2. Kudykina T. Rotation Curves of the Cosmic Objects and Attractive Force in the Universe // Mediterranean Journal of Physics. – 2016, 1(1). – P. 32-36.

3. Бейтмен Г., Эрдейи А. Высшие трансцендентные функции. Функции Бесселя, функции параболического цилиндра, ортогональные многочлены. – М., «Наука». 1974. – 296 с.

УДК 511.2/.3

Студ. Н.М. Гулевич, Т.И. Гулешов
Науч. рук. доц. Е.И. Ловенецкая (кафедра высшей математики, БГТУ)

ФАКТОРИЗАЦИЯ НАТУРАЛЬНЫХ ЧИСЕЛ

Факторизация натуральных чисел – одна из ключевых задач теории чисел, заключающаяся в разложении числа на простые множители. Эта задача имеет важное значение в криптографии, в частности в алгоритме RSA, где безопасность основана на вычислительной сложности факторизации больших чисел. Алгоритм RSA использует пару ключей: открытый для шифрования и закрытый для расшифровки, причем нахождение закрытого ключа по открытому требует факторизации произведения двух больших простых чисел.

В данной работе рассмотрены три алгоритма факторизации: метод перебора делителей, алгоритм Ферма и ρ-метод Полларда. Метод перебора делителей проверяет все возможные делители до квадратного корня числа. Алгоритм Ферма использует представление числа как разности квадратов. Метод Полларда основан на вероятностном подходе, эффективность зависит от выбранной функции. Были реализованы указанные алгоритмы, проведено сравнение их производительности на числах разной величины и структуры. Метод перебора делителей наиболее эффективен для относительно небольших чисел. Алгоритм Ферма эффективен, когда число можно представить как разность квадратов двух чисел, близких по значению. ρ-метод Полларда, будучи вероятностным, показывает высокую эффективность для чисел с умеренно большими множителями. Изучались также некоторые модификации алгоритмов: метод Ферма получил обратную реализацию, метод Полларда – множество реализаций с различными внутренними функциями. Результатом работы является программа на языке Python, позволяющая выполнять факторизацию натуральных чисел с использованием алгоритма перебора (до 10 000), далее применяющая алгоритмы Ферма и Полларда параллельно, что позволяет пользоваться преимуществами всех алгоритмов для поиска делителей одновременно.

ЛИТЕРАТУРА

1. Кнут, Д.Э. Искусство программирования. Том 2: Получисленные алгоритмы / Д.Э. Кнут. – М.: Вильямс, 2018.