Отчёт по лабораторной работе №6

Разложение чисел на множители

Кодже Лемонго Арман

Содержание

Список иллюстраций

# Цель работы

Целью данной является Изучение p-алгоритма Поллрада и разложить на множители.

# Теоретические сведения

Разложение на множители — это процесс представления алгебраического выражения, такого как многочлен, в виде произведения более простых выражений или множителей. Этот метод позволяет упростить сложные уравнения и облегчить их решение.

Согласно Основной теореме арифметики любое положительное целое число больше единицы может быть уникально записано в следующей главной форме разложения на множители, где — простые числа и — положительные целые числа.

К сожалению, совершенный алгоритм для этого пока не найден. Хотя есть несколько алгоритмов, которые могут разложить число на множители, ни один не способен провести разложение достаточно больших чисел в разумное время. Позже мы увидим, что это хорошо для криптографии, потому что современные криптографические системы полагаются на этот факт. В этой секции мы даем несколько простых алгоритмов, которые проводят разложение составного числа. Цель состоит в том, чтобы сделать процесс разложения на множители менее трудоёмким.

Заметим, что этот метод требует сделать операций возведения в степень . Есть быстрый алгоритм возведения в степень, который выполняет это за операций. Метод также использует вычисления НОД, который требует операций. Мы можем сказать, что сложность — так или иначе больше, чем или , где — число битов в . Другая проблема – этот алгоритм может заканчиваться сигналом об ошибке. Вероятность успеха очень мала, если имеет значение, не очень близкое к величине .

## p-алгоритм Поллрада

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

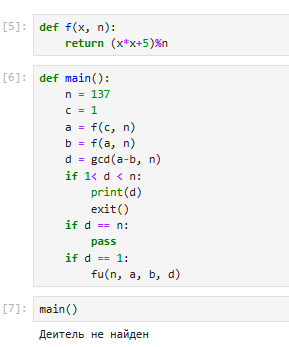
1. Положить
2. Вычислить
3. Найти
4. Если , то положить и результат: . При результат: ДЕЛИТЕЛЬ НЕ НАЙДЕН. При вернуться на шаг 2.

# Выполнение работы

## Реализация алгоритма на языке Python

Алгоритм, реализующий р-метод Полларда  
  
from math import gcd  
  
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(d)  
 exit()  
 if d == n:  
 print("Деитель не найден")  
 if d == 1:  
 fu(n, a, b, d)  
  
Разложить на множители данное преподавателем число  
  
def f(x, n):  
 return (x\*x+5)%n  
  
def 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:  
 fu(n, a, b, d)

## Контрольный пример

# Выводы

в конце нашего лабораторная работа, я изучил задачу разложения на множители и p-алгоритм Поллрада. P-алгоритм Полларда представляет собой мощный инструмент для разложения на множители, который сочетает в себе теоретические основы и практическое применение в области вычислительной математики.

# Список литературы

1. [Разложение на множители](https://infourok.ru/razlozhenie-na-mnozhiteli-mnogochlena-3-sposoba-4385153.html)
2. [Альгоритм P-метод Полларда](https://habr.com/ru/sandbox/163811/)