**Факторизация целых чисел методом квадратичного решета.**

Гамов П.А.

Научный руководитель —Ухов П.А.

МАИ, Москва

Факторизацией натурального числа называется разложение этого числа в произведение простых сомножителей. Эта задача имеет большую вычислительную сложность. Один из самых популярных методов криптографии с открытым ключом, метод RSA, основан на трудоемкости задачи факторизации длинных целых чисел. [1]

Первым серьёзным прорывом было квадратичное решето, quadratic sieve (QS). Это относительно простой алгоритм факторизации, предложенный Carl Pomerance в 1981 г., который может разлагать на множители числа до 110 десятичных разрядов или около того и для таких чисел остается лучшим. [2]

Решение задачи факторизации имеет прикладное значение, так как ставит под сомнение безопасность шифровальных алгоритмов, на которых строится современная криптография. Метод квадратичного решета является вторым по скорости факторизации чисел, его обгоняет только метод общего решета числового поля. Принцип работы алгоритма квадратичного решета основана на идее факторизации Ферма – поиске двух чисел, которые являются полными квадратами по модулю искомого числа. Нахождение таких чисел ставит перед нами необходимость долгого поиска необходимой факторной базы, гладких чисел, решение достаточно большой разряженной матрицы в конечном числовом поле.

Работа состоит в исследовании и реализации метода квадратичного решета, сравнении его с другими существующими алгоритмами, подборе оптимальных начальных условий, необходимых для ускорения алгоритма. Так же в исследовании различных способов решения разряженных матриц, алгоритмов поиска больших простых чисел.

Понимание этого алгоритма является фундаментальным, он лежит в основе понимания более тяжелых алгоритмов, которые способны факторизовать числа, длинною более ста цифр.

Список использованных источников:

1. Ишмухаметов Ш. Т. Методы факторизации натуральных чисел: учебное пособие. — Казань: Казан. ун., 2011.
2. И. В. Агафонова Факторизация больших целых чисел и криптография.