Информационная безопасность. Отчет по лабораторной работе № 6

Разложение чисел на множители

Мухамеджанов Исматулло Иззатуллоевич

Содержание

# 1 Цель работы

Освоить на практике применение разложения числа на множители.

# 2 Указание к работе

Метод Полларда Факторизация числа

# 3 Выполнение лабораторной работы

1. Метод Полларда

Вход. Число п, начальное значение с, функция f, обладающая сжимающими свойствами. Выход. Нетривиальный делитель числа п.

Положить п ‹= с, b ‹=- С. Вычислить п +- f{а) mod п), b ‹= f(b) (mod п) Найти d ‹= Н0Д(п — b, n). Если 1 < d < п, то положить р +- d и результат: р. При d —— п результат: Делитель не найден»; при d —— 1 вернуться на шаг 2.

1. Факторизация числа

Метод кеадратов. (Teope.ha Фер.›іа о разло,жении) Для любого положительного нечетного числа п существует взаимно однозначное соответствие между множеством делителей числа п, не меньших, чем , и множеством пар is, fi} таких неотрицательных целых чисел, что п = s 2 — fi2.

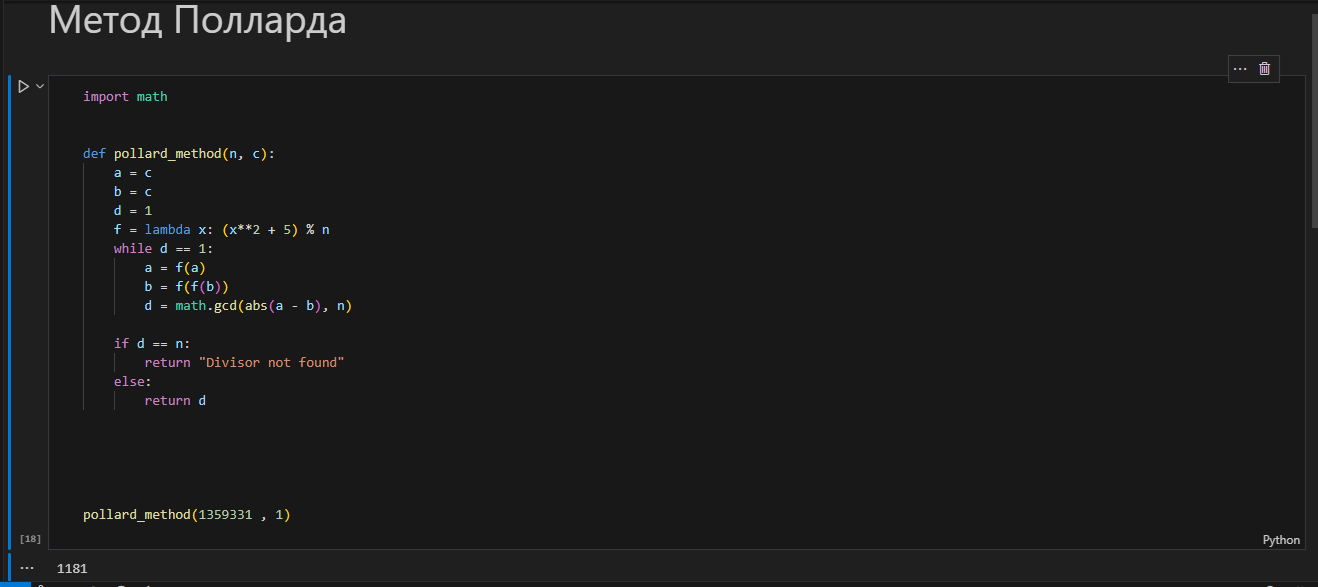


Figure 1: Программа (1)

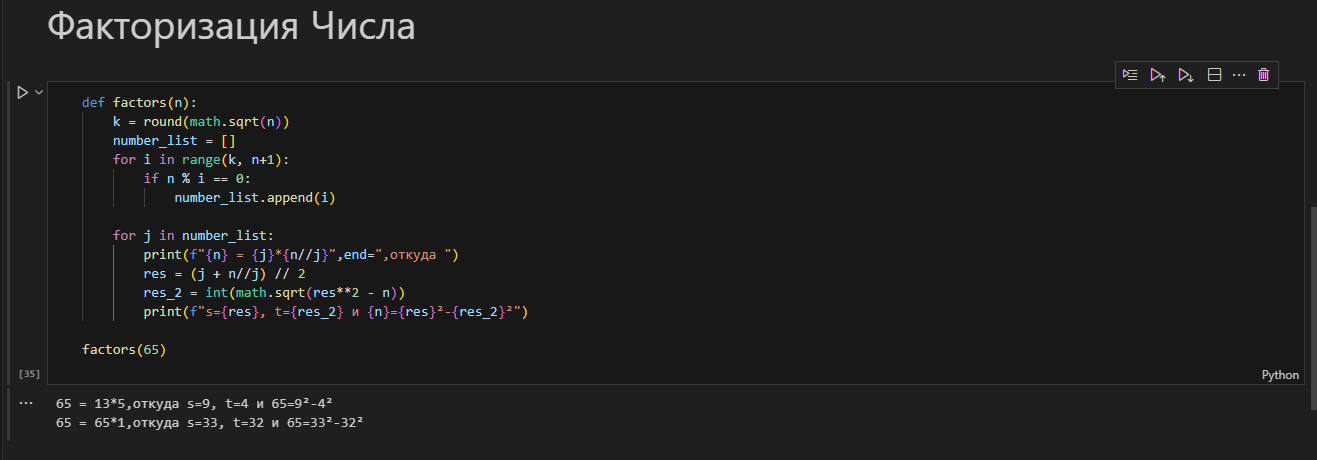


Figure 2: Программа (2)

# 4 Выводы

Освоены методы разложения чисел на множители

# 5 Список литературы

1. Методические материалы курса