ОТЗЫВ

научного руководителя о диссертации Кондратёнка Никиты Васильевича «Свойства теоретико-числовых и криптографических алгоритмов в дедекиндовых кольцах», представленной на соискание ученой степени кандидата физико-математических наук по специальности 01.01.06 – математическая логика, алгебра и теория чисел

1. Научная оценка диссертации.

Актуальность темы диссертации.

Начиная с 70-х годов XX века интенсивно развивается алгоритмическая теория чисел, что объясняется значительными успехами в криптографии с открытым ключом и появлением высокопроизводительной вычислительной техники. Центральное место в современной алгоритмической теории чисел занимают проблемы, связанные с тестированием на простоту, генерацией больших простых чисел, факторизацией и дискретным логарифмированием. Несмотря на то, что в работах Г. Миллера, М. Рабина, Р. Соловея, А. Ленстры, Х. Ленстры мл., Дж. Полларда, М. Агравала и других математиков за последние 30-40 лет были получены глубокие и важные результаты по упомянутым направлениям, многие важные проблемы остаются нерешенными и привлекают внимание лучших математиков мира. С 90-х годов XX века осуществляются исследования на стыке алгебраической и алгоритмической теории чисел, что связано с нахождением значительных приложений алгебраических числовых полей к решению задач факторизации и дискретного логарифмирования. Несмотря на существенное усложнение объектов исследования, в работах Э. Баха, Х. Коэна, Э. Поста, Н.В. Кондратёнка, Н.П. Прохорова и других математиков, показано, что классические методы алгоритмической теории чисел с соответствующими изменениями продолжают работать в применении к более сложным алгебраическим структурам, в том числе, дедекиндовым кольцам.

Критерии Миллера и Эйлера простоты числа являются ключевыми для современных алгоритмов тестирования на простоту и генерации больших простых чисел. Нахождение критериев простоты идеалов в дедекиндовых кольцах, приводящих к эффективным алгоритмам тестирования простоты, является сложной и актуальной задачей.

Алгоритм Евклида является составной частью многих теоретико-числовых и криптографических алгоритмов, включая алгоритмы генерации ключей для криптосистем с открытым ключом. В работах Г. Ламе, Л. Кронекера, Т. Валена и других математиков исследовались экстремальные свойства алгоритма Евклида. Как показано в работах Э. Калтофена, Х. Роллетчека и других математиков, исследование арифметических свойств алгоритма Евклида в алгебраических числовых кольцах существенно усложняется по сравнению с аналогичными задачами в кольцах целых чисел и многочленов над полем. В частности, аналог теоремы Кронекера-Валена о кратчайшей длине цепочек деления не выполняется в некоторых мнимых квадратичных евклидовых кольцах. В действительных квадратичных кольцах задача исследования экстремальных свойств алгоритма Евклида ещё больше усложняется, что объясняется бесконечностью группы обратимых элементов. Первые систематические исследования алгоритма Евклида в таких алгебраических структурах были даны в работах М.М. Васьковского и диссертанта.

В 70-е годы XX века в работе Р. Ривеста, А. Шамира, Л. Адльмана были заложены основы нового направления в криптографии: предложена первая криптосистема с открытым ключом, названная впоследствии RSA-криптосистемой. Криптографическая стойкость этой криптосистемы основана на вычислительной сложности задачи факторизации. Ввиду своей простоты и надежности криптосистема RSA стала использоваться повсеместно. В конце XX века в работе П. Шора был предложен квантовый полиномиальный алгоритм факторизации чисел. Впоследствии аналогичный алгоритм был предложен для решения задачи дискретного логарифмирования. Тем самым появление высокопроизводи-

тельных квантовых компьютеров поставит под угрозу надежность многих современных криптосистем с открытым ключом, включая криптосистему 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.

Основные результаты диссертации, их новизна, достоверность, научная и практическая значимость.

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. 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.

Третья глава диссертации посвящена доказательству теорем об экстремальных свойствах алгоритма Евклида в факториальных кольцах. В диссертации выделен класс колец, в которых выполняется аналог теоремы Кронекера-Валена о кратчайшей длине цепочки деления. Разработан алгоритм, позволяющий проверить принадлежность кольца этому данному классу. Построен метод автоматического доказательства невыполнимости теоремы Кронекера-Валена в числовых кольцах, что позволило доказать утверждение о невыполнимости аналога Кронекера-Валена в произвольном действительном квадратичном норменно-евклидовом кольце. Таким образом, полностью решена проблема о выполнимости аналога теоремы Кронекера-Валена в квадратичных норменно-евклидовых кольцах. Доказан аналог теоремы Ламе о длине цепочки делений с выбором минимального по норме остатка в факториальных кольцах.

Четвертая глава диссертации посвящена исследованию свойств RSA-криптосистемы в дедекиндовых кольцах. Доказаны теоремы, являющиеся аналогами теорем об эквивалентности нахождения секретного ключа криптосистемы и факторизации ее модуля. Доказан аналог теоремы Винера о малой секретной экспоненте и некоторые другие теоремы, накладывающие необходимые условия на параметры RSA-криптосистемы для обеспечения ее криптостойкости.

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

Таким образом, Н.В. Кондратёнок получил новые научные результаты в алгоритмической теории чисел и её приложениях к криптографии. Научные результаты Н.В. Кондратёнка признаны математическим сообществом, как в Беларуси, так и за рубежом. Полученные результаты опубликованы в 14 научных работах, среди которых 7 статей в изданиях, соответствующих пункту 18 Положения о присуждении ученых степеней и присвоении ученых званий в Республике Беларусь, и 7 статей в сборниках трудов 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. Методы и результаты диссертационной работы многократно обсуждались на международных научных конференциях, научных семинарах в БГУ и ГНУ «Институт математики» НАН Беларуси.

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

2. Характеристика научной, научно-педагогической и производственной деятельности соискателя.

Несмотря на то, что Кондратёнок Н.В. является аспирантом первого года обучения, он имеет многолетний успешный научно-исследовательский опыт, что подтверждается наличием публикаций в высокорейтинговых научных журналах, входящих в БД Scopus и Web of Science, а также значительными наукометрическими показателями (Индекс цитирования равен 26, h-индекс равен 3 согласно Google Scholar).

Н.В. Кондратёнок является участником и призером многих престижных конкурсов научно-исследовательских работ молодых ученых, включая Intel ISEF, EUCYS, ICYS, ITYM. Является лауреатом республиканского конкурса научных работ студентов УВО Республики Беларусь, кроме того, он дважды был отмечен дипломом 1 категории. Является лауреатом специального фонда Президента Республики Беларусь по социальной поддержке одаренных учащихся и студентов. Награждался стипендией имени А.Н. Севченко, является получателем гранта Huawei.

Кондратёнок Н.В. является старшим преподавателем кафедры высшей математики БГУ, на которой он работает с 2021 года после окончания с отличием университета и магистратуры. Кондратёнок Н.В. на высоком научно-методическом уровне читает лекции и проводит практические занятия по специальной дисциплине «Криптографические системы с открытым ключом» для студентов военного факультета БГУ. Диссертант проводит большую работу с одаренными учащимися и студентами: является автором задач и членом жюри на республиканских турнирах юных математиков, участвовал в подготовке команд Беларуси на международных турнирах юных математиков, регулярно проводит занятия с одаренными учащимися в Республиканской летней научно-исследовательской школе учащихся и учителей, руководит научно-исследовательской работой студентов на факультете прикладной математики и информатики.

Выводы. Считаю, что научные работы Кондратёнка Н.В. выполнены на высоком уровне, вносят значительный вклад в алгоритмическую теорию чисел и ее приложения и соответствуют требованиям, предъявляемым ВАК к кандидатским диссертациям, а их автор заслуживает присуждения степени кандидата физико-математических наук по специальности 01.01.06 – математическая логика, алгебра и теория чисел за следующие новые научные 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.

Научный руководитель
доктор физ.-мат. наук, профессор,
заведующий кафедрой высшей математики БГУ М.М. Васьковский

ПОДПИСЬ Васьковского М.М. УДОСТОВЕРЯЮ
Начальник управления
организационной работы и
документационного обеспечения
Н.Б. Черкасская
09.11