О Т З Ы В

официального оппонента о диссертации Кондратенка 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.

Соответствие диссертации специальностям и отрасли науки, по которым она представлена к защите. Диссертационное исследование относится к алгоритмической теории чисел. При доказательстве теорем используются методы алгебраической теории чисел и теории колец. Таким образом, все полученные результаты соответствуют специальности 01.01.06 – математическая логика, алгебра и теория чисел.

Актуальность темы диссертации.

Алгоритмическая теория чисел является одним из активно развивающихся разделов теории чисел. Ее развитие стимулируется разнообразными применениями в криптографии. Во второй половине XX века были получены принципиально новые критерии простоты чисел, например, критерий Миллера, что позволило создать новые алгоритмы проверки чисел на простоту – алгоритмы Соловея-Штрассена и Миллера-Рабина. В 2002 году в работе М. Агравала, Н. Каяла и Н. Саксены был предложен алгоритм тестирования на простоту полиномиальной сложности. При переходе от кольца целых чисел к более общим кольцам, в которых не выполняется основная теорема арифметики, Э.Э. Куммер предложил рассматривать идеалы этих колец и разложение идеалов в произведение простых идеалов, что является аналогом разложения чисел на простые множители. В диссертации разработан подход, позволяющий переносить доказательства критериев простоты на различные алгебраические структуры. В частности, критерии простоты Миллера и Эйлера были доказаны в случае кольца целых алгебраических элементов квадратичного числового поля. Используя доказанные критерии, были получены аналоги алгоритмов Миллера-Рабина и Соловея-Штрассена, и построены оценки их вычислительной сложности. Это свидетельствует об актуальности темы диссертации.

Степень новизны результатов, полученных в диссертации, и научных положений, выносимых на защиту. Все результаты, полученные в диссертации и научные положения, выносимые на защиту, являются новыми. В диссертации получены следующие новые результаты: доказаны критерии простоты идеалов в дедекиндовых кольцах с конечной нормой; доказаны теоремы о длине цепочек делений в алгоритме Евклида в евклидовых кольцах; найдены необходимые условия криптографической стойкости криптосистемы RSA в дедекиндовых кольцах.

Диссертация состоит из оглавления, перечня сокращений и обозначений, введения, общей характеристики работы, четырех глав с выводами, заключения, списка использованных источников, включающего 48 наименований, списка публикаций соискателя, включающего 14 публикаций, приложения А «Документы, подтверждающие практическое применение результатов диссертации» и приложения В «Исходный код программы нахождения контрпримеров к теореме Кронекера-Валена». Полный объем диссертации составляет 102 страницы.

В первой главе содержится обзор литературы по теме диссертации.

Вторая глава посвящена тестированию идеалов на простоту в дедекиндовых кольцах. Напомним, что кольцо R называется *дедекиндовым*, если любой нетривиальный идеал однозначно раскладывается в произведение простых идеалов с точностью до порядка множителей. В данной главе рассматриваются дедекиндовы кольца с конечной нормой, т.е. обладающие свойством: для любого собственного идеала $J \subset R$ факторкольцо R/J конечно. Основными результатами главы являются следующие 2 теоремы, предлагающие новые критерии простоты идеала.

Теорема 2.1. *Пусть $\mathfrak{n}$ – нетривиальный идеал нечетной нормы дедекиндового кольца R. Тогда $\mathfrak{n}$ – простой идеал тогда и только тогда, когда для любого $a \in I_{R/\mathfrak{n}}$ выполнено*

$$a^{\frac{Nm(\mathfrak{n})-1}{2}} \equiv \left(\frac{a}{\mathfrak{n}}\right) (\operatorname{mod} \mathfrak{n})$$

Если кольцо R факториальное и удовлетворяет условию А, то $\mathfrak{n}$ – простой идеал тогда и только тогда, когда для любого $a \in I_{R/\mathfrak{n}}$, $Nm(a) \le f_R(Nm(\mathfrak{n}))$ выполнено

$$a^{\frac{Nm(\mathfrak{n})-1}{2}} \equiv \left(\frac{a}{\mathfrak{n}}\right) (\operatorname{mod} \mathfrak{n})$$

Теорема 2.2. *Пусть $\mathfrak{n}$ – нетривиальный идеал нечетной нормы дедекиндового кольца R. Пусть $Nm(\mathfrak{n}) - 1 = 2^t u$, $(u,2) = 1$. Тогда $\mathfrak{n}$ – простой идеал тогда и только тогда, когда для любого $a \in I_{R/\mathfrak{n}}$, $a^u \not\equiv 1 (\operatorname{mod} \mathfrak{n})$, существует $k \in \{0,\ldots,t-1\}$, такое что $a^{2^k u} \equiv -1 (\operatorname{mod} \mathfrak{n})$.*

Пусть кольцо R факториальное и удовлетворяет условию А. Тогда $\mathfrak{n}$ – простой идеал тогда и только тогда, когда для любого $a \in I_{R/\mathfrak{n}}$, $Nm(a) \le f_R(Nm(\mathfrak{n}))$, $(a,\mathfrak{n}) = 1$, $a^u \not\equiv 1 (\operatorname{mod} \mathfrak{n})$, существует $k \in \{0,\ldots,t-1\}$, такое что $a^{2^k u} \equiv -1 (\operatorname{mod} \mathfrak{n})$.

Эти теоремы позволяют получить 2 вероятностных алгоритма проверки идеала на простоту. В параграфе 2.4 приведены оценки сложности данных алгоритмов.

В третьей главе рассматривается арифметика факториальных колец. В 1977 г. Д. Лазаром было доказано, что в кольце целых чисел алгоритм Евклида, который на каждом шаге выбирает минимальный по модулю остаток, приводит к цепочке делений минимальной длины. Этот результат часто называют теоремой Кронекера-Валена. Д. Лазаром был также доказан аналог теоремы Кронекера-Валена в кольце $k[x]$ многочленов над полем. В 1990 г. Г. Роллетчеком был доказан аналог теоремы Кронекера-Валена в кольце целых поля $\mathbb{Q}(\sqrt{d})$, где $d<0$, $d \neq -11$. В диссертации введены два класса факториальных колец – $\mathcal{S}$ и $\mathcal{T}$, при этом $\mathcal{S} \subset \mathcal{T}$. В теореме 3.1 доказано, что в кольцах из класса $\mathcal{T}$ справедлива теорема Кронекера-Валена. На основе теоремы 3.1 построен алгоритм, который позволяет проверить, принадлежит ли заданное факториальное кольцо классу $\mathcal{T}$. Работа этого алгоритма продемонстрирована на примере колец $\mathbb{Z}$, $K[t]$, где K – поле, $\mathbb{Q}(i)[t,t^{-1}]$, $\mathbb{Z}[t]$. Доказано, что эти кольца лежат в классе $\mathcal{S}$. В примере 3.6 показано, что кольцо целых гауссовых чисел $\mathbb{Z}[i]$ лежит в классе $\mathcal{T}$, но не лежит в классе $\mathcal{S}$. Из работы Роллетчека следует. что кольцо $\mathcal{O}_{\mathbb{Q}(\sqrt{-11})}$ не принадлежит классу $\mathcal{T}$. В диссертации также предложен метод доказательства невыполнимости теоремы Кронекера-Валена в кольце целых алгебраических элементов числового поля K, а также модификация этого алгоритма в случае, когда $\mathcal{O}_K$ – действительное квадратичное норменно-евклидово кольцо. Известно, что существует 16 полей $K=\mathbb{Q}(\sqrt{d})$ таких, что $\mathcal{O}_K$ – действительное квадратичное норменно-евклидово кольцо. В теореме 3.2 доказано, используя разработанные методы, что ни для одного из этих колец не выполняется теорема Кронекера-Валена. В параграфе 3.3 рассматриваются аналоги теоремы Ламе в факториальных кольцах. Следует отметить следующую теорему.

Теорема 3.4. *Пусть $d \neq 1$ – целое число, свободное от квадратов. Если кольцо* $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ евклидово относительно нормы поля $\mathbb{Q}(\sqrt{d})$, то $l_n(\mathcal{O}_{\mathbb{Q}(\sqrt{d})}) = O(\log n)$.

В четвертой главе исследуется аналог криптосистемы RSA в дедекиндовых кольцах с конечным полем остатков, предложенный ранее в работе Петуховой и Тронина. Доказан аналог теоремы Винера о малой секретной экспоненте и ряд теорем, связанных с криптостойкость криптосистемы RSA. Приведен способ защиты от атаки повторного шифрования. Разработан метод сведения задачи факторизации идеалов в числовых дедекиндовых кольцах к задаче факторизации целых чисел с полиномиальной сложностью.

Таким образом, диссертация Н.В. Кондратенка является цельным, глубоким научным исследованием в области алгоритмической теории чисел, а ее содержание полностью соответствует специальности 01.01.06 – математическая логика, алгебра и теория чисел. Данное исследование является важным научным вкладом в развитие алгоритмической теории чисел.

Обоснованность и достоверность выводов и рекомендаций, сформулированных в диссертации. Все изложенные в диссертации результаты выводы достоверны и обоснованы. Это подтверждено публикациями в ведущих научных журналах. Диссертация прошла апробацию на многих международных и республиканских конференциях.

Научная, практическая, экономическая и социальная значимость результатов диссертации с указанием рекомендаций по их использованию.

Результаты диссертации носят фундаментальный характер и могут быть использованы в дальнейших исследованиях по алгоритмической теории чисел, а также при построении новых криптосистем с открытым ключом. Они могут быть использованы в учебном процессе при чтении спецкурсов на математических факультетах университетов, при подготовке курсовых и дипломных проектов, магистерских диссертаций.

Опубликованность результатов диссертации в научной печати.

Основные результаты диссертации полностью опубликованы и отражены в 14 работах, 7 из которых составляют научные статьи в рецензируемых математических журналах, 7 из которых входит в перечень ВАК Беларуси.

Результаты диссертации докладывались соискателем на ряде международных математических конференций.

Считаю, что результаты, полученные Н.В. Кондратенком при написании диссертационной работы, опубликованы в необходимом объеме.

Соответствие оформления диссертации требованиям ВАК.

Автореферат диссертации точно и правильно отражает ее содержание и основные положения, выносимые на защиту. Диссертация и автореферат оформлены в соответствии с требованиями ВАК Беларуси.

Соответствие научной квалификации соискателя ученой степени, на которую он претендует. На основании уровня и обоснованности полученных в диссертации результатов Н.В. Кондратенок заслуживает присвоения ученой степени кандидата физико-математических наук.

Замечания.

1. С. 27. В определении 2.28, по-моему, индекс m следует заменить на r. Также вместо $(e_1,\ldots,e_n)_{\mathbb{Z}}$ следует писать $(e_1,\ldots,e_r)_{\mathbb{Z}}$.
2. С. 44. В определении 3.1 при определении цепочки делений пропущено, что $r_k = 0$.
3. С. 44, 15 строка сверху. В определении числа $l_{a,b}$ вместо знака $\cap$ должен быть $\cup$.

4. С. 45. В определении 3.5 следует указать, что такое F_1. По смыслу можно догадываться, что это то же множество, которое определялось в предыдущей главе.
5. С. 59. В формулировке леммы 3.4 следовало бы указать, что обозначают Φ, $Orb(x)$ и K.

Эти замечания не влияют на качество диссертации, поскольку смысл легко восстанавливается из контекста. В тексте диссертации также существует некоторое количество синтаксических и пунктуационных ошибок. Поскольку математический смысл при этом не страдает, то их можно считать несущественными.

Заключение. Диссертация Н.В. Кондратенка «Свойства теоретико-числовых и криптографических алгоритмов в дедекиндовых кольцах» является квалификационной научной работой, ее содержание соответствует специальности 01.01.06 – математическая логика, алгебра и теория чисел, а ее автор Н.В. Кондратенок заслуживает присуждения ему ученой степени кандидата физико-математических наук за следующие новые научные результаты:

1. Доказательство критериев простоты идеалов в дедекиндовых кольцах с конечной нормой.
2. Выделение класса факториальных колец, для которых справедлив аналог теоремы Кронекера-Валена.
3. Доказательство того, что действительные квадратичные норменно-евклидовы кольца не удовлетворяют теореме Кронекера-Валена.
4. Нахождение необходимых условий криптографической стойкости криптосистемы RSA в дедекиндовых кольцах.

Заведующий кафедрой высшей алгебры
и защиты информации
Белорусского государственного университета,
доктор физико-математических наук,
профессор В. В. Беняш-Кривец

Подпись Беняш-Кривца В.В. удостоверяю
Зам.начальника управления
по работе с персоналом
«23» 01 2023 г.