Отчет по лабораторной работе №5

Вероятностные алгоритмы проверки чисел на простоту

Бармина Ольга Константиновна

2024 September 7th

Содержание

# 1 Цель работы

Цель данной работы: научиться реализовывать алгоритмы проверки чисел на простоту.

# 2 Задание

1. Реализовать алгоритмы проверки чисел на простоту.

# 3 Теоретическое введение

Пусть а - целое число. Числа ‡1, ‡а называются тривиальными делителями числа а. Целое число р €Z/{0) называется простым, если оно не является делителем единицы и не имеет других делителей, кроме тривиальных. В противном случае число p €Z/{-1, 0, 1) называется составным.

# 4 Выполнение лабораторной работы

1. Прописываем функцию для алгоритма теста Ферма (рис. fig. 1).

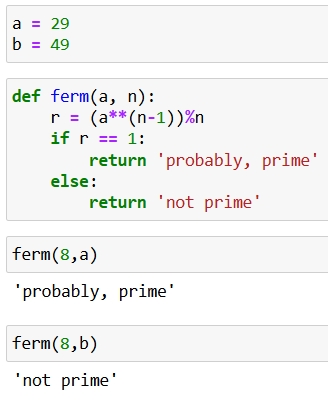


Figure 1: Программная реализация алгоритма теста Ферма.

1. Прописывается функция для алгоритма вычисления символа Якоби. (рис. fig. 2).

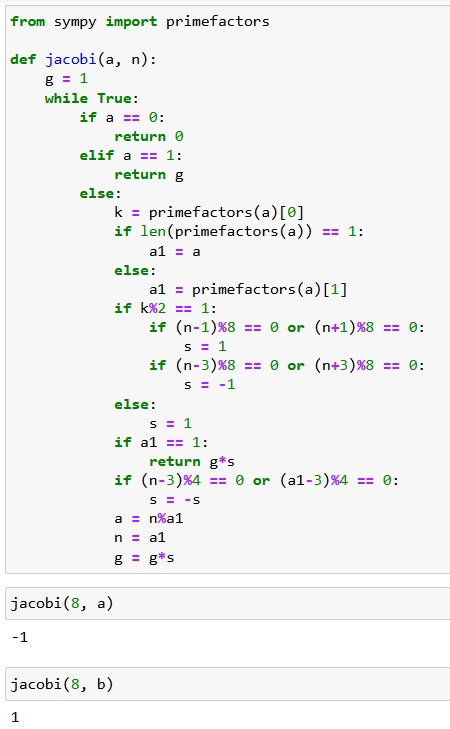


Figure 2: Алгоритм вычисления символа Якоби

1. Программная реализация алгоритма Соловэй-Штрассена. (рис. fig. 3).

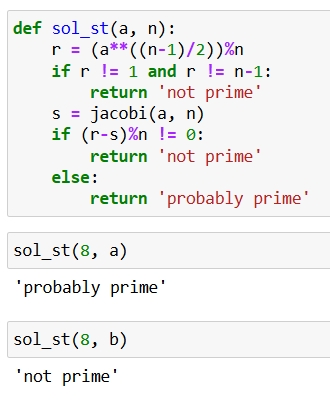


Figure 3: Программная реализация алгоритма Соловэй-Штрассена

1. Программная реализация алгоритма Миллера-Рабина. (рис. fig. 4).

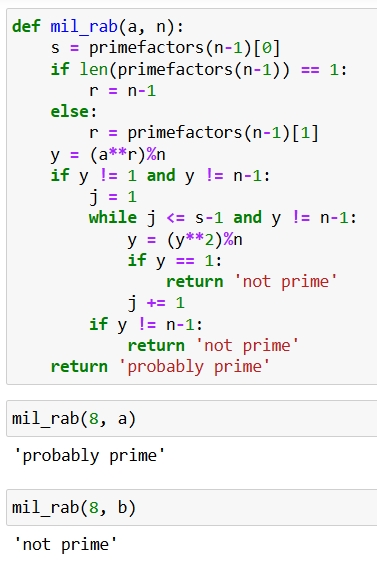


Figure 4: Программная реализация алгоритма Миллера-Рабина.

# 5 Выводы

В ходе работы были реализованы алгоритмы проверки чисел на простоту.

# 6 Список литературы

1. Методические материалы курса