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

Диссертация посвящена вычислительным проблемам теории чисел, связанных с разработкой эффективных алгоритмов подъема локальных решений систем полиномиальных уравнений до соответствующих решений рассматриваемых систем в объемлющих глобальных полях.

Решение полиномиальных уравнений в различных полях и кольцах является одной из классических задач алгебры и теории чисел. Среди многочисленных методов решения этой задачи следует выделить наиболее эффективный метод связанный с подъемом локальных решений системы полиномиальных уравнений по модулю некоторого простого идеала до соответствующего глобального решения рассматриваемой системы. Исходную идею указанного подъема впервые описал К. Гензель в 1904 г. на основе введенного им в рассмотрение понятия p - адического числа. Позже в 1968 г. первоначальный подход Гензеля был несколько модифицирован Г. Цассенхаузом, сделав предложенный Гензелем алгоритм экспоненциальным. В дальнейшем (1982) подход Гензеля был использован А. Ленстрой, Х. Ленстрой и Л. Ловасом для создания знаменитого быстрого алгоритма факторизации многочленов с целыми рациональными коэффициентами (LLL - алгоритма). Несколько позже подобный подход был использован Д. Диксоном для разработки быстрого алгоритма нахождения рациональных решений целочисленной квадратной линейной системы уравнений. Наконец, в 1993 г. предложенный Гензелем процесс подъема решения сравнения по $(\bmod p^k)$ был использован Д. Бухлером, Х. Ленстрой и К. Померансом для описания алгоритма извлечения квадратного корня в кольце целых чисел $\mathbb{Z}[\omega]$, где ω - целое алгебраическое число степени $d \geq 2$.

В первой главе диссертации указанный выше алгоритм Бухлера-Ленстры-Померанса расширен автором до общего случая многочленов произвольной степени с коэффициентами, лежащими в произвольном порядке поля алгебраических чисел. При этом указана итерационная формула, позволяющая производить подъем решений рассматриваемого полиномиального сравнения $f(x) \equiv 0(\bmod p)$ по модулю простого числа p до соответствующего решения по модулю p^{2^k}, где k - произвольное положительное целое число. Затем в диссертации указывается эффективная граница, до которой следует проводить подъем для того, чтобы найти точное решение исходного

полиномиального уравнения $f(x) = 0$ в изначально рассматриваемом порядке при условии, если таковое существует.

Во второй главе диссертационной работы автором предложен алгоритм нахождения неособых целых решений в произвольном заданном порядке поля алгебраических чисел полных алгебраических систем, состоящих из полиномиальных уравнений с однородными или неоднородными многочленами с целыми коэффициентами. Указанный алгоритм основан на найденной автором диссертации формуле подъема решений заданной полиномиальной системы сравнений с целыми коэффициентами по простому модулю p до решения рассматриваемой системы по модулю p^{2^k} с произвольным положительным целым k. Указанная автором диссертации итерационная формула позволяет указать эффективную границу, до которой следует поднимать решения исследуемой системы сравнений для того, чтобы найти рациональное решения соответствующей полиномиальной системы уравнений.

Хорошо известно, что указанный выше метод подъема Гензеля является по сути дела дискретным аналогом классического метода касательных Ньютона. С другой стороны, указанный метод касательных Ньютона имеет соответствующий аналог в многомерном случае. Во второй главе диссертации автор значительно расширяет подход Гензеля и по аналогии с многомерным аналогом метода Ньютона в классической ситуации распространяет метод Гензеля на изучаемый в диссертации многомерный дискретный случай. В результате, автор указывает эффективный алгоритм нахождения решений однородных систем полиномиальных уравнений

$$P_i(x_0, x_1, \ldots, x_n) = 0, \quad i = 1, 2, \ldots, n.$$

в произвольных порядках полей алгебраических чисел. При этом автором приводится весьма простая итерационная формулу, позволяющая проводить подъем решений по модулю исходного простого числа p до соответствующего решения по модулю p^{2^k}. После этого указывается эффективная граница, до которой следует осуществлять подъем до получения требуемого точного решения исходного уравнения в заданном порядке.

В целом, диссертация посвящена актуальным вопросам современной теории чисел, имеющим большое практическое значение при решении серии трудных проблем дискретной математики, теории вычислений и криптографии. Результаты рассматриваемой диссертационной работы демонстрируют способность автора решать трудные задачи классической и современной теории чисел. Полученные в диссертации результаты свидетельствуют о высокой математической культуре и высоком профессиональном уровне автора. Все представленные в диссертационной работе результаты являются новыми, весьма интересными и вносящими существенный вклад в развитие современной теории чисел, а также ее вычислительных аспектов.

Диссертация содержит 90 страниц, состоит из введения, двух глав и списка литературы из 31 источника, в том числе трех публикаций автора, две из которых опубликованы в журналах из перечня ВАК. Автореферат диссертации довольно полно и четко отражает содержание диссертации и

полученные в ней результаты.

Диссертационная работа выполнена очень аккуратно. У рецензента имеется лишь одно замечание, касающихся используемой в диссертации терминологии. Именно, на стр. 4, а также при дальнейшем изложении, автор употребляет выражения "однородные полиномиальные системы"и "неоднородные полиномиальные системы". Рецензенту представляется, что в отличие от классического линейного случая, рассматриваемые автором диссертации системы уравнений уместнее называть системами однородных полиномиальных уравнений и, соответственно, системы неоднородных полиномиальных уравнений.

Исходя из изложенного считаю, что диссертационная работа М.Е. Зеленовой "Решение систем уравнений в полях алгебраических чисел"удовлетворяет всем требованиям ВАК, предъявляемым к диссертациям на соискание ученой степени кандидата физико-математических наук,а её автор заслуживает присуждения ей ученой степени кандидата физико-математических наук по специальности 01.01.06 - математическая логика, высшая алгебра и теория чисел.

Доктор физико-математических наук по специальности 01.01.06 — математическая логика, алгебра и теория чисел, ведущий научный сотрудник лаборатории №1 им. М.С. Пинскера ФГБУН Института Проблем Передачи Информации им. А.А. Харкевича Российской Академии Наук, рабочий адрес: 127051, г. Москва, Большой Каретный переулок, д.19 стр.1, тел.: +7(495)650-42-25, e-mail: sa-stepanov@iitp.ru.

Сергей Александрович Степанов

12. 11. 2015

Подпись Степанова С.А.
УДОСТОВЕРЯЮ
Зав. канцелярией