УДК 511.1

Студ. Е.И. Харченко, А.В. Собаль
Науч. рук. доц. Е.И. Ловенецкая
(кафедра высшей математики, БГТУ)

ОПРЕДЕЛЕНИЕ ПРОСТОТЫ ЧИСЕЛ МЕРСЕННА

Числа Мерсенна, имеющие вид $M_p = 2^p - 1$, где p – простое число, представляют особый интерес в математике и криптографии, поскольку среди них регулярно обнаруживаются рекордно большие простые числа. Несмотря на существование эффективного теста Люка-Лемера, проверка простоты чисел Мерсенна весьма трудоемка из-за огромной величины исследуемых чисел.

Целью работы является изучение практической применимости критерия Люка-Лемера для проверки простоты чисел Мерсенна и анализ временных затрат алгоритма.

Для проверки чисел Мерсенна был написан код на Python, реализующий критерий Люка-Лемера с использованием библиотеки «gmpy2», которая может обрабатывать большие числа почти на уровне аппаратной скорости. Программа проверяет простоту показателя p, вычисляет $M_p = 2^p - 1$ и проводит итерационный тест, замеряя время выполнения. Особое внимание уделено оптимизации операций по модулю M_p, так как именно они определяют общую производительность алгоритма при работе с гигантскими числами.

Проведение серии вычислений для различных значений p позволило выявить характер зависимости времени выполнения теста от величины показателя.

На графике (рис. 1) четко прослеживается резкий рост временных затрат с увеличением p, что соответствует теоретическим оценкам сложности алгоритма.

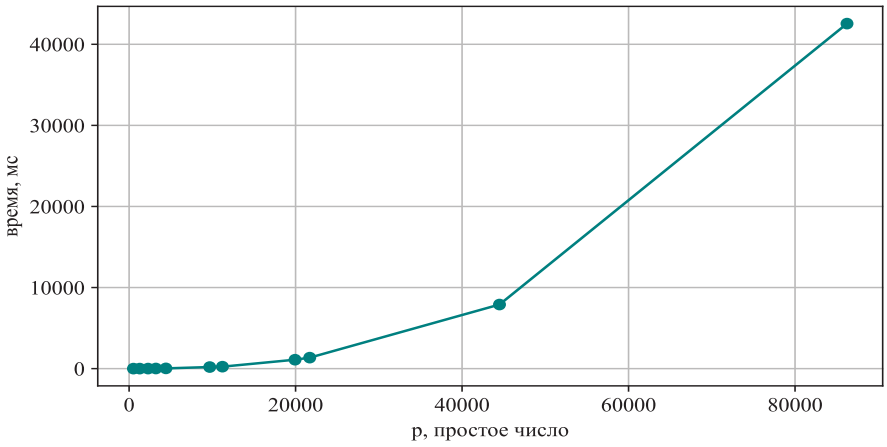

Рисунок 1 – Зависимость времени выполнения теста Люка-Лемера от p