Математические основы защиты информации и информационной безопасности.

Лабораторная работа №4.

Сапёров Максим Александрович.

Содержание

List of Figures

List of Tables

1 Цель работы

Освоить на практике вычисление наибольшего делителя разными способами

2 Задание

1. Реализовать вычисление НОД алгоритмом Евклида
2. Реализовать вычисление НОД бинарным алгоритмом Евклида
3. Реализовать вычисление НОД расширенным алгоритмом Евклида
4. Реализовать вычисление НОД расширенным бинарным алгоритмом Евклида

3 Выполнение лабораторной работы

Написал код для вычисление НОД алгоритмом Евклида

```
[ ]    def euclid(a,b):
         r = [a,b]
         i = 1
         while True:
           r_new = r[-2]%r[-1]
           if r_new == 0:
             return r[-1]
           else:
             i+=1
             r.append(r_new)
```

Figure 3.1: вычисление НОД алгоритмом Евклида

Реализовал вычисление НОД бинарным алгоритмом Евклида

```
[ ]    def euclid_bin(a,b):
         g = 1
         while a%2==0 and b%2==0:
           a = a/2
           b = b/2
           g = 2*g

         u = copy(a)
         v = copy(b)
         while u!=0:
           if u%2==0:
             u=u/2
           if v%2==0:
             v=v/2
           if u>=v:
             u = u-v
           else:
             v = v-u
         return g*v
```

Figure 3.2: НОД бинарным алгоритмом Евклида

Реализовать вычисление НОД расширенным алгоритмом Евклида

```
[ ]    def euclid_ext(a,b):
         r = [a,b]
         x = [1,0]
         y = [0,1]
         i = 1
         while True:
           q = r[-2]//r[-1]
           r_new = r[-2]%r[-1]
           if r_new==0:
             return r[-1], x[-1], y[-1]
           else:
             x.append(x[-2]-q*x[-1])
             y.append(y[-2]-q*y[-1])
             r.append(r_new)
             i+=1
```

Figure 3.3: НОД расширенным алгоритмом Евклида

Реализовать вычисление НОД расширенным бинарным алгоритмом Евклида

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

  u = copy(a)
  v = copy(b)
  A = 1
  B = 0
  C = 0
  D = 1
  while u!=0:
    if u%2==0:
      u=u/2
      if A%2==0 and B%2==0:
        A = A/2
        B = B/2
      else:
        A = (A+b)/2
        B = (B-a)/2
    if v%2==0:
      v=v/2
      if C%2==0 and D%2==0:
        C = C/2
        D = D/2
      else:
        C = (C+b)/2
        D = (D-a)/2
    if u>=v:
      u = u-v
      A = A-C
      B = B-D
    else:
      v = v-u
      C = C-A
      D = D-B
  return g*v, C, D
```

Figure 3.4: НОД расширенным бинарным алгоритмом Евклида

Результаты тестов.

```
[10]  euclid(2468,1234),euclid_bin(2468,1234),euclid_ext(2468,1234),euclid_ext_bin(2468,1234)
(1234, 1234.0, (1234, 0, 1), (1234.0, 0, 1))

[6]   euclid(2468,51)
1

[7]   euclid_bin(24,12)
12.0

[8]   euclid_ext(27,6)
(3, 1, -4)

[9]   euclid_ext_bin(27,6)
(3.0, 3.0, -13.0)
```

Figure 3.5: результаты тестов

4 Выводы

Освоил на практике вычисление наибольшего делителя разными способами