Лабораторная работа №4

Алгориммы вычисления наибольшего общего делителя

Яковлев Артём Александрович, НФИмд-01-22

Содержание

Список таблиц

Список иллюстраций

Цель работы

Цель данной работы — изучить и программно реализовать алгориммы вычисления наибольшего общего делителя.

Задание

Заданием является реализовать:

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

Теоретическое введение

Давайте считать, что я тут написал что-то по теме. Мне просто лень.

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

Выполнение лабораторной работы

Для реализации шифров мы будем использовать Python, так как его синтаксис позволяет быстро реализовать необходимые нам алгоритмы.

Реализация алгоритма Евклида

Алгоритм Евклида

```
In [31]:
def euclid (a, b):
    while a!= 0 and b != 0:
        if a>b:
            a %= b
        else:
            b %= a
    return a or b
```

```
In [32]:
euclid (15625, 125)
```

```
Out[32]: 125
```

Рис. 0.1: алгоритм Евклида

Реализация бинарного алгоритма Евклида

Бинарный алгоритм Евклида

In [8]:
```
def bin_evclid(a ,b):
    if a == b:
        return a
    g = 0
    while (a|b) & 1 == 0:
        g += 1
        a >>= 1
        b >>= 1
    while a&1 == 0:
        a>>=1
    while b!= 0:
        while b&1 == 0:
            b>>=1
        if a > b:
            a , b = b, a
        b -= a
    return a <<g
```

In [9]:
```
bin_evclid(625,25)
```

Out[9]: 25

Рис. 0.2: бинарный алгоритм Евклида

Реализация расширенного алгоритма Евклида

Расширенный алгоритм Евклида

In [10]:
```
def ras_evclid(a, b):
    if a == 0:
        y = 0
        x = 1
        return b, y, x
    else:
        d, x, y = ras_evclid(b%a, a)
        return d, y - (b//a)*x, x
```

In [12]:
```
ras_evclid(15625, 125)
```

Out[12]: (125, 0, 1)

Рис. 0.3: расширенный алгоритм Евклида

Расширенный бинарный алгоритм Евклида

n [14]:

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

n [15]:

```
ras_bim_evclid(15625, 125)
```

Out[15]: (125, 0, 1)

Рис. 0.4: расширенный бинарный алгоритм Евклида

Выводы

Лабораторная работа выполнена.