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 , начальное значение , функция , обладающая сжимающими свойствами.
* Выход. Нетривиальный делитель числа .

1. Положить
2. Вычислить
3. Найти
4. Если , то положить и результат: . При результат: ДЕЛИТЕЛЬ НЕ НАЙДЕН. При 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