Отчёт по лабораторной работе №4

Дисциплина: Математические основы защиты информации и информационной безопасности

Дэнэилэ Александр Дмитриевич, НПМмд-02-23

Содержание

Список таблиц

Список иллюстраций

1 Цель работы

Изучить алгоритмы вычисления наибольшего общего делителя.

2 Задание

1. Реализовать алгоритм Евклида.
2. Реализовать бинарный алгоритм Евклида
3. Реализовать расширенный алгоритм Евклида
4. Реализовать расширенный бинарный алгоритм Евклида

3 Теоретическое введение

Пусть числа a и b целые и $b \neq 0$. Разделить a на b с остатком - значит представить a в виде $a = qb + r$, где $q, r \in \mathbb{Z}$ и $0 \leq r \leq |b|$. Число q называется неполным частным, число r - неполным остатком от деления a на b.

Целое число $d \neq 0$ называется *наибольшим общим делителем* целых чисел $a_1, a_2, \dots, a_k$ (обозначается $d =$ НОД($a_1, a_2, \dots, a_k$)), если выполняются следующие условия:

1. Каждое из чисел $a_1, a_2, \dots, a_k$ делится на d;
2. Если $d_1 \neq 0$ - другой общий делитель чисел $a_1, a_2, \dots, a_k$, то d_1 делится на d.

Например, НОД(12345, 24690) = 12345, НОД(12345, 54321) = 3, НОД(12345, 12541) = 1.

Ненулевые целые числа a и b называются *ассоциированными* (обозначается a b), если a делится на b и b делится на a.

Для любых целых чисел $a_1, a_2, \dots, a_k$ существует наибольший общий делитель d и его можно представить в виде *линейной комбинации* этих чисел:

$d = c_1a_1 + c_2a_2 + \cdots + c_ka_k, c_i \in \mathbb{Z}$

Например, НОД чисел 91, 105, 154 равен 7. В качестве линейного представления можно взять

$7 = 7 \cdot 91 - 6 \cdot 105 + 0 \cdot 154,$

либо

$7 = 4 \cdot 91 + 1 \cdot 105 - 3 \cdot 154$

Целые числа $a_1, a_2, \dots, a_k$ называются *взаимно простыми в совокупности*, если НОД($a_1, a_2, \dots, a_k$) = 1. Целые числа a и b называются *взаимно* простыми, если НОД(*a, b*) = 1.

Целые числа $a_1, a_2, \dots, a_k$ называются *попарно взаимно простыми*, если НОД(a_i, a_j) = 1 для всех $1 \leq i \neq j \leq k$.

4 Выполнение лабораторной работы

1. Реализация алгоритма Евклида нахождения наименьшего общего делителя (рис. 4.1).

```
a = int(input())
b = int(input())
d = None

r0 = a; r1 = b
r2 = None

while r2 != 0:
  d = r2
  r2 = r0 % r1
  r0 = r1
  r1 = r2

print("НОД =", d)
```

```
48
36
НОД = 12
```

Рис. 4.1: Алгоритм Евклида

2. Реализация бинарного алгоритма Евклида нахождения наименьшего общего делителя (рис. 4.2).

```
a = int(input())
b = int(input())
d = None

g = 1

while (a % 2 == 0) & (b % 2 == 0):
  a /= 2; b /= 2; g *= 2

u = a; v = b

while u != 0:
  while u % 2 == 0:
    u /= 2
  while v % 2 == 0:
    v /= 2
  if u >= v:
    u = u - v
  else:
    v = v - u

d = g*v
print("НОД =", d)
```

```
48
36
НОД = 12.0
```

Рис. 4.2: Бинарный алгоритм Евклида

3. Реализация расширенного алгоритм Евклида нахождения наименьшего общего делителя и представление его в виде линейной комбинации чисел a и b (рис. 4.3).

```
a = int(input())
b = int(input())
d = None

r0 = a; r1 = b
r2 = None
x0 = 1; x1 = 0; y0 = 0; y1 = 1
x2 = None; y2 = None

while r2 != 0:
  d = r2
  x = x2
  y = y2
  r2 = r0 % r1
  q = r0 // r1
  r0 = r1
  r1 = r2
  x2 = x0 - q * x1
  y2 = y0 - q * y1

print("НОД =", d)
print(x, y, a*x + b*y)
```

```
48
36
НОД = 12
1 -1 12
```

Рис. 4.3: Расширенный алгоритм Евклида

4. Реализация расширенного бинарного алгоритма Евклида нахождения наименьшего общего делителя и представление его в виде линейной комбинации чисел a и b (рис. 4.4).

```python
a = int(input())
b = int(input())
d = None

g = 1

while (a % 2 == 0) & (b % 2 == 0):
  a /= 2; b /= 2; g *= 2

u = a; v = b
A = 1; B = 0; C = 0; D = 1

while u != 0:
  while u % 2 == 0:
    u /= 2
    if (A % 2 == 0) & (B % 2 == 0):
      A /= 2; B /= 2
    else:
      A = (A+b)/2; B = (B-a)/2
  while v % 2 == 0:
    v /= 2
    if (C % 2 == 0) & (D % 2 == 0):
      C /= 2; D /= 2
    else:
      C = (C+b)/2; D = (D-a)/2
  if u >= v:
    u = u - v
    A -= C
    B -= D
  else:
    v = v - u
    C -= A
    D -= B

d = g*v
x = C
y = D
print("НОД =", d)
print(x, y, d)
```

```
48
36
НОД = 12.0
1.0 -1.0 12.0
```

Рис. 4.4: Расширенный бинарный алгоритм Евклида

5 Выводы

Ознакомился с различными вариациями реализации алгоритмов нахождения наименьшего общего делителя.

Список литературы