Математические основы защиты информации и информационной безопасности.

Лабораторная работа №5.

Подмогильный Иван Александрович.

Содержание

# 1 Цель работы

Освоить на практике вероятностные алгоримты проверки чисел на простоту

# 2 Задание

1. Реализовать алгоритм теста Ферма
2. Реализовать вычисления символа Якоби
3. Реализовать алгоритм теста Соловэя-Штрассена
4. Реализовать алгоритм теста Миллера-Рабина

# 3 Выполнение лабораторной работы

Написал код для вычисления теста Ферма. Все функции реализованы шаблонами:

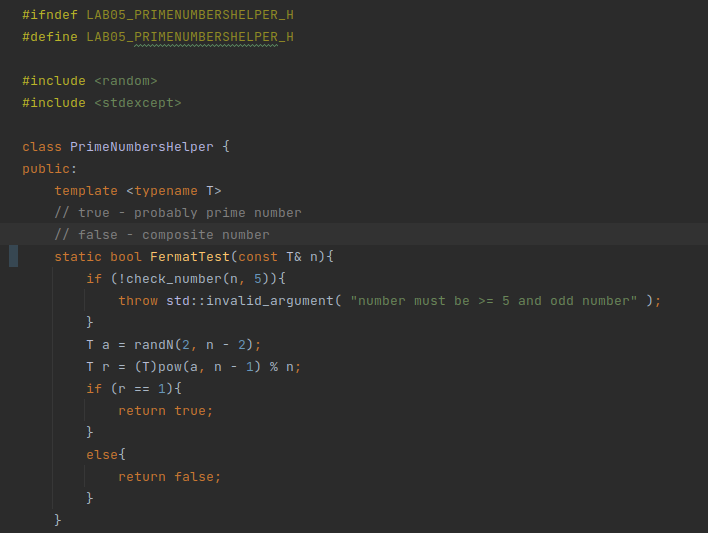


Figure 1: Функция теста Ферма

Написал код для вычисления теста Соловэя-Штрассена.

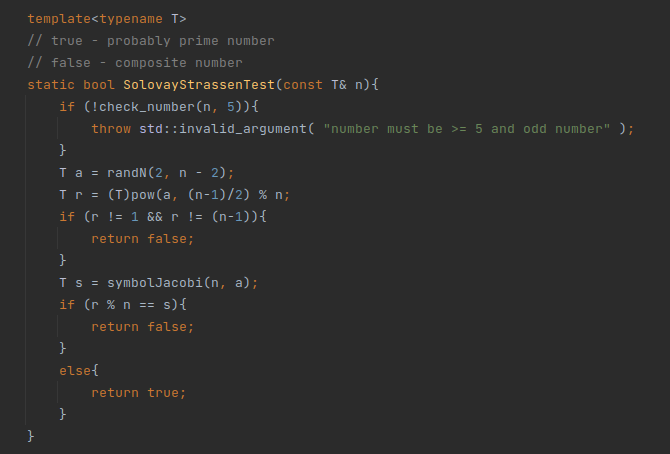


Figure 2: Функция теста Соловэя-Штрассена

Реализовал вычисление теста Миллера-Рабина

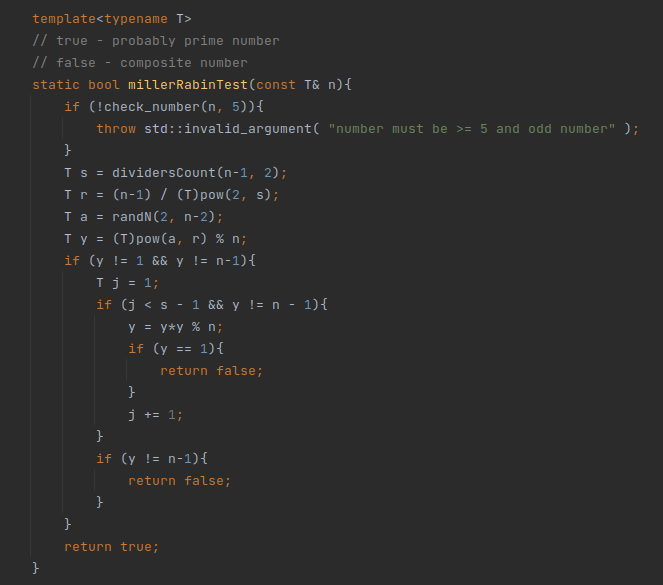


Figure 3: тест Миллера-Рабина

Реализовал вспомогательную функцию вычисления случайного числа

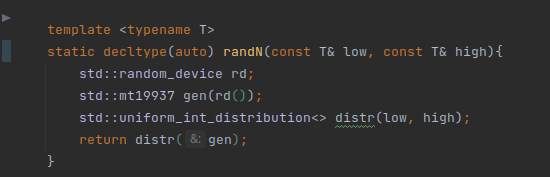


Figure 4: Вспомогательная функция вычисления случайного числа

Написал вспомогательную функцию вычисления символа Якоби

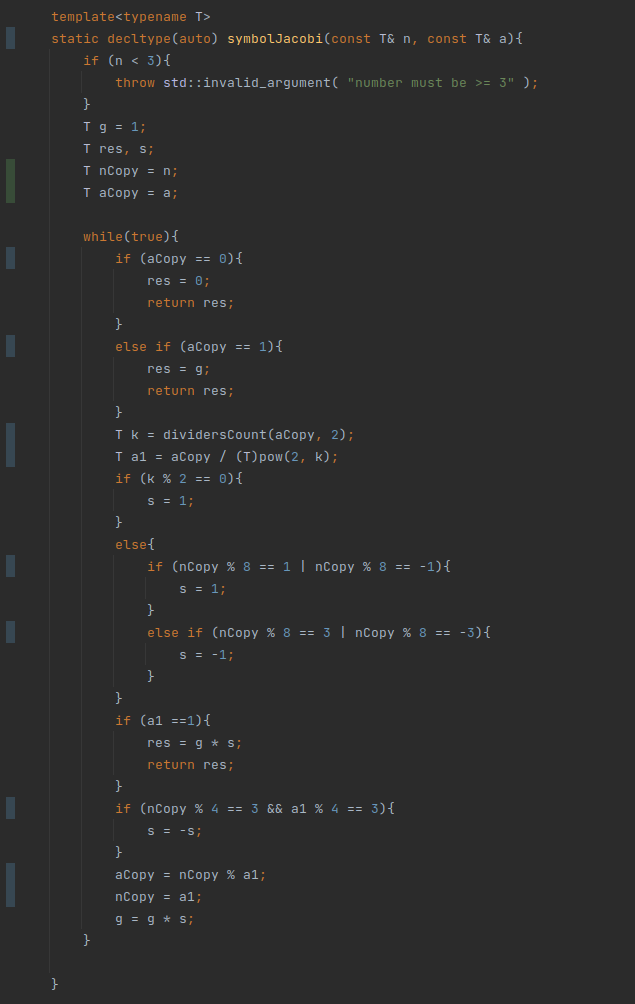


Figure 5: Вспомогательная функция вычисления символа Якоби

Написал вспомогательную функцию подсчета делителей divider в числе n

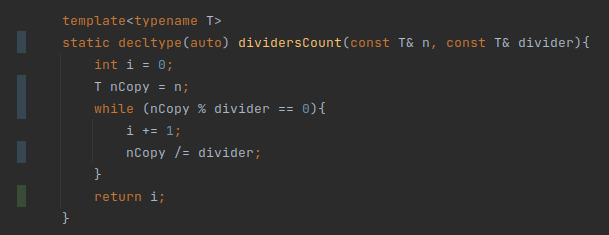


Figure 6: Вспомогательная функция подсчета делителей

Написал вспомогательную функцию проверки числа (она используется в начале каждой функции)

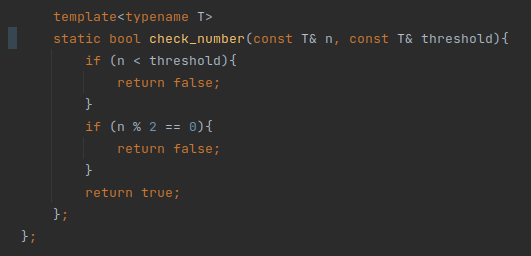


Figure 7: Вспомогательная функция проверки числа

Написал CMake файл

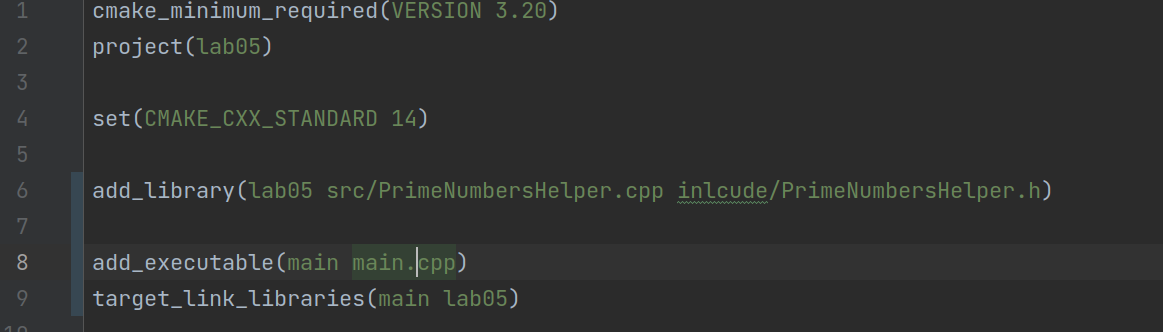


Figure 8: CMake файл

Написал main.cpp файл, в котором есть тесты реализованных функций.

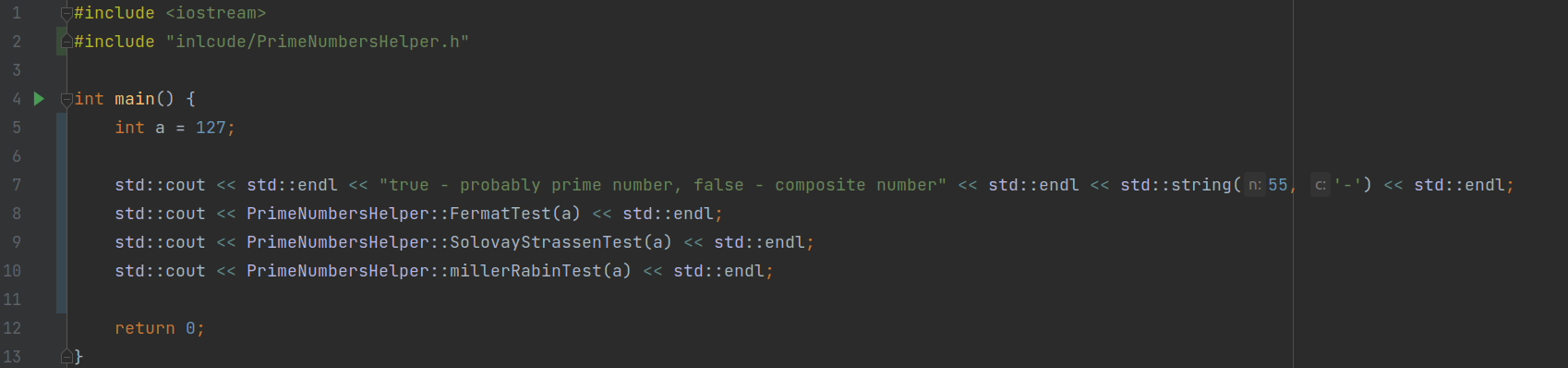


Figure 9: main.cpp файл

Результаты тестов.

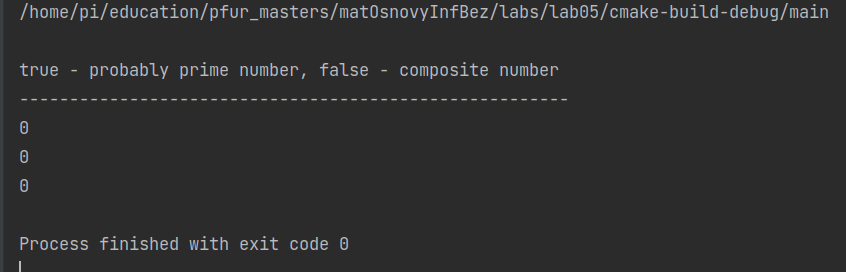


Figure 10: Результаты тестов

# 4 Выводы

Освоил на практике вероятностные алгоримты проверки чисел на простоту