ОТЗЫВ

официального оппонента
о диссертационной работе КОНДРАТЁНКА Никиты Васильевича
«Свойства теоретико-числовых и криптографических алгоритмов
в дедекиндовых кольцах»,
представленной на соискание учёной степени
кандидата физико-математических наук по специальности
01.01.06 — математическая логика, алгебра и теория чисел

1. Соответствие содержания диссертации заявленной специальности и отрасли науки. Диссертация относится к области коммутативной алгебры, непосредственно примыкающей к алгебраической и алгоритмической теории чисел. Полученные результаты соответствуют отрасли физико-математических наук и специальности «01.01.06 — математическая логика, алгебра и теория чисел».

2. Актуальность темы диссертации. В алгоритмической теории чисел ключевую роль играют простые числа. В связи с этим актуальны задачи проверки целых чисел на простоту. Примечательно, что здесь проявляется связь с фундаментальными вопросами аналитической теории чисел, установленная, в частности, в работах Н.К. Анкени, Г. Миллера, М. Рабина, Э. Баха. Наибольшее значение для современных подходов к проверке на простоту и генерации больших простых чисел имеют критерии Эйлера и Миллера. Поиск аналогичных критериев простоты для идеалов в дедекиндовых кольцах с ограниченной нормой является актуальной задачей.

Алгоритм Евклида является критически важной частью многих теоретико-числовых и криптографических алгоритмов. Вычислительная сложность алгоритма Евклида определяется длиной цепочки делений. Зависимость этой длины от правила выбора остатка деления изучали Г. Ламе, Л. Кронекер, Т. Вален и другие исследователи. Работы Х. Роллечека и Э. Кальтофена показывают, что поведение алгоритма Евклида в алгебраических числовых кольцах оказывается заметно сложнее, чем в кольцах целых чисел и многочленов над полем: появляются исключительные случаи и связь со структурой группы единиц. Здесь возникает вопрос о свойствах алгоритма Евклида в более общих кольцах.

Шифр RSA, предложенный Р. Ривестом, А. Шамиром и Л. Адлеманом, до сих пор является одной из основных криптосистем с открытым ключом. В основе RSA лежит задача факторизации, которая в настоящее время считается вычислительно трудной для классического компьютера. Однако для квантового компьютера полиномиальный алгоритм факторизации — алгоритм П. Шора — известен. Исследования по переносу криптосистемы RSA на иные кольца обу-

словлены как общетеоретическим интересом, так и уязвимостью шифра RSA в случае доступности квантовых вычислений.

3. Степень новизны результатов и научных положений, выносимых на защиту. Первому положению посвящена вторая глава, где доказаны аналоги критериев Эйлера и Миллера для дедекиндовых колец с ограниченной нормой (т.н. абстрактных числовых колец). На основе доказанных критериев разработаны вероятностные алгоритмы проверки на простоту. Установлены оценки вычислительной сложности этих алгоритмов.

Второе положение раскрывается в третьей главе, в которой изучается длина цепочки делений в алгоритме Евклида в факториальных кольцах в зависимости от правила выбора остатка. Здесь разработан метод автоматического доказательства невыполнимости теоремы Кронекера—Валена в факториальном кольце. С помощью этого метода доказано, что теорема Кронекера—Валена не выполняется во всех действительных квадратичных норменно-евклидовых кольцах. Установлены оценки длины цепочки делений, когда выбирается наименьший по норме остаток.

Третье положение подробно излагается в четвёртой главе, где автор возвращается к дедекиндовым кольцам с ограниченной нормой. Здесь для RSA-подобной криптосистемы на таких кольцах, которую предложили С.Н. Тронин и К.А. Петухова в 2016 году, соискатель доказывает полные аналоги теорем о стойкости классической системы RSA.

Все результаты и научные положения, вынесенные на защиту, являются новыми.

4. Обоснованность и достоверность выводов и рекомендаций. Результаты диссертации Н.В. Кондратёнка установлены путём развития и обобщения классических идей и методов алгебраической теории чисел. Все математические утверждения и теоремы в диссертации сопровождены подробными доказательствами либо ссылками на источники. Обоснованность научных положений и выводов диссертации подтверждается сопоставлением с классическими теоремами для целых рациональных и алгебраических чисел, а также с новыми результатами по обобщению других теоретико-числовых утверждений. Вошедшие в диссертацию результаты опубликованы в рецензируемых научных изданиях и докладывались на научных конференциях.

Ввиду сказанного выше, обоснованность и достоверность результатов и выводов диссертационного исследования, а также положений, выносимых на защиту, сомнений не вызывает.

5. Научная, практическая и социальная значимость результатов диссертации с указанием рекомендаций по их использованию. Диссертационное исследование вносит существенный вклад в понимание свойств

дедекиндовых колец с конечной нормой и факториальных колец. Результаты диссертации могут стать основой для дальнейших исследований, направленных как на изучение справедливости классических теоретико-числовых утверждений в более общих кольцах, так и на поиск конкретных колец, пригодных для создания более стойких аналогов системы RSA и иных криптосистем с открытым ключом. Также эти результаты могут быть полезны при разработке вычислительных экспериментов для фундаментальных и прикладных исследований в смежных областях математики. Кроме того, наработки диссертационного исследования могут найти применение в учебных курсах по общей алгебре и теории чисел с уклоном в коммутативную алгебру. Важно отметить, что результаты третьей главы диссертации уже внедрены в учебный процесс и используются при чтении спецкурса «Криптографические системы с открытым ключом».

6. Опубликованность результатов диссертации в научной печати. Все результаты диссертации, на основе которых сформулированы выводы и положения на защиту, опубликованы в научной печати. По теме диссертации опубликовано 14 работ: 7 статей в рецензируемых научных изданиях и 7 публикаций в сборниках трудов научных конференций. Из них две публикации без соавторов. Результаты докладывались, в частности, на 5 международных научных конференциях и на международном конгрессе по информатике.

Содержание работы достаточно полно раскрыто в автореферате.

7. Соответствие оформления диссертации требованиям ВАК. Оформление диссертации соответствует требованиям ВАК Беларуси. Автореферат диссертации отвечает содержанию работы и правильно отражает результаты и основные положения, выносимые на защиту.

8. Соответствие научной квалификации соискателя учёной степени. Анализ содержания диссертации и уровень полученных результатов и опубликованных работ показывают, что научная квалификация Никиты Васильевича Кондратёнка соответствует учёной степени кандидата физико-математических наук по специальности «01.01.06 — математическая логика, алгебра и теория чисел».

9. Замечания.

1) В определении 2.20 нормы $v(\cdot)$ на с. 23 во втором пункте нужно указать, что элемент y ненулевой.

2) На с. 25 в формуле для $(xy)_i$ у мнимых компонент, т.е. при $r_1+r_2 < i \leq n$, нужен «+», а не «−».

3) В определении нормы $v(\xi)$ на основе мультипликативной функции $\mathcal{N}(\cdot)$ на с. 25 нужно взять абсолютное значение $|\mathcal{N}(\Phi(\xi))|$, а вместо x должно быть ξ; кроме того, более естественно принять $v(0) = 0$. Тогда квадрат нормы нуля

будет равен норме нуля. Как вариант исправления, если руководствоваться аддитивностью, для ненулевых ξ принять $v(\xi) = \log|\mathcal{N}(\xi)|$ и оставить $v(0) = -\infty$, но тогда нужно исправить область значений нормы $v(\cdot)$.

4) Утверждение сразу после формулы для $v(\xi)$ на с. 25 неверно, потому что любое евклидово кольцо есть область главных идеалов, а в общем случае кольцо целых алгебраических элементов числового поля не является областью главных идеалов.

5) Кое-где вещественные и мнимые части комплексных чисел обозначены несогласованно: нестандартные обозначения в определении отображения Ф на с. 25 и более привычные обозначения в примере 3.6 на с. 54.

6) Третью и четвёртую главы, ввиду их содержания и рассматриваемых в них колец, более естественно было бы включить в обратном порядке.

7) Формулировка «теоремы Кранакиса» в основном тексте диссертации нигде явно не обозначена. Есть лишь упоминания на с. 6, 7, 18 и 81.

Указанные замечания не затрагивают сути основных положений диссертации и не снижают научной ценности полученных результатов.

10. Заключение. Диссертация Н.В. Кондратёнка является завершённым научным исследованием. По уровню научной новизны она соответствует требованиям, установленным для кандидатских диссертаций согласно «Положению о присуждении учёных степеней и присвоении учёных званий в Республике Беларусь». Никита Васильевич Кондратёнок заслуживает присуждения учёной степени кандидата физико-математических наук по специальности «01.01.06 — математическая логика, алгебра и теория чисел» за новые научно обоснованные результаты:

1) критерии простоты идеалов в дедекиндовых кольцах с конечной нормой;

2) теоремы о длине цепочек делений в факториальных кольцах;

3) необходимые условия криптографической стойкости криптосистемы RSA в дедекиндовых кольцах.

Официальный оппонент,
старший научный сотрудник
Института математики НАН Беларуси,
кандидат физико-математических наук, доцент Д.В. Коледа

23.01.2023

Подпись Д.В. Коледы удостоверяю:
Ведущий специалист
по кадрам
Института математики
НАН Беларуси