Отчёт по лабораторной работе №4: Вычисление наибольшего общего делителя

Дисциплина: Математические основы защиты информации и информационной безопасности

Савченко Елизавета Николаевна

Содержание

1 Общая информация о задании лабораторной работы

1.1 Цель работы

Выполнить лабораторную работу 4 и изучить алгоритмы вычисления наибольшего общего делителя

1.2 Задание

Реализовать все рассмотренные алгоритмы программно.

2. Теоретическое введение

2.1 Алгоритм Евклида

Основан на принципе, что НОД двух чисел a и b равен НОД числа b и остатка от деления a на b. Формально:

- НОД(a, b) = НОД(b, a mod b)
- Процесс повторяется, пока остаток не станет 0.
- Тогда НОД равен последнему ненулевому делителю.

2.2 Бинарный алгоритм Евклида

Также известен как алгоритм на основе сдвигов. Использует свойства двоичной арифметики:

- Если оба числа чётные, НОД(a, b) = 2 × НОД(a/2, b/2)
- Если одно число чётное, другое нечётное, делим чётное на 2 (сдвигаем вправо)
- Если оба нечётные, заменяем большее число на разность с меньшим
- Повторяем, пока числа не сравняются

Преимущество — отсутствие операций деления и взятия остатка, что ускоряет вычисления на двоичных системах.

2.3 Расширенный алгоритм Евклида

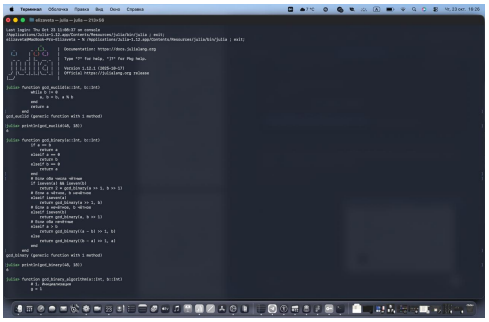
Помимо вычисления НОД, позволяет найти коэффициенты x и y в уравнении:
a×x + b×y = НОД(a, b)
Коэффициенты важны для решения уравнений в целых числах (например, диофантовы уравнения), криптографии (например, для нахождения обратного по модулю числа).

2.4 Расширенный бинарный алгоритм Евклида

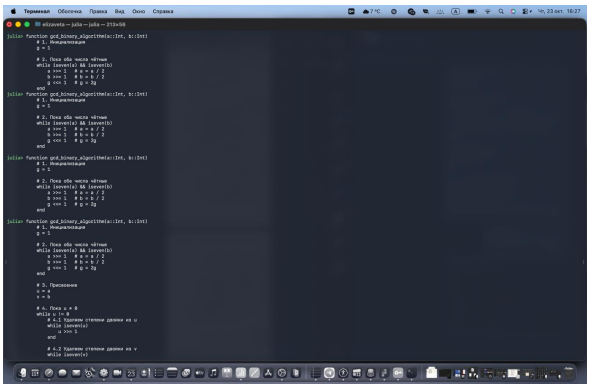
Комбинирует идеи расширенного алгоритма и бинарного, используя двоичные операции для ускорения и одновременно вычисляя коэффициенты x, y, что полезно при работе с большими числами.

3. Выполнение лабораторной работы

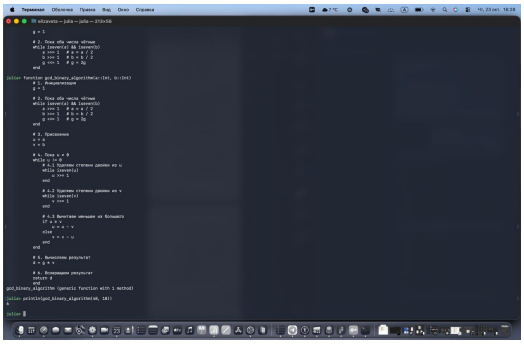
3.1 Алгоритм Евклида и Бинарный алгоритм Евклида



3.2 Расширенный алгоритм Евклида



3.3 Расширенный бинарный алгоритм Евклида



4. Выводы

В результате работы мы смогли реализовать все рассмотренные алгоритмы программно с помощью Julia