МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М.В. ЛОМОНОСОВА

МЕХАНИКО - МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

ОТЗЫВ НА ДИПЛОМНУЮ РАБОТУ

студентки 5 курса Новиковой Александры Николаевны
Руководитель: чл.-корр. РАН Нестеренко Ю.В.
Тема: Об алгоритме Шнорра факторизации целых чисел.

Как известно, задача разложения целых чисел на множители очень сложна в вычислительном отношении. На этом основано её применение в криптографии. Наиболее совершенный алгоритм просеивания в числовых полях требует $O(e^{c\ln^{1/3}N\ln\ln^{2/3}N})$ арифметических операций для разложения на множители числа N. Поэтому задача создания новых более эффективных алгоритмов разложения чисел на множители является актуальной и важной для приложений.

В дипломной работе А.Н. Новиковой изучается новый алгоритм факторизации, предложенный в 2013г. К.П. Шнорром. Нужно отметить, что работа Шнорра не завершена, а то что опубликовано, написано не очень хорошо. Поэтому попытки разобраться с идеями автора и изложить их на понятном математическом языке требуют достаточно напряженных усилий. Именно эта задача и была поставлена А.Н. Новиковой в дипломной работе.

Алгоритм Шнорра разложения чисел на множители состоит из двух этапов. На первом задача разложения сводится к построению некоторой решётки в пространстве достаточно большой размерности и поиску в этой решётке векторов близких к заданному вектору, зависящему от N. Второй этап связан именно с поиском близких векторов решётки. В дипломной работе рассматривается только первая часть алгоритма. К сожалению алгоритм в целом оказался слишком сложным для понимания.

А.Н. Новикова, основываясь на двух работах Шнорра, восстановила некоторые детали доказательств в первой части алгоритма. Она проделала достаточно большую работу. К сожалению, на изучение второй части алгоритма у неё не хватило времени. Я полагаю, что дипломная работа заслуживает оценку хорошо.

Ю.В. Нестеренко

чл.-корр. РАН Ю.В.Нестеренко