Отчёт по лабораторной работе №6

Разложение чисел на множители

Студент: Гонсалес Ананина Луис Антонио, 1032175329
Группа: НФИмд-02-21
Преподаватель: Кулябов Дмитрий Сергеевич,
д-р.ф.-м.н., проф.

Москва 2021

Содержание

List of Figures

1 Цель работы

Цель данной лабораторной работы- изучить теорию и реализовать рассмотренный алгоритм программно.

2 Теоретические сведения

Любое натуральное число n > 1 можно представить в виде произведения простых чисел. Это представление называется разложением числа n на простые множители.

Натуральное число n называется делителем целого числа m, если для подходящего целого числа k верно равенство m = n ⊠k. В этом случае говорят, что m делится на n или что число m кратно числу n.

Простым числом называют натуральное число p >= 2, делящееся только на себя и на единицу. Составным числом называют число, имеющее больше двух различных делителей (любое натуральное число m, не равное 1, имеет как минимум два делителя: 1 и |m|). Например, числа 2, 3, 5, 7, 11 – простые, а числа 9 = 3x3, 26 = 2 x 13 – составные[1].

p-Метод Полларда

Число называется B-гладкостепенным, если все его простые делители, в степенях, в которых они входят в разложение этого числа p^v, удовлетворяют p^v<=B. Согласно малой теореме Ферма для любого простого числа p и для любого целого числа a, такого что a и p взаимно просты, или, что в данном случае равносильно, p не делит a , справедливо[2]:

$$a^{(p-1)} \equiv 1 \mod p, \text{ более того } \forall M = (p-1)l, l \in N \Rightarrow a^M \equiv 1 \mod p.$$

Figure 2.1: Метод Полларда

3 Выполнение работы

In [1]:
```
from math import gcd
```

In [2]:
```
ag=1
bg=1
def f(x,n):
    return (x*x+5)%n
```

In [3]:
```
def fu(n,a,b,d):
    a=f(a,n)%n
    b=f(f(b,n),n)%n
    d=gcd(a-b,n)
    if 1<d<n:
        p=d
        print(p)
        exit()
    if d==n:
        print('Делитель не найден')
    if d==1:
        global ag
        ag=b
        fu(n,a,b,d)
```

In [4]:
```
def main():
    n=1359331
    c=1
    a=c
    b=c
    a=f(a,n)%n
    b=f(a,n)%n
    d=gcd(a-b,n)
    if 1<d<n:
        p=d
        print(p)
        exit()
    if d==n:
        pass
    if d==1:
        fu(n,a,b,d)
```

In [5]:
```
main()
```

```
1181
```

Figure 3.1: Код

4 Выводы

В итоге в данной лабораторной работы я изучил теорию и реализовал рассмотренный алгоритм программно.

Список литературы

1. Разложение чисел на множетели [Электронный ресурс]. Википедия, 2021. URL: https://umath.ru/calc/factorization/.
2. Метод Полларда [Электронный ресурс]. Википедия, 2021. URL: https://ru.wikipedia.org/wiki/P−1-метод_Полларда#Определения_и_математические_сведения.