

Отчёт по лабораторной работе №4

Вычисление наибольшего общего делителя
Еленга Невлора Люглеш

Содержание

1. Цель работы	1
2. Задание	1
3. Теоретическое введение	1
4. Выполнение лабораторной работы	2
5. Выводы	5
Список литературы	5

1. Цель работы

Изучить и реализовать Вычисление наибольшего общего делителя и реализовать все рассмотренные алгоритмы программно.

2. Задание

Реализовать все рассмотренные алгоритмы программно.

- Алгоритм Евклида
- Бинарный алгоритм Евклида
- Расширенный алгоритм Евклида
- Расширенный бинарный алгоритм Евклида

3. Теоретическое введение

В 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 $0 \leq r < |b|$. Число q называется неполным частным, число r - неполным остатком от деления a на b .

Целое число $d \neq 0$ называется наибольшим общим делителем целыхаског чисел

a_1, a_2, \dots, a_n (обозначается $d = \text{НОД}(a_1, a_2, \dots, a_n)$), если выполняются следующие

условия:

1. каждое из чисел a_1, a_2, \dots, a_k делится на d ; Г. Черн
2. если $d \neq 0$ - другой общий делитель чисел a_1, a_2, \dots, a_k ,

Например, $\text{НОД}(12345, 24690) = 12345$, $\text{НОД}(12345, 54321) = 3$, Ненулевые целые числа a и b называются ассоциированными (обозначается $a \sim b$), 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:

$d = ca_1 + ca_2 + \dots + ca_k$ (Скаж, $C \in \mathbb{Z}$ (\mathbb{Z} - множество целых чисел)).

Например, НОД чисел 91, 105, 154 равен 7. В качестве линейного представления можно взять Вайгосуда $a = 7 = 7 \cdot 91 + (-6) \cdot 105 + 0 \cdot 154$

Целые числа a_1, a_2, \dots, a_k называются взаимно простыми в совокупности, если $\text{НОД}(a_1, a_2, \dots, a_k) = 1$. Целые числа a и b называются взаимно простыми, если $\text{НОД}(a, b) = 1$. Например, $\text{НОД}(91, 105, 154) = 7$.

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

4. Выполнение лабораторной работы

- Код

- функция для Алгоритма Евклида:

```
def algo_euclid(a,b):
    r0, r1 = a, b
    i = 1
    while True :
        ri_plus_1 = r0 % r1
        if ri_plus_1 == 0:
            return r1
        r0, r1 = r1, ri_plus_1
        i = i+1
```

- функция для Бинарного алгоритма Евклида :

```
def binar_algo_euclid(a,b):
    g=1
    while a%2 == 0 and b%2 == 0:
        a = a // 2
        b = b // 2
```

```

    g *= 2
    u, v = a, b

    while u != 0:
        while u % 2 == 0:
            u = u // 2
        while v % 2 == 0:
            v = v // 2
        if u >= v:
            u = u - v
        else :
            v = v-u
    d =g*v
    return d

```

- функция для расширенного алгоритма Евклида :

```

def raschi_algo_euvclida(a,b):
    r0, r1 = a, b
    x0, x1 = 1, 0
    y0, y1 = 0, 1
    i = 1
    while True:
        qi = r0 // r1
        ri_plus_1 = r0 % r1
        if ri_plus_1 == 0:
            d = r1
            x = x1
            y = y1
            return d, x, y
        xi_plus_1 = x0 - qi * x1
        yi_plus_1 = y0 - qi * y1

        r0, r1 = r1, ri_plus_1
        x0, x1 = x1, xi_plus_1
        y0, y1 = y1, yi_plus_1
        i += 1

```

- функция для расширенного бинарного алгоритма Евклида :

```

def raschi_binar_algo_euvclida(a,b):
    original_a , original_b = a, b
    g=1

```

```

while a%2 == 0 and b%2 == 0:
    a = a // 2
    b = b // 2
    g *= 2
u, v = a, b
A, B, C, D = 1, 0, 0, 1

while u != 0:
    while u % 2 == 0:
        u = u // 2
        if A % 2 == 0 and B % 2 == 0:
            A = A // 2
            B = B // 2
        else :
            A = (A + original_b) // 2
            B = (B - original_a) // 2
    while v % 2 == 0:
        v = v // 2
        if C % 2 == 0 and D % 2 == 0:
            C = C // 2
            D = D // 2
        else:
            C = (C + original_b) // 2
            D = (D - original_a) // 2
    if u >= v:
        u = u - v
        A = A - C
        B = B - D
    else :
        v = v - u
        C = C - A
        D = D - B

d = g*v
x, y = C, D
return d , x, y

```

- Результаты:

```
    algo_euvclida(12345, 24690)
-- 12345

    binar_algo_euvclida(12345, 24690)
-- 12345

    binar_algo_euvclida(12345, 54321)
-- 3

    raschi_algo_euvclida(12345, 24690)
-- (12345, 1, 0)
> ~
    raschi_algo_euvclida(12345, 54321)
-- (3, 3617, -822)

    raschi_binar_algo_euvclida(12345, 24690)
[23]
... (12345, 12345, -6172)

    raschi_binar_algo_euvclida(12345, 54321)
[24]
... (3, -14490, 3293)

    raschi_binar_algo_euvclida(12345, 12541)
[25]
... (1, 4159, -4094)
```

5. Выводы

В ходе выполнения данной лабораторной работы изучили и реализовали :

- Алгоритм Евклида

- Бинарный алгоритм Евклида
- Расширенный алгоритм Евклида
- Расширенный бинарный алгоритм Евклида

.Список литературы

::: {#Методические указания к лабораторной работе №4.}