Цель работы

Основной целью работы является реализовать алгоритм дискретного логарифмирования.

Выполнение лабораторной работы

Алгоритм, реализующий p-метод Полларда для задач дискретного логарифмирования

```
                end
                invr = modinv_safe(r, order)
                if invr === nothing
                    if verbose
                        @printf("Итерация %d: нет обратного для r=%d, перезапуск.\n", iter, r)
                    end
                    break
                end
                x_candidate = mod(lhs * invr, order)
                if powermod(g, x_candidate, p) == h % p
                    if verbose
                        @printf("Найдено решение: x=%d\n", x_candidate)
                    end
                    return x_candidate
                else
                    if verbose
                        @printf("x=%d не подошёл, перезапуск.\n", x_candidate)
                    end
                    break
                end
            end
        end
    end
    error("Не удалось найти дискретный логарифм после $max_restarts попыток.")
end
p = 1024
g = 2
x_true = 123
h = powermod(g, x_true, p)
x_found = pollard_rho_dlog(g, h, p; max_iter=10^5, max_restarts=50, partition_type=:hash, verbose=true)
@printf("Результат: найден x = %d (истинный x = %d)\n", x_found, x_true)
```

```
x=0 не подошёл, перезапуск.
Попытка 44: старт a=25 b=713 X=0
x=0 не подошёл, перезапуск.
Попытка 45: старт a=206 b=313 X=0
Итерация 1: нет обратного для r=51, перезапуск.
Попытка 46: старт a=389 b=119 X=0
Итерация 1: нет обратного для r=187, перезапуск.
Попытка 47: старт a=292 b=137 X=0
x=0 не подошёл, перезапуск.
Попытка 48: старт a=933 b=368 X=0
Итерация 1: нет обратного для r=486, перезапуск.
Попытка 49: старт a=380 b=189 X=0
Итерация 1: нет обратного для r=549, перезапуск.
Попытка 50: старт a=927 b=829 X=0
x=0 не подошёл, перезапуск.
```

Вывод

В ходе выполнения лабораторной работы был реализован алгоритм дискретного логарифмирования.