Разложение чисел на множители

Тагиев Байрам Алтай оглы

Содержание

1 Цель работы

Изучение задачи разложения на множители, изучение p-алгоритма Полларда.

2 Теоретические сведения

2.1 p-алгоритм Полларда

- Вход. Число n, начальное значение c, функция f, обладающая сжимающими свойствами.
- Выход. Нетривиальный делитель числа n.

1. Положить $a = c, b = c$
2. Вычислить $a = f(a)(mod n), b = f(b)(mod n)$
3. Найти $d = GCD(a - b, n)$
4. Если $1 < d < n$, то положить $p = d$ и результат: p. При $d = n$ результат: ДЕЛИТЕЛЬ НЕ НАЙДЕН. При $d = 1$ вернуться на шаг 2.

3 Выполнение работы

3.1 Реализация алгоритма на языке Python

```
from math import gcd

def f(x, n):
    return (x*x+5)%n

def fu(n, a, b, d):
    a = f(a, n)
    b = f(f(b, n), n)
    d = gcd(a-b, n)
    if 1 < d < n:
        print(a, b, d, sep="\t")
        print()
        print("result: ", d)
        exit()
    if d == n:
        print("doesn't exist")
    if d == 1:
        print(a, b, d, sep="\t")
        fu(n, a, b, d)
```

```
if __name__ == "__main__":
    n = 1359331
    c = 1
    a = f(c, n)
    b = f(a, n)
    d = gcd(a-b, n)
    if 1 < d < n:
        print(d)
        exit()
    if d == n:
        pass
    if d == 1:
        print(a, b, d, sep="\t")
        fu(n, a, b, d)
```

3.2 Контрольный пример

```
6   41  1
41  123939  1
1686    391594  1
123939  438157  1
435426  582738  1
391594  1144026 1
1090062 885749  1181

result:  1181
```