Лабораторная работа 6

Разложение чисел на множители

Греков Максим Сергеевич

Содержание

# Цель работы

* Ознакомиться с задачей разложения простого числа на множители
* Рассмотреть каноническое представление числа
* Реализовать метод нахождения нетривиальных сомножителей

# Описание задачи

## Каноническое разложение

Задача разложения на множители - одна из первых задач, использованных для построения криптосистем с открытым ключом.

Задача разложения составного числа на множители формулируется следующим образом:

для данного положительного целого числа найти его каноническое разложение , где - попарно различные простые числа,

## Задача нахождения сомножителей

На практике не обязательно находить каноническое разложение числа .

Достаточно найти его разложение на два нетривиальных сомножителя: .

Далее будем понимать задачу разложения именно в этом смысле. Для её решения воспользуемся p-Методом Полларда (рис. 1) и реализуем его посредством Python (рис. 2)

# Описание алгоритма

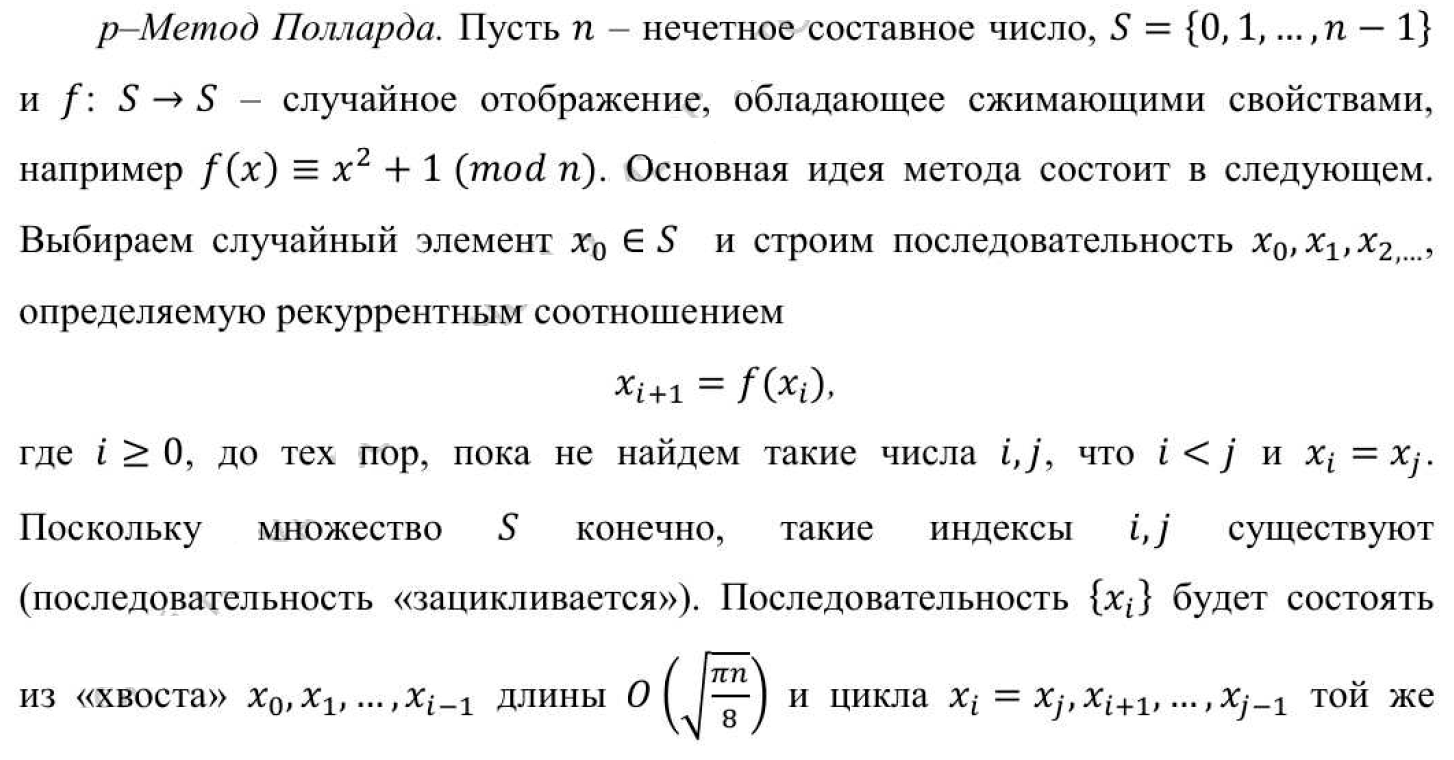


Figure 1: p-Метод Полларда

# Реализация алгоритма

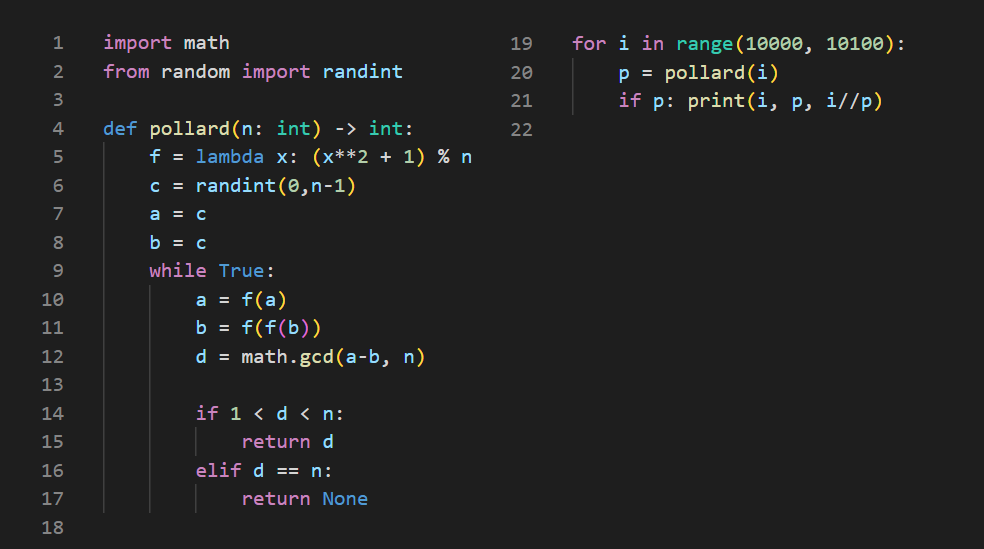


Figure 2: Реализация алгоритма

# Программный код

import math   
from random import randint  
  
def pollard(n: int) -> int:  
 f = lambda x: (x\*\*2 + 1) % n  
 c = randint(0,n-1)  
 a = c  
 b = c  
 while True:  
 a = f(a)  
 b = f(f(b))  
 d = math.gcd(a-b, n)  
  
 if 1 < d < n:  
 return d  
 elif d == n:  
 return None  
  
for i in range(10000, 10100):  
 p = pollard(i)  
 if p: print(i, p, i//p)

# Выводы

* Ознакомились с задачей разложения простого числа на множители
* Рассмотрели каноническое представление числа
* Реализовали метод нахождения нетривиальных сомножителей