**Факторизация целых чисел методом квадратичного решета.**

Гамов П.А.

Научный руководитель —Ухов П.А.

МАИ, Москва

Существует такая категория задач, которая занимается поиском лучших путей факторизации чисел. Данный раздел математики имеет прикладное значение, так как ставит под сомнение безопасность различных шифровальных алгоритмов, на которых строится современная криптография. Новые алгоритмы стремятся поставить под сомнение надежность современных методов шифрования. Моя работа состоит в объяснении достаточно сложного, но не менее красивого алгоритма факторизации целых чисел.

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.

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

Моя работа ставит перед собой введение в математическую составляющую данного алгоритма, объяснения основ. Так же в планах – нахождения оптимальных размер факторных баз, улучшения скорости алгоритма, так как его возможно запускать на многих ядрах и даже процессорах.

Список использованных источников:

1. Carl Pomerance, Analysis and Comparison of Some Integer Factoring Algorithms, in Computational Methods in Number Theory, Part I, H.W. Lenstra, Jr. and R. Tijdeman, eds., Math. Centre Tract 154, Amsterdam, 1982, pp 89-139.
2. Pomerance, Carl. A Tale of Two Sieves (декабрь 1996), С. 1473–1485.
3. Ишмухаметов Ш. Т. Методы факторизации натуральных чисел: учебное пособие. — Казань: Казан. ун., 2011. — 190 с.
4. Нестеренко А. Введение в современную криптографию.Теоретико-числовые алгоритмы. — 2011. — 190 с.
5. Дональд Кнут. Искусство программирования, том 2. Получисленные методы = The Art of Computer Programming, vol.2. Seminumerical Algorithms. — 3-е изд. — М.: «Вильямс», 2007. — 832 с. — ISBN 5-8459-0081-6.
6. K. Lenstra, H. W. Lenstra (1993), The Development of the Number Field Sieve, Springer, ISBN 9783540570134
7. И. В. Агафонова Факторизация больших целых чисел и криптография.