Алгоритм Евклида

Мохаммад хоссейн фарзанфар

4 , 2, 2025, Москва, Россия

Российский Университет Дружбы Народов

Цели и задачи

Цель лабораторной работы

Изучение алгоритма Евклида нахождения НОД и его вариаций.

Выполнение лабораторной работы

Наибольший общий делитель

Наибольший общий делитель (НОД) – это число, которое делит без остатка два числа и делится само без остатка на любой другой делитель данных двух чисел. Проще говоря, это самое большое число, на которое можно без остатка разделить два числа, для которых ищется НОД.

Алгоритм Евклида

- Вход. Целые числа $a, b; 0 < b < a$.
- Выход. $d = \text{НОД}(a, b)$.

1. Положить $r_0 = a$, $r_1 = b$, $i = 1$.
2. Найти остаток $r_i + 1$ от деления $r_i{-}1$ на r_i.
3. Если $r_i + 1 = 0$, то положить $d = r_i$. В противном случае положить $i = i + 1$ и вернуться на шаг 2.
4. Результат: d.

Бинарный алгоритм Евклида

- Вход. Целые числа $a, b; 0 < b \leq a$.
- Выход. $d = \text{НОД}(a, b)$.

1. Положить $g = 1$.
2. Пока оба числа a и b четные, выполнять $a = a/2, b = b/2, g = 2g$ до получения хотя бы одного нечетного значения a или b.
3. Положить $u = a, v = b$.
4. Пока $u \neq 0$, выполнять следующие действия.
   - Пока u четное, полагать $u = u/2$.
   - Пока v четное, полагать $v = v/2$.
   - При $u \geq v$ положить $u = u - v$. В противном случае положить $v = v–u$.
5. Положить $d = gv$.
6. Результат: d

Расширенный алгоритм Евклида

- Вход. Целые числа $a, b; 0 < b \leq a$.
- Выход: $d = \text{НОД}(a, b)$; такие целые числа x, y, что $ax + by = d$.

1. Положить
   $r_0 = a, r_1 = b, x_0 = 1, x_1 = 0, y_0 = 0, y_1 = 1, i = 1$
2. Разделить с остатком r_i–1 на r_i :
   $r_(i–1) = q_i * r_i + r_i + 1$
3. Если $r_(i + 1) = 0$, то положить $d = r_i, x = x_i, y = y_i$.
   В противном случае положить
   $x_(i + 1) = (x_(i–1)–q_i * x_i, y_(i + 1) = y_(i–1)–q_i * y_i,$
   $i = i + 1$ и вернуться на шаг 2.
4. Результат: d, x, y.

Пример работы алгоритма

```
PS C:\Users\AbdulazizMohammedAlg> & C:/Python311/python.exe "d:/Master/Sub/Математические основы защиты информации и информационной безопасности (02.04.02, НФИмд)/lab4/04/lab4.py"
Введите число a: 999
Введите число b: 99
Простой алгоритм Евклида: 9
Расширенный алгоритм Евклида: (9, 1, -10)
Бинарный алгоритм Евклида: 9
Расширенный бинарный алгоритм Евклида: (9, 34, -343)
PS C:\Users\AbdulazizMohammedAlg>
```

Рис. 1: Работа алгоритма

Выводы

Результаты выполнения лабораторной работы

Изучили алгоритм Евклида нахождения НОД.