Отчёт по лабораторной работе №6 Математические основы защиты информации и информационной безопасности

Разложение чисел на множители

Выполнил: Мануэл Марсия Педру,
НФИмд-02-25, 1032255503

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Изучить алгоритм разложения чисел на множители и научиться его реализовывать.

2 Выполнение лабораторной работы

2.1 Реализация вычисления символа Якоби

Ро-алгоритм — предложенный Джоном Поллардом в 1975 году алгоритм, служащий для факторизации (разложения на множители) целых чисел. Данный алгоритм основывается на алгоритме Флойда поиска длины цикла в последовательности и некоторых следствиях из парадокса дней рождения. Алгоритм наиболее эффективен при факторизации составных чисел с достаточно малыми множителями в разложении.

Выполним реализацию этого алгоритма на языке Julia (рис. 2.1 - рис. 2.6):

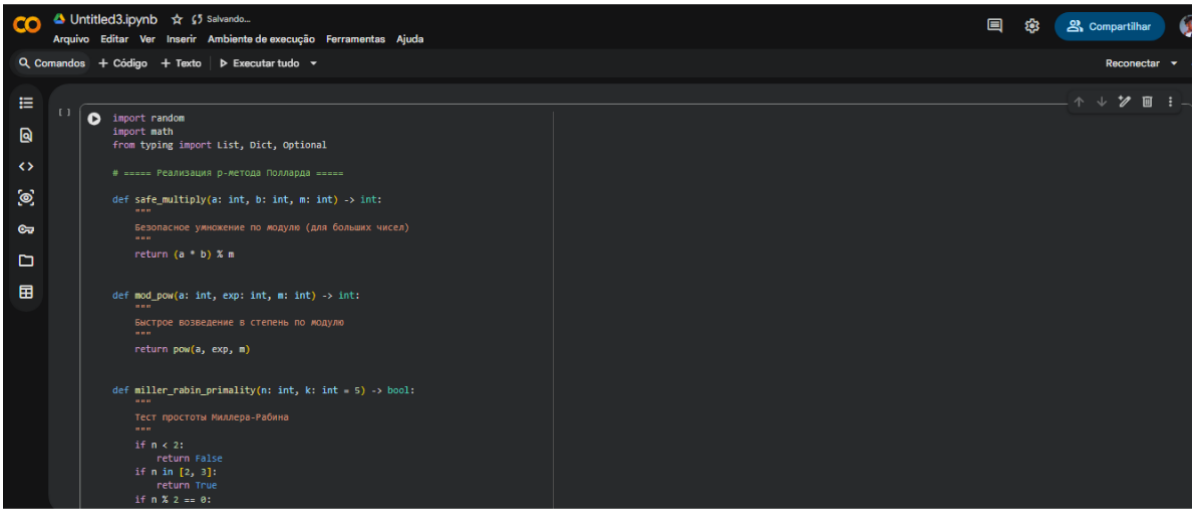

Рис. 2.1: Реализация p-Метода Полларда

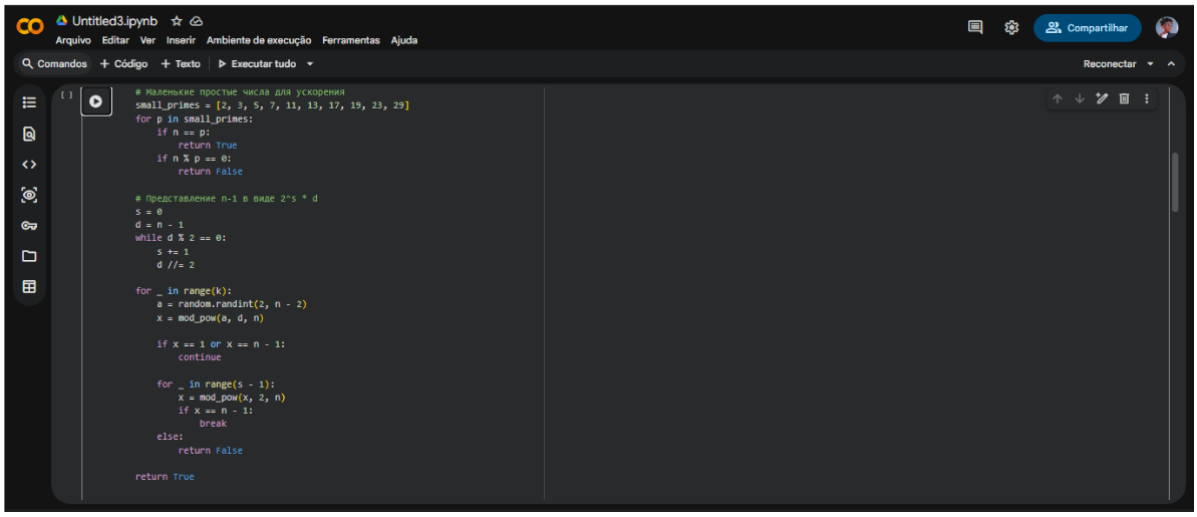

Рис. 2.2: Реализация p-Метода Полларда

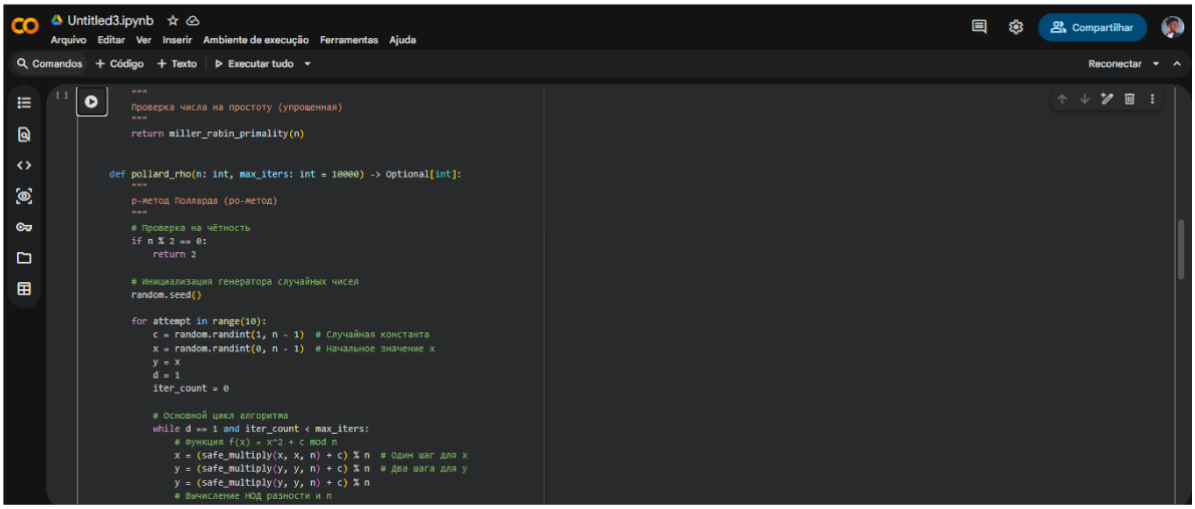

Рис. 2.3: Реализация p-Метода Полларда

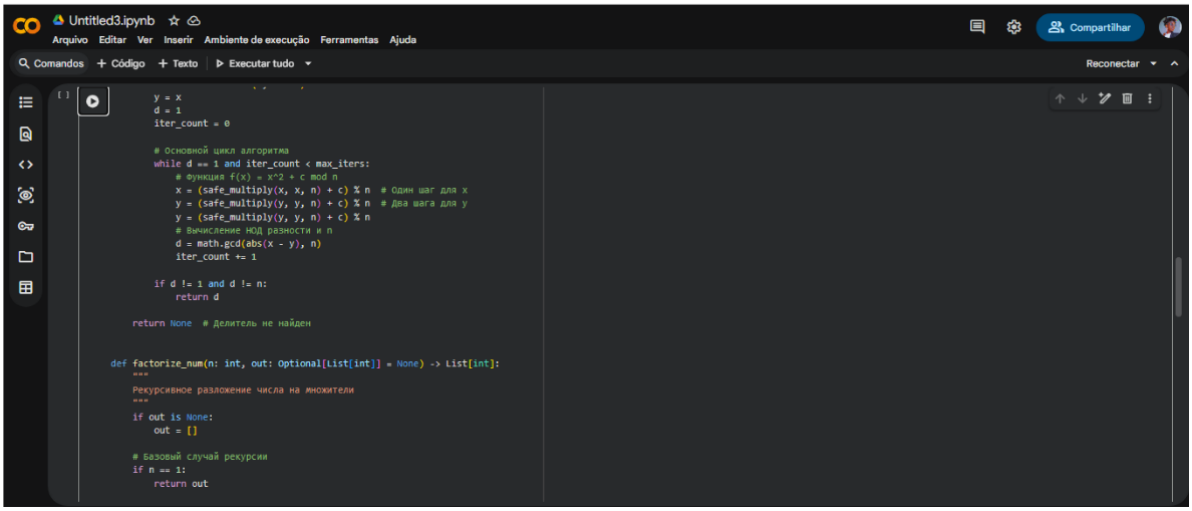

Рис. 2.4: Реализация p-Метода Полларда

Реализация p-Метода Полларда

Рис. 2.5: Реализация p-Метода Полларда

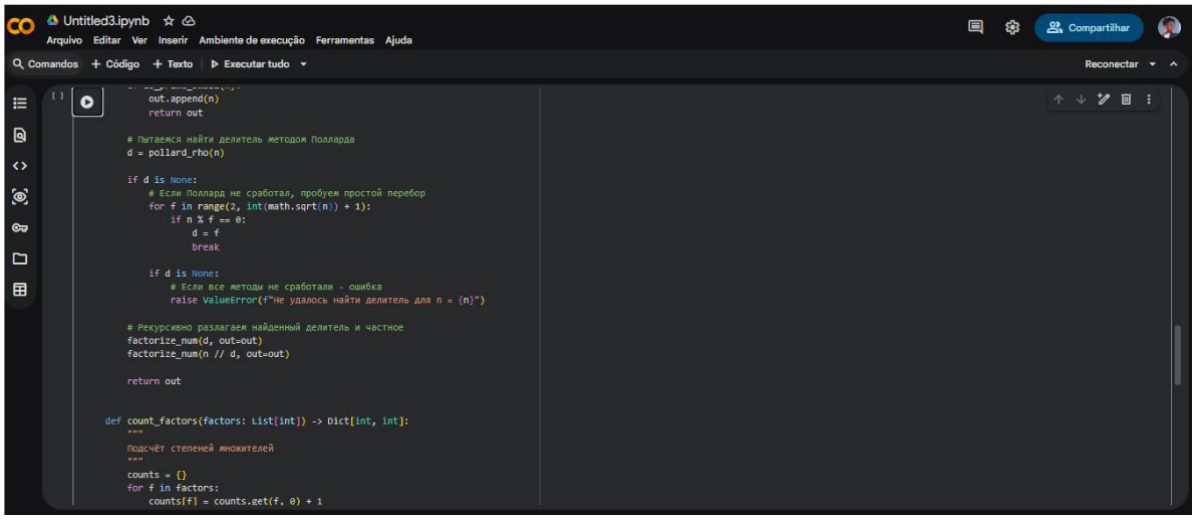

Рис. 2.6: Реализация p-Метода Полларда

Проверим работу алгоритма (рис. 2.7):

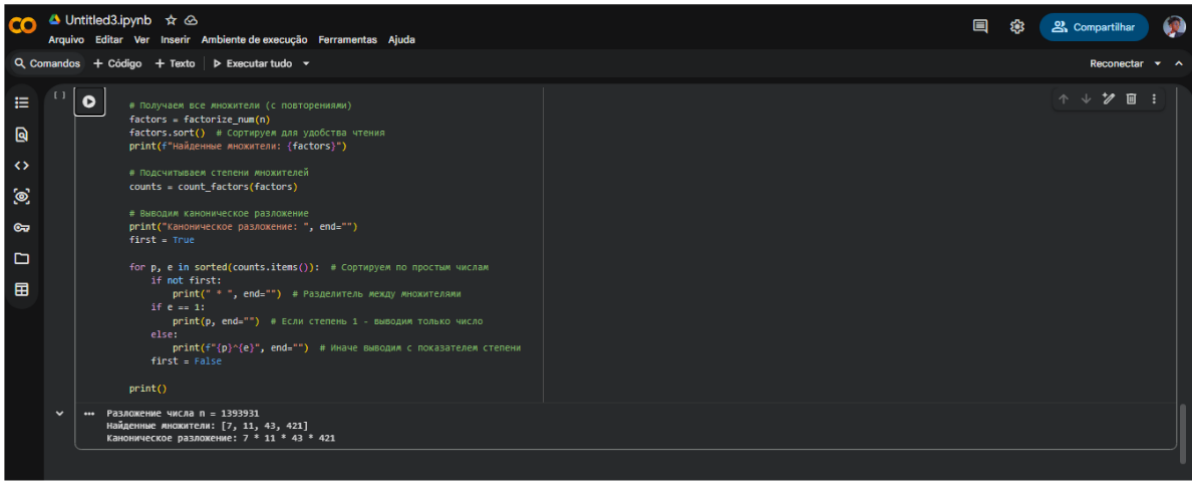

Рис. 2.7: Проверка

3 Список литературы. Библиография