Математические основы защиты информации и информационной безопасности

Дарижапов Тимур Андреевич

26 Октября 2024

РУДН, Москва, Россия

Лабораторная работа 4

алгоритм Евклида

In [4]:

```
number1 = 15
number2 = 61

num1 = number1
num2 = number2
while num1 != 0 && num2 != 0
    if num1 >= num2
        num1 = num1 % num2
    else
        num2 = num2 % num1
    end
end

nod1 = num1 + num2
println(nod1)
```

```
1
```

Рис. 1: Реализация программы

Бинарный алгоритм Евклида

In [5]:

```
num1 = number1
num2 = number2
shift = 0

while (num1 | num2) & 1 == 0
    shift += 1
    num1 >>= 1
    num2 >>= 1
end

while num1 & 1 == 0
    num1 >>= 1
end

while num2 != 0
    while num2 & 1 == 0
        num2 >>= 1
    end
    if num1 > num2
        num1, num2 = num2, num1
    end
    num2 -= num1
end

println(num1 << shift)
```

```
1
```

Расширенный алгоритм Евклида

In [21]:

```
function ext_evk(a, b)
    if b == 0
        return a, 1, 0
    else
        nod, x1, y1 = ext_evk_2(b, a % b)
        x = y1
        y = x1 - div(a, b) * y1
        return nod, x, y
    end
end
x, y, g = ext_evk(number1, number2)
println(x, '*', number1, '+','(', y,')' ,'*',number2, '=', g)
```

```
1*15+(-4)*61=1
```

Рис. 3: Реализация программы

Расширенный бинарный алгоритм Евклида

```python
def ext_gcd(a, b):
    if a == 0: return 1, 1, b
    if b == 0: return 1, 1, a
    if not a & 1 | b & 1:
        x, y, g = ext_gcd(a >> 1, b >> 1)
        return x, y, g << 1
    elif not a & 1:
        x, y, g = ext_gcd(a >> 1, b)
        return (x - b >> 1, y + (a >> 1), g) if x & 1 else (x >> 1, y, g)
    elif not b & 1:
        x, y, g = ext_gcd(a, b >> 1)
        return (x + (b >> 1), y - a >> 1, g) if y & 1 else (x, y >> 1, g)
    elif b > a:
        x, y, g = ext_gcd(a, b - a)
        return x - y, y, g
    else:
        x, y, g = ext_gcd(a - b, b)
        return x, y - x, g
```

Рис. 4: Реализация программы

Ответы всех программ

```
1
1
-4 * 15 + ( 1 ) * 61 = 1
57 * 15 + ( -14 ) * 61 = 1
```

Рис. 5: Вывод программ

Выводы

- Познакомился с алгоритмами вычисления наибольшего общего делителя.
- Применил алгоритмы на практике.

Спасибо за внимание!