Лабораторная работа №6: отчет.

Разложение чисел на множители

Евдокимов Максим Михайлович. Группа - НФИмд-01-24.

Содержание

# Цели и задачи работы

## Цель лабораторной работы

Изучить представленные способы разложение чисел на множители и реализовать их в коде.

## Задание

Реализовать рассмотренные алгоритмы программно (алгоритм реализующий p-метод Полларда).

# Теоретическое введение

## Метод разложения числа на множители: p-метод Полларда

p-метод Полларда (метод ρ-Полларда) — это вероятностный алгоритм факторизации целых чисел, который находит нетривиальный делитель числа за время, пропорциональное .

Алгоритм основан на поиске цикла в псевдослучайной последовательности чисел, получаемой с помощью некоторой функции , примененной к числу по модулю .

### Алгоритм:

1. Выбираем начальное значение и функцию , например, .
2. Строим две последовательности чисел:
   * — последовательность, получаемая итеративным применением функции : .
   * — последовательность, получаемая с задержкой: .
3. Вычисляем наибольший общий делитель на каждом шаге.
4. Если и , то мы нашли нетривиальный делитель .
5. Если , то алгоритм завершился неудачно, и нужно выбрать другое начальное значение или функцию .

### Особенности:

* **Эффективность:** В среднем алгоритм работает за время , что значительно быстрее полного перебора делителей.
* **Вероятностный:** Алгоритм не гарантирует нахождение делителя, и в худшем случае может работать долго.
* **Простота реализации:** Алгоритм легко реализуется и требует небольшого объема памяти.
* **Применимость:** Метод хорошо подходит для факторизации чисел среднего размера (до 100 десятичных цифр).

### Пример:

Рассмотрим число .

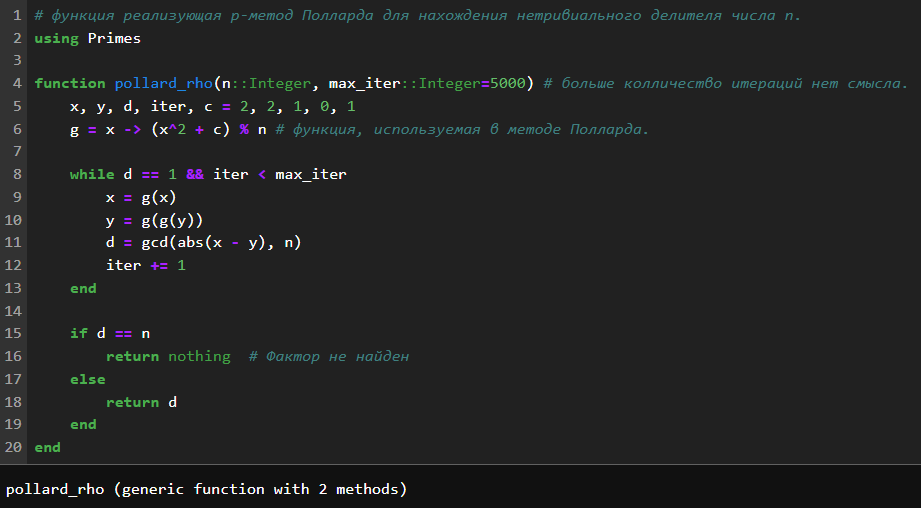
1. Выбираем и .
2. Строим последовательности:
3. Вычисляем .
4. 97 — нетривиальный делитель 8051.

### Заключение:

P-метод Полларда — это эффективный и простой в реализации алгоритм факторизации, который широко используется в криптографии и других областях.

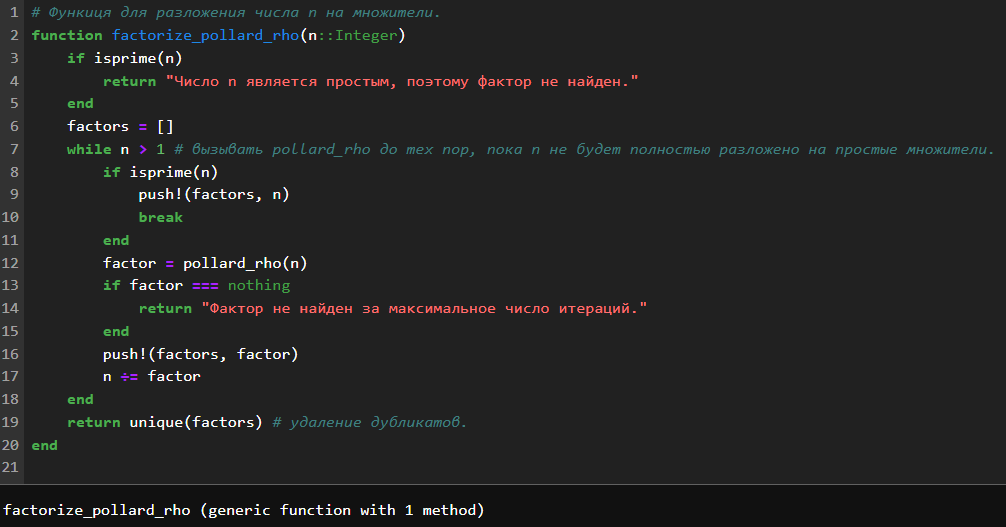
# Ход работы

## Функция p-метод Полларда



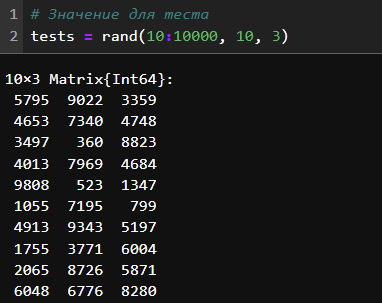
Функция p-метод Полларда и библиотека для простых чисел

## Функция разложения и проверки числа n

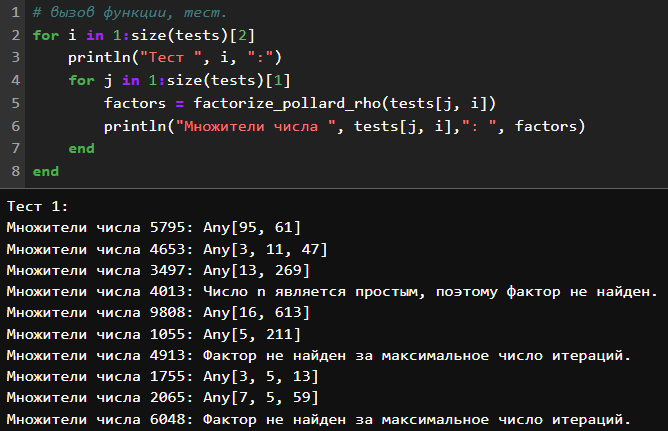


Функция разложения и проверки числа n

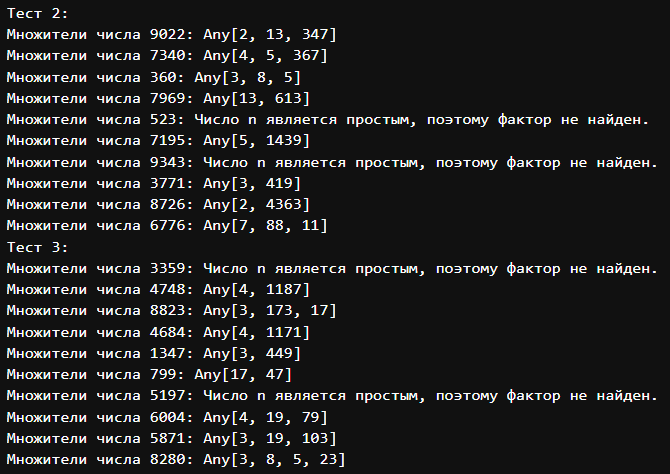
## Результаты



Тестовые значения



Вызов функции и тестовая группа 1



тестовая группа 2 и тестовая группа 3

# Выводы по проделанной работе

## Вывод

В ходе выполнения лабораторной работы я изучил способ нахождение всех множителей числа алгоритмом реализующим p-метод Полларда.

# Список литературы

1. [Глава 2. Факторизация целых чисел с экспоненциальной сложностью](https://studfile.net/preview/2439346/page:7/)
2. [P-1 метод Полларда](https://algolist.ru/maths/teornum/factor/p-1.php)
3. [Оптимизация (p — 1)-алгоритма Полларда Климина Александра Сергеевна](https://cyberleninka.ru/article/n/optimizatsiya-p-1-algoritma-pollarda)
4. [Факторизация Целых Чисел](https://habr.com/ru/sandbox/163811/)