УТВЕРЖДАЮ
Ректор
Учреждения образования
«Гомельский государственный
университет имени Ф. Скорины»
С.А. Хахомов
2023

ОТЗЫВ ОППОНИРУЮЩЕЙ ОРГАНИЗАЦИИ
Учреждения образования «Гомельский государственный университет имени Франциска Скорины»
на диссертацию Кондратёнка Никиты Васильевича
«Свойства теоретико-числовых и криптографических алгоритмов в дедекиндовых кольцах», представленную на соискание ученой степени кандидата физико-математических наук по специальности «01.01.06 – математическая логика, алгебра и теория чисел».

Соответствие содержания диссертации заявленной специальности и отрасли науки

Алгоритмическая теория чисел является активно развиваемым разделом современной теории чисел, в котором строятся эффективные алгоритмы решения таких проблем, как тестирование на простоту, целочисленная факторизация, дискретное логарифмирование, нахождение решений диофантовых уравнений и др. Актуальность решения таких задач обусловлена запросами и успехами криптографии с открытым ключом, а также дальнейшим развитием высокопроизводительных компьютеров.

К настоящему времени задача эффективной проверки на простоту решена для кольца целых чисел. В работах Г. Миллера, М. Рабина, Р. Соловея и других математиков разработаны вероятностные полиномиальные алгоритмы тестирования на простоту. В 2002 году М. Агравалом и его учениками был предложен детерминированный полиномиальный тест на простоту, называемый AKS тестом. Большой интерес представляет решение аналогичной задачи в кольцах более общего вида. При таком переходе задача существенно усложняется, однако классические методы алгоритмической теории чисел продолжают работать, хотя и с изменениями. Это было показано в работах Э. Баха, Х. Коэна, Э. Поста. Однако до появления работ диссертанта задача построения эффективного алгоритма проверки на простоту была практически не исследована для дедекиндовых колец.

Важной частью многих теоретико-числовых и криптографических алгоритмов является алгоритм Евклида, который позволяет находить наибольший общий делитель двух чисел и их коэффициенты Безу. При этом важно знать сколько шагов алгоритма необходимо будет проделать для

получения результата. Данные (экстремальные) свойства алгоритма Евклида исследовались в работах Г. Ламе, Л. Кронекера, Т. Валена. Как было показано в работах Х. Роллетчека и Э. Калтофена, при исследовании алгоритма Евклида в более общих кольцах задача становится сложнее и содержательней. Отметим, что до работ диссертанта доказательства аналогов теоремы Кронекера-Валена для различных колец (в частности, факториальных) сильно опирались на структуру кольца и их было трудно переносить на другие кольца.

Выделенные выше задачи имеют не только (внутреннее) значение для развития теории колец, близких к числовым (дедекиндовых, факториальных и др.), но имеют прикладное значение для криптографии с открытым ключом.

В 1976 году в знаменитой работе Р. Ривеста, А. Шамира, Л. Адльмана была опубликована первая криптосистема с открытым ключом (RSA-криптосистема). Криптографическая стойкость RSA базируется на вычислительной сложности задачи факторизации в кольце целых чисел. В силу своей простоты и надежности криптосистема RSA широко применяется в настоящее время. В 1995 году Питер Шор продемонстрировал полиномиальный алгоритм для взлома криптографических систем с открытым ключом при использовании квантового компьютера. Поэтому появление квантовых вычислителей достаточной размерности поставит под угрозу надежность многих современных криптосистем с открытым ключом, в частности, криптосистемы RSA. Это обстоятельство побудило многих исследователей, включая Б. Ли, А. Коваля, С.Н. Тронина, Н.В. Кондратёнка и др., изучать свойства аналогов RSA-криптосистемы в более сложных алгебраических структурах.

Таким образом, тема диссертационной работы Н.В. Кондратёнка «Свойства теоретико-числовых и криптографических алгоритмов в дедекиндовых кольцах» является актуальной, а ее содержание соответствует отрасли «физико-математические науки» и паспорту специальности ВАК Республики Беларусь 01.01.06 – математическая логика, алгебра и теория чисел.

Научный вклад соискателя в решение научной задачи с оценкой его значимости

В рассматриваемой диссертации соискателем доказаны новые критерии простоты идеалов в дедекиндовых кольцах, обобщающие известные критерии Миллера и Эйлера, которые являются основой для построения эффективных алгоритмов тестирования простоты; разработаны новые методы исследования экстремальных свойств алгоритма Евклида в факториальных кольцах, на основе которых доказаны аналоги теорем Кронекера-Валена и Ламе; впервые исследованы свойства аналога криптосистемы RSA в дедекиндовых кольцах и найдены необходимые условия криптостойкости криптосистемы RSA в дедекиндовых кольцах.

Следовательно, Н.В. Кондратёнок получил новые научные результаты в алгоритмической теории числовых колец (дедекиндовых, факториальных и др.) и её приложениях к криптографии. Научные результаты Н.В. Кондратёнка заслуживают признания математическим сообществом, как в Беларуси, так и за рубежом.

Научный вклад диссертанта, значимость его результатов также

подтверждается их полной опубликованностью в 14 научных работах, из которых 7 статей в ведущих рецензируемых журналах, входящих в перечень ВАК Республики Беларусь (Доклады НАН Беларуси – 2 статьи, Вестник БГУ. Серия 1 Физика, Математика, Информатика – 1 статья, Журнал Белорусского государственного университета. Математика. Информатика, Scopus – 1 статья, Journal of Number Theory, Scopus и ISI – 1 статья, Journal of Symbolic Computation, Scopus и ISI – 2 статьи), 2 статьи в сборниках статей лауреатов и авторов научных работ, получивших первую категорию XXIV и XXV Республиканских конкурсов научных работ студентов, и 5 материалов в сборниках международных и республиканских научных конференций.

Исследования проводились в рамках ГПНИ «Анализ асимптотических свойств решений дифференциальных и алгебраических систем» (2016-2020 гг.), «Анализ общих и асимптотических свойств решений стохастических дифференциальных уравнений с приложениями в криптографии и теории кредитных рисков» (2021-2025 гг.). Научные результаты Н.В. Кондратёнка внедрены в учебный процесс БГУ, что подтверждается 1 актом о внедрении в образовательный процесс.

Исходя из сказанного, можно сделать вывод об оригинальности полученных результатов и методов, их высокой теоретической и практической значимости.

Результаты диссертации обсуждались на научных семинарах в БГУ, отдела теории чисел Института математики НАН Беларуси и на расширенном семинаре кафедры алгебры и геометрии Гомельского государственного университета имени Франциска Скорины.

Конкретные научные результаты (с указанием их новизны и практической значимости), за которые соискателю может быть присуждена искомая ученая степень

Остановимся подробнее на основных результатах диссертации.

В первой главе диссертации приводится обзор литературы по теме исследования и формулируются решаемые задачи.

Вторая глава диссертации посвящена доказательству новых критериев простоты в дедекиндовых кольцах и разработке полиномиальных алгоритмов тестирования простоты идеалов. В диссертации доказаны аналоги критериев Миллера и Эйлера в дедекиндовых кольцах (теоремы 2.1, 2.2). Построены вероятностные алгоритмы тестирования на простоту, опирающиеся на полученные критерии. Доказано, что построенные алгоритмы являются полиномиальными относительно арифметических операций. Найден класс колец, для которых полученные алгоритмы можно модифицировать, получив детерминированные полиномиальные алгоритмы тестирования на простоту. Показано, что полученные критерии можно использовать для построения эффективных вероятностных алгоритмов проверки идеалов на простоту. В предположении справедливости расширенной гипотезы Римана найдены классы дедекиндовых колец, в которых справедливы усиленные аналоги критериев Миллера и Эйлера, приводящие к детерминированным полиномиальным алгоритмам тестирования простоты идеалов.

В третьей главе диссертации исследуются экстремальные свойства

алгоритма Евклида в факториальных кольцах. Разработан метод автоматического доказательства теоремы Кронекера-Валена в фиксированном факториальном кольце (теорема 3.1). Разработан метод автоматического доказательства невыполнимости теоремы Кронекера-Валена в кольцах целых алгебраических элементов числового поля (алгоритм 3.4). Используя этот метод, доказано, что теорема Кронекера-Валена не выполняется во всех действительных квадратичных норменно-евклидовых кольцах (теорема 3.2). Доказан аналог теоремы Ламе в факториальных кольцах (теорема 3.3).

В четвертой главе диссертации доказаны теоремы, накладывающие необходимые условия на параметры криптосистемы RSA в дедекиндовых кольцах с конечной нормой для обеспечения ее криптостойкости. В частности, доказаны аналоги теоремы об эквивалентности взлома криптосистемы и факторизации ее модуля (теоремы 4.1, 4.4), теоремы Винера о малой секретной экспоненте (теорема 4.2) и теоремы, обеспечивающей защиту от атаки методом повторного шифрования (теорема 4.3).

Все основные результаты диссертации, выносимые на защиту, являются новыми и получены автором впервые. Все результаты диссертации строго доказаны и сопоставлены с известными ранее фактами.

Таким образом, диссертация Н.В. Кондратёнка содержит научные результаты высокого уровня, представляющие несомненный научный интерес и дающие важный вклад в развитие алгоритмической теории чисел и её приложений к криптографии. С учетом вышесказанного, можно сделать вывод об новизне полученных результатов и методов, их высокой теоретической и практической значимости.

Конкретные рекомендации по использованию результатов диссертации

Диссертационная работа относится к алгоритмической теории чисел, активно развивающемуся разделу современной математики. Полученные в ней результаты и методы могут найти применение при проведении дальнейших исследований теоретико-числовых и криптографических алгоритмов не только в дедекиндовых, но и в кольцах более общего вида. Кроме того, материалы диссертации могут применяться при решении задач прикладного характера, в частности, в криптографии. Результаты диссертации также могут быть использованы в образовательном процессе для подготовки дипломных, магистерских и кандидатских диссертаций, чтения спецкурсов на математических и компьютерных специальностях высших учебных заведений.

Замечания по диссертации и автореферату

Диссертация и автореферат оформлены в соответствии с требованиями ВАК Беларуси. Автореферат полностью отражает содержание диссертации и положения, выносимые на защиту. Решаемые задачи четко обоснованы, их решения проводятся строго математически. Имеется несколько замечаний технического характера, которые не влияют на научную ценность полученных результатов:

1. На стр. 23 в определении 2.19 факториального кольца надо дополнить « с точностью до перестановки множителей» до « с точностью до перестановки

сомножителей и умножения на обратимый элемент».

2. На стр. 23, 12-я строка сверху: утверждение «Факториальное кольцо является кольцом главных идеалов» неверно. Видимо надо писать «Кольцо главных идеалов является факториальным».

3. На стр. 14, 9-я строка сверху надо вместо «… называется жадным алгоритмов Евклида.» писать «… называется жадным алгоритмом Евклида.»

4. На стр. 70, 9 строка снизу надо вместо «$f(x) \equiv x^e \pmod{\varphi(\Re)}$» писать «$f(x) \equiv x^e \pmod{\Re}$», 6 строка снизу надо вместо «$f^{-1}(x) \equiv x^d \pmod{\varphi(\Re)}$» писать «$f^{-1}(x) \equiv x^d \pmod{\Re}$».

5. В ряде формулировок определений, утверждений, теорем пропущены необходимые тире. Например, на стр. 19 в определении 2.1 вместо «Пусть R коммутативное кольцо …» надо «Пусть R − коммутативное кольцо …». Аналогичные замечания касаются определений 2.11, 2.12, 2.13 на стр. 21, 2.15-2.16 на стр. 22, 2.20-2.21 на стр. 23, 2.22 на стр. 24, утверждений 2.11-2.13 на стр. 33, предложений 2.12-2.13 на стр. 42, определений 3.1-3.2 на стр. 44, теорем 3.4 на стр. 67 и 4.4 на стр. 74.

6. В ряде предложений текста отсутствуют необходимые запятые. Например, на стр. 81, 5-я строка снизу: вместо «Доказаны теоремы накладывающие необходимые условия …» надо писать «Доказаны теоремы, накладывающие необходимые условия …», на этой же странице, строка 3-я строка снизу: вместо «В частности теорема Винера …» надо писать «В частности, теорема Винера …»

7. На стр. 84, 10-я строка снизу: вместо «Васьльев Д.В.» надо писать «Васильев Д.В.».

Сделанные замечания не снижают научную и практическую значимость полученных автором результатов.

Соответствие научной квалификации соискателя ученой степени, на которую он претендует

Из вышесказанного следует, что диссертация «Свойства теоретико-числовых и криптографических алгоритмов в дедекиндовых кольцах» Кондратёнка Никиты Васильевича является завершенной квалификационной научной работой и содержит новые научно обоснованные результаты, совокупность которых вносит существенный вклад в алгоритмическую теорию чисел. Диссертационная работа Н.В. Кондратёнка «Свойства теоретико-числовых и криптографических алгоритмов в дедекиндовых кольцах» полностью соответствует требованиям ВАК Республики Беларусь, предъявляемым к диссертациям на соискание ученой степени кандидата физико-математических наук, соответствует требованиям пп. 19-20 «Положения о присуждении ученых степеней и присвоении ученых званий в Республике Беларусь», а ее автор Кондратёнок Никита Васильевич заслуживает присуждения ему ученой степени кандидата физико-математических наук по специальности ВАК Республики Беларусь 01.01.06 - математическая логика, алгебра и теория чисел за:

– нахождение и доказательство критериев простоты идеалов в дедекиндовых кольцах с конечной нормой, аналогичных критериям Эйлера и Миллера в кольце целых чисел;

– нахождение и доказательство аналогов теорем Кронекера-Валена и Ламе о наименьшей длине цепочек делений в алгоритме Евклида в факториальных кольцах;

– необходимые условия криптографической стойкости криптосистемы RSA в дедекиндовых кольцах.

Отзыв о диссертации Н.В. Кондратёнка «Свойства теоретико-числовых и криптографических алгоритмов в дедекиндовых кольцах» на соискание ученой степени кандидата физико-математических наук по специальности 01.01.06 - математическая логика, алгебра и теория чисел согласно приказу от 03 января 2023 года № 4 ректора учреждения образования «Гомельский государственный университет имени Франциска Скорины» рассмотрен и обсужден на заседании расширенного научного семинара кафедры алгебры и геометрии 16 января 2023 года, протокол № 1.

Н.В. Кондратёнок выступил на семинаре с докладом. На семинаре состоялась дискуссия, соискатель дал исчерпывающие ответы на заданные вопросы.

В работе семинара и в голосовании приняли участие 5 докторов физико-математических (А.Н. Скиба, В.С. Монахов, М.В. Селькин, А.Ф. Васильев, С.Ф. Каморников) и 5 кандидатов физико-математических наук (В.В. Аниськов, Р.В. Бородич, Т.И. Васильева, В.И. Мурашко, Д.А. Ходанович).

Результаты открытого голосования: «за» – 10, «против» – нет, «воздержались» – нет.

Председатель научного семинара:
профессор кафедры алгебры и геометрии,
доктор физ.-мат. наук, профессор _____ А.Н. Скиба

Секретарь заседания научного семинара:
доцент кафедры алгебры геометрии, кандидат
физ.-мат. наук _____ В.И. Мурашко

Эксперт оппонирующей организации:
профессор кафедры алгебры и геометрии,
доктор физ.-мат. наук, доцент _____ А.Ф. Васильев