Математические основы защиты информации и информационной безопасности. Лабораторная работа №4. Вычисление наибольшего общего делителя

Лесков Данила Валерьевич, учебная группа: НФИмд-02-21
Преподаватель: Кулябов Дмитрий Сергеевич

20 ноября, 2021, Москва, Россия

Российский Университет Дружбы Народов

Цели и задачи

Цель лабораторной работы

Ознакомиться с алгоритмами вычисления наибольшего общего делителя.

Задачи лабораторной работы

Реализовать четыре алгоритма вычисления НОД: 1. Алгоритм Евклида; 2. Бинарный алгоритм Евклида; 3. Расширенный алгоритм Евклида; 4. Расширенный бинарный алгоритм Евклида.

Выполнение лабораторной работы

Наибольший общий делитель

Наибольшим общим делителем (НОД) для двух целых чисел `a` и `b` называется наибольший из их общих делителей. Наибольший общий делитель существует и однозначно определён, если хотя бы одно из чисел `a` или `b` не равно нулю.

Алгоритм Евклида

Для вычисления наибольшего общего делителя двух целых чисел применяется способ повторного деления с остатком, называемый алгоритмом Евклида.

Бинарный алгоритм Евклида

Бинарный алгоритм Евклида является более быстрым при реализации на компьютере, поскольку использует двоичное представление чисел `a` и `b`.

Расширенный алгоритм Евклида

Расширенный алгоритм Евклида находит наибольший общий делитель `d` чисел `a` и `b` и его линейное представление, т. е. целые числа `x` и `y`, для которых $+ by = d$.

Расширенный бинарный алгоритм Евклида

Расширенный бинарный алгоритм Евклида так же, как и предыдущий алгоритм, позволяет найти наибольший общий делитель `d` чисел `a` и `b` и его линейное представление, но при том используется двоичное представление чисел `a` и `b`.

Описание реализации алгоритмов

В данной работе были описаны 4 метода для нахождения наибольшего общего делителя. Каждый из методов принимает на вход два целых положительных числа `a` и `b`, причем `a` не должно быть меньше `b`. В результате отработки каждый из методов возвращает наибольший общий делитель этих двух целых чисел, а расширенные версии этих методов дополнительно возвращают `x` и `y` коэффициенты такие, что выполняется следующее равенство:

$$ax + by = d,$$

где `d` - наибольший общий делитель чисел `a` и `b`.

Полученные результаты

Алгоритм Евклида

```
Выберите алгоритм нахождения НОД:
    1 - Алгоритм Евклида;
    2 - Бинарный алгоритм Евклида;
    3 - Расширенный алгоритм Евклида;
    4 - Расширенный бинарный алгоритм Евклида;
    ------------------------
    0 - Выход из программы
Введите номер операции: 1
Введите первое число: 4
Введите второе число: 12

Ваши числа:
    a = 12
    b = 4

НОД для 12 и 4 = 4
```

Figure 1: Алгоритм Евклида

Бинарный алгоритм Евклида

```
Выберите алгоритм нахождения НОД:
    1 - Алгоритм Евклида;
    2 - Бинарный алгоритм Евклида;
    3 - Расширенный алгоритм Евклида;
    4 - Расширенный бинарный алгоритм Евклида;
    ------------------------
    0 - Выход из программы
Введите номер операции: 2
Введите первое число: 9
Введите второе число: 18

Ваши числа:
    a = 18
    b = 9

НОД для 18 и 9 = 9
```

Figure 2: Бинарный алгоритм Евклида

Расширенный алгоритм Евклида

```
Выберите алгоритм нахождения НОД:
    1 - Алгоритм Евклида;
    2 - Бинарный алгоритм Евклида;
    3 - Расширенный алгоритм Евклида;
    4 - Расширенный бинарный алгоритм Евклида;
    ------------------------
    0 - Выход из программы
Введите номер операции: 3
Введите первое число: 4
Введите второе число: 16

Ваши числа:
    a = 16
    b = 4

НОД для 16 и 4 = 4
x = 0
y = 1

16*0 + 4*1 = 4
```

Figure 3: Расширенный алгоритм Евклида

Расширенный бинарный алгоритм Евклида

```
Выберите алгоритм нахождения НОД:
    1 - Алгоритм Евклида;
    2 - Бинарный алгоритм Евклида;
    3 - Расширенный алгоритм Евклида;
    4 - Расширенный бинарный алгоритм Евклида;
    ------------------------
    0 - Выход из программы
Введите номер операции: 4
Введите первое число: 25
Введите второе число: 5

Ваши числа:
    a = 25
    b = 5

НОД для 25 и 5 = 5
x = 0
y = 1

25*0 + 5*1 = 5
```

Figure 4: Расширенный бинарный алгоритм Евклида

Выводы

Результаты выполнения лабораторной работы

В ходе выполнения данной лабораторной работы было выполнено ознакомление с различными методами нахождения наибольшего общего делителя.
В результате проделанной работы были программно реализованы следующие методы нахождение НОД: алгоритм Евклида, бинарный алгоритм Евклида, расширенный алгоритм Евклида и расширенный бинарный алгоритм Евклида.