ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА

на диссертацию Зеленовой Марии Евгеньевны
"Решение систем уравнений в полях алгебраических чисел",
представленную к защите в диссертационный совет Д 501.001.84
на соискание ученой степени кандидата физико-математических
наук по специальности 01.01.06 — математическая логика, алгебра и теория чисел

Основные результаты диссертации М.Е. Зеленовой посвящены построению алгоритмов решения полиномиальных уравнений и систем в полях алгебраических чисел, основанных на лемме о подъеме решения полиномиального сравнения.

Полученные результаты основаны на идеях подъема решения полиномиального сравнения, впервые высказанные К. Гензелем в 1904г. Позднее, в 1969г. Г. Цассенхауз модифицировал алгоритм подъема решения таким образом, чтобы скорость приближения к решению стала экспоненциальной. В 1982г. идея Гензеля была использована А.К. Ленстрой, Х.В. Ленстрой и Л. Ловасом при построении алгоритма факторизации многочленов с целыми коэффициентами (так называемый LLL-алгоритм). В 1982г. Д.Д. Диксон сформулировал алгоритм нахождения рациональных решений целочисленной квадратной линейной системы уравнений. Он в явном виде выписал формулы, позволяющие из решения системы сравнений по модулю p получить решения по модулю p^k. В 1993г. подъем решения сравнения использовали Д. Бухлер, Х.В. Ленстра, и К. Померанс при разработке алгоритма извлечения квадратного корня в порядке $\mathbb{Z}(\omega)$ поля алгебраических чисел, где w — целое алгебраическое число степени d. В настоящей диссертации описан алгоритм, обобщающий метод Д. Бухлера, Х.В. Ленстры и К. Померанса на многочлены произвольной степени с коэффициентами, лежащими в произвольном порядке порядке поля алгебраических чисел.

Приведенные факты показывают актуальность темы диссертационной работы М.Е. Зеленовой.

Во введении дается общая характеристика работы, обосновывается актуальность темы диссертации, освещаются цели и методы исследования, выносимые на защиту результаты, дается обзор содержания диссертации и сведения о ее апробации.

В первой главе описываются алгоритмы 1.1 и 1.2 решения полиномиальных уравнений в произвольном порядке поля алгебраических чисел и дается их полное обоснование. В алгоритме 1.1 осуществляется экспоненциальный подъем решения по модулям p^{2^k}, где p — изначально выбираемое простое число с некоторым набором ограничений. Формулы для итерационного подъема решения выписаны явно и, что хочется отметить, не содержат операций деления. Дана оценка на количество шагов в подъеме в зависимости от коэффициентов многочлена, определяющего уравнение, и порядка, в котором ищем решение. В ходе алгоритма 1.1 возникает многочлен $\overline{\mu_\omega(x)}(p)$, к которому предъявляется требование неприводимости. Не приведено оценки, как быстро такой

многочлен можно построить, и сам факт существования такого многочлена полностью не обоснован в диссертации. Но этот вопрос полностью снимает алгоритм 1.2, который позволяет отказаться от требования неприводимости многочлена $\overline{\mu_\omega(x)}(p)$. При этом на практике можно применять оба алгоритма, поскольку если они находят решение, то оно является решением.

Во второй главе описываются два алгоритма — алгоритм 2.1 нахождения рациональных решений неоднородной системы уравнений с целыми коэффициентами и алгоритм 2.2 нахождения целых решений соответствующей однородной системы. Алгоритм основан на экспоненциальном подъеме решения по модулям p^{2^k} простого числа p. Приведены необходимые сведения из теории полиномиальных идеалов. Выписаны явные итерационные формулы для подъема решения. Еще одним основополагающим результатом второй главы является оценка модуля решения системы полиномиальных уравнений нулевой размерности, полученная с помощью теории полиномиальных идеалов.

Указанные выше замечания не влияют на высокую оценку диссертации в целом. Все основные результаты диссертации являются новыми, снабжены достоверными доказательствами и своевременно опубликованы. В диссертации применяются методы коммутативной алгебры и методы построения решений в полях p-адических чисел с помощью подъема по степеням простых идеалов. Результаты диссертации прошли необходимую апробацию, имеют теоретическое значение и определенно найдут применения в области алгоритмической и алгебраической теории чисел.

Диссертация содержит 90 страниц, состоит из введения, двух глав и списка литературы из 31 источника, в том числе 3 публикаций автора, две из которых опубликованы в журналах из перечня ВАК. Автореферат диссертации полностью соответствует ее содержанию.

Диссертация М.Е.Зеленовой является завершенной научно-квалификационной работой.

Считаю, что диссертация удовлетворяет всем требования ВАК, предъявляемым к диссертациям на соискание ученой степени кандидата физико-математических наук, а ее автор Мария Евгеньевна Зеленова заслуживает присуждения ученой степени кандидата физико-математических наук по специальности 01.01.06 — математическая логика, алгебра и теория чисел.

Кандидат физико-математических наук по специальности 01.01.06 — математическая логика, алгебра и теория чисел, руководитель проекта, ООО "ГТК СЕРВИС", рабочий адрес: 127055, г. Москва, ул. Новослободская, д. 36/1, строение 1, помещение 1, комната 6, тел. 8 (800) 505-89-02, +7 (495) 109-0-700, email: serjikk@gmail.com.

Сергей Владимирович Михайлов

3 декабря 2015г.