверка команды выхода из программы
15    input == "выход" && break
16    # Блок обработки ошибок ввода
17    try
18        # Разделение строки на части и преобразование в BigInt
19        p,a,b,r = parse.(BigInt, split(input))
20        # Определение функции ρ-метода Полларда
21        function ρ(p,a,b,r)
22            # Инициализация: случайные u, v из [0, r-1]
23            u,v = rand(0:r-1,2)
24            # Вычисление начальной точки c = a^u * b^v mod p
25            c = powermod(a,u,p)*powermod(b,v,p)%p
26            # Черепаха и заяц: начальные точки одинаковы
27            d = c
28            # Инициализация логарифмов: log(c) = u + v*x, log(d) = u + v*x
29            α1,β1,α2,β2 = u,v,u,v
30            # Цикл поиска коллизии (метод Флойда)
31            while (c = (c<p÷2 ? a*c : b*c)%p) != d
32                # Обновление d (два шага)
33                (d = (d<p÷2 ? a*d : b*d)%p; d = (d<p÷2 ? a*d : b*d)%p)
34                # Обновление логарифмов для c (один шаг)
35                α1,β1 = (α1+(c<p÷2))%r, (β1+(c≥p÷2))%r
36                # Обновление логарифмов для d (два шага)
37                α2,β2 = (α2+2(d<p÷2))%r, (β2+2(d≥p÷2))%r
38            end
39            # После нахождения коллизии: решение уравнения
40            # Находим коэффициенты (β1-β2)*x ≡ (α2-α1) (mod r)
41            g,x,_ = gcdx((β1-β2)%r, r)
42            # Проверка разрешимости и возврат решения
43            (Δα=(α2-α1)%r)%g ≠ 0 ? nothing : (x*Δα÷g)%r
44        end
45        # Вызов функции и получение результата
46        x = ρ(p,a,b,r)
47        # Вывод результата
48        println(x==nothing ? "Нет решений" : "x = $x")
49        # Обработка ошибок при некорректном вводе
50        catch
51            println("Ошибка: введите 4 числа или 'выход'")
52        end
53    end
54    # Сообщение о завершении программы
55    println("Программа завершена")
56
57

```