Московский Государственный Университет имени М.В. Ломоносова

Механико-математический факультет

ОТЗЫВ НА ИТОГОВУЮ КВАЛИФИКАЦИОННУЮ (ДИПЛОМНУЮ) РАБОТУ

**Студент** 6 курса 610 группы, кафедра теории чисел,

Щемелёва Анна Михайловна.

**Научный руководитель** Нестеренко Юрий Валентинович.

**Тема:** Об одном алгоритме перебора точек решётки.

В настоящее время наиболее эффективным алгоритмом разложения целых чисел на простые множители является метод просеивания в числовых полях. Одним из наиболее трудоёмких этапов его классической реализации (Поллард, Фрикке, Кляйнюнг) является поиск гладких чисел вида . Здесь  – фиксированное выбранное специальным способом целое алгебраическое число,  – целые рациональные с заданными ограничениями на их величину. Гладкими же называются алгебраические числа из поля ***Q***(), норма которых раскладывается в произведение сравнительно небольших простых чисел. Поиск чисел вида с нормой, делящейся на фиксированное не очень большое простое p, сводится к перечислению точек некоторой решётки. Если p не делит индекс кольца в кольце всех целых чисел поля ***Q()*** и простой идеал лежит над  , то множество пар a,b с условием образует решетку в , причём если 𝔭 – идеал первой степени, то ее базис составляют вектора  Эффективное перечесление точек этой решётки и составляет процесс просеивания. Точно так же множество точек образует решётку в с базисом , а числа v, uопределены равенством 𝔭=(p, ).

Двумерные решётки сейчас используются в алгоритмах разложения больших чисел на множители. Идея использовать простые идеалы второй степени и соответствующие им трёхмерные решётки возникла сравнительно недавно, и в теоретическом плане она пока не проработана. В использовании двумерных решёток важную роль играют цепные дроби, с их помощью строится так называемый приведённый базис. А он служит в дальнейшем для перечисления точек решётки. Целью дипломной работы было исследование возможности использования алгоритма Минковского, представляющего собой трёхмерное обобщение алгоритма цепных дробей, для построения алгоритма перечисления точек трёхмерной решётки. Во второй части дипломной работы А.Щемелёвой достаточно подробно излагается алгоритм просеивания двумерных решёток. Здесь акцент делается на испольцование цепных дробей и восстанавливаются некоторые детали, опущенные ради краткости в работе Фрикке и Кляйнюнга. Третья часть посвящена подробному изложению алгоритма Минковского. Задача построения алгоритма просеивания на этой основе оказалась достаточно сложной и А. Щемелёвой не хватило времени на построение соответствующего алгоритма. Тем не менее хотел бы отметить, что она выполнила большую подготовительныю работу, и исследования на этой основе могут быть продолжены. А. Щемелёва относилась к написанию дипломной работы очень серьёзно. Я полагаю, что дипломная работа заслуживает оценку «отлично».

Профессор

Ю.В. Нестеренко