ГОСУДАРСТВЕННОЕ НАУЧНОЕ УЧРЕЖДЕНИЕ
”ИНСТИТУТ МАТЕМАТИКИ
НАЦИОНАЛЬНОЙ АКАДЕМИИ НАУК БЕЛАРУСИ”

УДК 512.713

Кондратёнок Никита Васильевич

Свойства теоретико-числовых и криптографических алгоритмов в дедекиндовых кольцах

Автореферат
диссертации на соискание ученой степени
кандидата физико-математических наук

по специальности 01.01.06 –
математическая логика, алгебра и теория чисел

Минск, 2022

Научная работа выполнена в Белорусском государственном университете.

Научный руководитель: **Васьковский Максим Михайлович**,
доктор физико-математических наук,
профессор,
заведующий кафедрой высшей математики
Белорусского государственного университета

Официальные оппоненты: **Беняш-Кривец Валерий Вацлавович**,
доктор физико-математических наук,
профессор,
заведующий кафедрой высшей алгебры и
защиты информации Белорусского
государственного университета
Коледа Денис Владимирович,
кандидат физико-математических наук,
доцент,
старший научный сотрудник отдела теории
чисел и дискретной математики ГНУ
”Институт математики Национальной академии
наук Беларуси”

Оппонирующая организация: **УО ”Гомельский государственный университет имени Франциска Скорины”**

Защита состоится 03 февраля 2023 г. в 16.00 на заседании совета по защите диссертаций Д 01.02.01 при Государственном научном учреждении ”Институт математики Национальной академии наук Беларуси” по адресу: 220072, г. Минск, ул. Сурганова, 11, конференц-зал. Тел. ученого секретаря: +375 17 379 17 78, e-mail: tbusel@gmail.com.

С диссертацией можно ознакомиться в библиотеке Государственного научного учреждения ”Институт математики Национальной академии наук Беларуси”.

Автореферат разослан ”14” декабря 2022 г.

Ученый секретарь
совета по защите диссертаций Д 01.02.01
кандидат физико-математических наук Т.С. Бусел

ВВЕДЕНИЕ

Алгоритмическая теория чисел изучает вычислительные методы для исследования и решения задач теории чисел, например алгоритмы для проверки на простоту, целочисленной факторизации, нахождения решений диофантовых уравнений. Интерес к алгоритмической теории чисел вызван тем, что она активно используется на практике, например в криптосистемах.

Во второй половине XX века начала активно развиваться информатика и криптография, что привело к увеличению активности работы в области алгоритмической теории чисел со стороны ведущих математиков. В частности, были получены принципиально новые критерии простоты, приводящие к эффективным алгоритмам тестирования простоты и генерации больших простых чисел. Примерами таких критериев служат критерий Эйлера и Миллера, приводящие к алгоритму Соловея-Штрассена и Миллера-Рабина соответственно. В предположении справедливости расширенной гипотезы Римана в работе Н. Анкени была доказана теорема, позволяющая получить детерминированный вариант алгоритма Миллера-Рабина.

В 2002 году в работе М. Агравала, Н. Каяла и Н. Саксены было конструктивно доказано, что задача проверки на простоту в кольце целых чисел решается за полиномиальное относительно размера входных данных время. Задача проверки на простоту существенно усложняется при переходе от целых чисел к более общим алгебраическим структурам. Был получен полиномиальный детерминированный алгоритм проверки на простоту в конечнопорожденных дедекиндовых кольцах.

В диссертации доказываются новые критерии простоты идеалов в дедекиндовых кольцах. Эти критерии являются аналогами критериев Эйлера и Миллера и позволяют строить эффективные тесты на простоту в дедекиндовых кольцах.

Алгоритм Евклида используется во многих теоретико-числовых алгоритмах, в частности при решении различных диофантовых уравнений. Важным является исследование экстремальных свойств этого алгоритма, а именно длины получаемых при его выполнении цепочек делений. Для кольца целых чисел известна теорема Кронекера-Валена о том, что цепочка делений с выбором минимального по абсолютной величине остатка является кратчайшей. Вопрос оптимальности цепочек деления с выбором минимального по норме остатка решен в кольце гауссовых чисел, кольце многочленов, мнимых

квадратичных кольцах, что показано в работах Э. Баха, Э. Калтофена, Г. Роллетчека и Д. Лазара. Задача проверки теоремы Кронекера-Валена к мнимых квадратичных кольцах существенно сложнее задачи в кольце целых чисел, так как существует мнимое квадратичное кольцо, в котором эта теорема не выполняется. Методы доказательства для мнимых квадратичных колец связаны с представлением элементов кольца точками на плоскости и не подходят для действительных квадратичных колец. Задача становится еще сложнее ввиду того, что в кольцах с бесконечной группой единиц длину кратчайшей цепочки делений можно ограничить сверху константой.

В диссертации разработаны новые подходы к исследованию экстремальных свойств цепочек делений в факториальных кольцах. Первый подход позволил разработать метод автоматического доказательства теоремы Кронекера-Валена в факториальных кольцах. Второй подход позволил решить проблему проверки теоремы Кронекера-Валена в квадратичных кольцах. Установлено, что теорема Кронекера-Валена выполняется в квадратичном норменно-евклидовом кольце $\mathcal{O}_{\mathbb{Q}[\sqrt{d}]}$ тогда и только тогда, когда $d \in \{-1, -2, -3, -7\}$.

Особый интерес представляет криптосистема RSA, так как ее идея достаточно проста, но при этом стойкость криптосистемы RSA основана на фундаментальной задаче факторизации. Впервые она была предложена Р.Л. Ривестом, А. Шамиром и Л.М. Адлеманом в 1977 году. При изучении криптосистемы RSA можно выделить два типа задач: использование криптосистемы RSA в кольцах более общего вида и получение необходимых условий криптостойкости. Известны аналоги криптосистемы RSA в кольце гауссовых чисел, кольце многочленов, дедекиндовых кольцах. В работе К.А. Петуховой и С.Н. Тронина предложено обобщение криптосистемы RSA на случай дедекиндовых колец.

В диссертации доказываются обобщения теорем Винера, Кранакиса, необходимых условий криптографической стойкости криптосистемы RSA в дедекиндовых кольцах.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с научными программами (проектами), темами

Исследования проводились в рамках следующих научных проектов:

- Анализ асимптотических свойств решений дифференциальных и алгебраических систем (2016–2020 гг., номер госрегистрации 20162496);
- Анализ общих и асимптотических свойств решений стохастических дифференциальных уравнений с приложениями в криптографии и теории кредитных рисков (2021–2025 гг., номер госрегистрации 20213106)

Цель, задачи, объект и предмет исследования

Целью диссертации является доказательство новых критериев простоты идеалов в дедекиндовых кольцах и исследование свойств теоретико-числовых и криптографических алгоритмов в дедекиндовых кольцах. Предметом исследования являются арифметические свойства идеалов в дедекиндовых кольцах.

Научная новизна

В диссертации 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 теоремы о длине цепочек делений; впервые исследованы свойства криптосистемы RSA в дедекиндовых кольцах и доказаны аналоги теоремы Винера, теоремы Кранакиса и другие теоремы о необходимых условиях криптостойкости криптосистемы RSA в дедекиндовых кольцах.

Положения, выносимые на защиту

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.

Личный вклад соискателя ученой степени

Работы [3; 5; 9; 10; 11; 14], написанные в соавторстве с Н.П. Прохоровым и научным руководителем М.М. Васьковским, посвящены исследованию простых элементов и идеалов в кольцах. Автору диссертации принадлежит разработка подхода, позволяющего переносить доказательства критериев простоты на различные классы колец. Н.П. Прохорову принадлежит применение этих подходов для конкретных классов колец, указанных в

работе. Научному руководителю М.М. Васьковскому принадлежит постановка задачи, выбор методов исследования и обсуждение полученных результатов.

Работы [1; 4; 7; 8], написанные в соавторстве с научным руководителем М.М. Васьковским, посвящены исследованию экстремальных свойств алгоритма Евклида в различных классах колец. Результаты, полученные в этих работах получены автором самостоятельно. Научному руководителю М.М. Васьковскому принадлежит постановка задачи, выбор методов исследования и обсуждение полученных результатов.

Работы [2; 6; 12; 13], написанные в соавторстве с научным руководителем М.М. Васьковским, посвящены исследованию свойств аналогов криптосистемы RSA в различных кольцах. Результаты, полученные в этих работах получены автором самостоятельно. Научному руководителю М.М. Васьковскому принадлежит постановка задачи, выбор методов исследования и обсуждение полученных результатов.

Апробация диссертации и информация об использовании ее результатов

Результаты работы докладывались и обсуждались на республиканском конкурсе работ исследовательского характера (Минск, 2013, 2014, 2015), на научно-инженерном конкурсе учащихся BelSEF (Минск, 2013, 2014, 2015), на балтийском научно-инженерном конкурсе (Санкт-Петербург, 2013, 2014, 2015), на XVI Республиканской научной конференции студентов и аспирантов (Гомель, 2013), на международной конференции EUCYS 2014 (Варшава, 2014), на международном конкурсе Intel ISEF (Лос-Анджелес, 2014), на международной конференции ICYS (Измир, 2015), на международной научной конференции ”XII Белорусская математическая конференция” (Минск, 2016), на всероссийской конференции ”Алгебра и теория алгоритмов”, посвященной 100-летию факультета математики и компьютерных наук Ивановского государственного университета (Иваново, 2018), на международной научной конференции ”XIII Белорусская математическая конференция” (Минск, 2021), на международном конгрессе по информатике CSIST’2022 (Минск, 2022).

Результаты, включенные в диссертацию, отмечены дипломами 1 степени за успешное выступление на республиканском конкурсе работ исследовательского характера (2013, 2014, 2015), дипломами 1 и 3 степени на научно-инженерном конкурсе учащихся BelSEF (2013, 2014, 2015), дипломами 1 степени и дипломами лауреата на балтийском научно-инженерном конкурсе (2013, 2014, 2015), Mu Alpha Theta Award за работу на BelSEF-2014 (2014), дипломом лауреата конкурса факультета прикладной математики и

информатики на лучшую студенческую научную работу за 2016 год (2017), грамотой за конкурс лучших научных работ студентов БГУ за 2017 год (2018), дипломом 1-й категории XXIV республиканского конкурса научных работ студентов (2018), второй премией Специального фонда Президента Республики Беларусь по социальной поддержке одаренных учащихся и студентов (2018), дипломом 1-й премией конкурса факультета прикладной математики и информатики на лучшую студенческую научную работу за 2017 год (2018), дипломом лауреата конкурса факультета прикладной математики и информатики на лучшую студенческую научную работу за 2018 год (2019), дипломом 1-й категории XXV республиканского конкурса научных работ студентов (2019), второй премией Специального фонда Президента Республики Беларусь по социальной поддержке одаренных учащихся и студентов (2019), дипломом лауреата XXVI республиканского конкурса научных работ студентов (2020), свидетельством о назначении стипендии Президента Республики Беларусь магистранту Белорусского государственного университета (2020).

Результаты диссертации внедрены в учебный процесс БГУ, что подтверждается актом о практическом использовании результатов исследования в образовательном процессе №24/14 от 26.01.2021 г.

Опубликованность результатов диссертации

Основные научные результаты диссертационного исследования опубликованы в полной мере в 14 научных работах, среди которых: 7 статей в научных изданиях в соответствии с пунктом 19 Положения о присуждении ученых степеней и присвоении ученых званий в Республике Беларусь, 4 из которых входят в наукометрические базы данных Scopus и Web of Science (общим объемом 4 авторских листа), 7 статей в сборниках трудов научных конференций.

Структура и объем диссертации

Диссертация состоит из перечня условных обозначений, введения, общей характеристики работы, основной части, включающей 4 главы, заключения, библиографического списка, приложений, включающих код программы, использующийся в работе, и документы о практическом применении результатов диссертации. Полный объем диссертации — 102 страницы, библиографический список содержит 62 наименования, включая собственные публикации автора, на 6 страницах, приложения занимают 14 страниц.

ОСНОВНАЯ ЧАСТЬ

В *первой главе* приводится обзор литературных источников по теме диссертации.

Основным объектом исследования *второй главы* диссертации являются простые идеалы в дедекиндовых кольцах.

Пусть характер χ задан на множестве идеалов кольца R, не является главным и определен по модулю идеала $\mathfrak{n} \subset R$. Через $\mathfrak{p}_\chi$ обозначим идеал минимальной нормы, для которого $\chi(\mathfrak{p}_\chi) \neq 0, 1$.

Пусть R дедекиндово кольцо с полем частных K. Пусть L расширение поля K степени не меньше 2. Будем говорить, что кольцо R *удовлетворяет условию A для идеала* $\mathfrak{n}$, если существует многочлен f_R, что для любого характера χ, не являющегося главным и определенного по модулю $\mathfrak{n}$, выполнено

$$\mathrm{Nm}(\mathfrak{p}_\chi) \leq f_R(\log \mathrm{Nm}(\mathfrak{n})).$$

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

$$a^{\frac{\mathrm{Nm}(\mathfrak{n})-1}{2}} \equiv \left(\frac{a}{\mathfrak{n}}\right) \pmod{\mathfrak{n}}.$$

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

$$a^{\frac{\mathrm{Nm}(\mathfrak{n})-1}{2}} \equiv \left(\frac{a}{\mathfrak{n}}\right) \pmod{\mathfrak{n}}.$$

Алгоритм 2.1 Дан нетривиальный идеал $\mathfrak{n} \subset R$. Необходимо определить является ли он простым.

1. Вычислить $\mathrm{Nm}(\mathfrak{n})$;
2. Выбрать случайное $a \in I_{R/\mathfrak{n}}$;
3. Вычислить $r_0 \equiv a^{\frac{\mathrm{Nm}(\mathfrak{n})-1}{2}} \pmod{\mathfrak{n}}$, $r_1 = \left(\frac{a}{\mathfrak{n}}\right)$;
4. Если $r_0 \equiv r_1 \pmod{\mathfrak{n}}$, то вернуть "неизвестно" и завершить алгоритм;
5. Вернуть "$\mathfrak{n}$ не простой" и завершить алгоритм.

Замечание 2.11 Алгоритм 2.1 является вероятностным. Если был получен ответ "неизвестно", то можно выполнить алгоритм еще раз.

Предложение 2.10 Пусть $\mathfrak{n}$ – не простой идеал. Тогда вероятность ответа "$\mathfrak{n}$ не простой" у алгоритма 2.1 не менее $1/2$.

Замечание 2.12 Если $\mathfrak{n}$ – составной, то при выполнении алгоритма 2.1 k раз вероятность получить ответ "$\mathfrak{n}$ не простой" не меньше $1 - \frac{1}{2^k}$.

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

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

Алгоритм 2.2 Дан идеал $\mathfrak{n} \subset R$. Необходимо определить является ли он простым.

1. Найти $u, t \in \mathbb{N}$, что $\mathrm{Nm}(\mathfrak{n}) - 1 = 2^t u$ и $(2, u) = 1$;
2. Выбрать случайный $a \in I_{R/\mathfrak{n}}$;
3. Вычислить $r_0 \equiv a^u \pmod{\mathfrak{n}}$;
4. Если $r_0 = 1$, то вернуть "неизвестно" и завершить алгоритм;
5. Положить $k = 0$;
6. Пока $k < t$ выполнять:
   а) Если $r_k = -1$, то вернуть "неизвестно" и завершить алгоритм;
   б) Увеличить k на 1;
   в) Вычислить $r_{k+1} \equiv r_k^2 \pmod{\mathfrak{n}}$;
7. Вернуть "$\mathfrak{n}$ не простой" и завершить алгоритм.

Замечание 2.13 Алгоритм 2.2 является вероятностным. Если был получен ответ "неизвестно", то можно выполнить алгоритм еще раз.

Предложение 2.11 Пусть $\mathfrak{n}$ – не простой идеал. Тогда вероятность ответа "$\mathfrak{n}$ не простой" у алгоритма 2.2 не менее $1/2$.

Замечание 2.14 Если $\mathfrak{n}$ – составной, то при выполнении алгоритма 2.2 k раз вероятность получить ответ "$\mathfrak{n}$ не простой" не меньше $1 - \frac{1}{2^k}$.

Предложение 2.12 Пусть K числовое поле и R кольцо целых алгебраических элементов числового поля K. Пусть $\mathfrak{n} \subseteq R$ идеал кольца R. Для того, чтобы использовать алгоритм 2.1 для $\mathfrak{n}$ требуется полиномиальное относительно $\log^2 l(\mathfrak{n})$ количество арифметических операций в $\mathbb{Z}$.

Предложение 2.13 Пусть $\mathfrak{n} \subseteq R$ идеал дедекиндового кольца R. Для того, чтобы использовать алгоритм 2.2 для $\mathfrak{n}$ требуется $O(\log \mathrm{Nm}(\mathfrak{n}))$ арифметических операций.

Пусть K числовое поле и R кольцо целых алгебраических элементов числового поля K. Пусть $\mathfrak{n} \subseteq R$ идеал кольца R. Для того, чтобы использовать алгоритм 2.2 для $\mathfrak{n}$ требуется $\tilde{O}(\log^2 l(\mathfrak{n}))$ бинарных операций.

Третья глава диссертации посвящена доказательству экстремальных свойств алгоритма Евклида в факториальных кольцах.

Определение 3.1 Пусть R факториальное кольцо и $a, b \in R$. Рассмотрим произвольные $k \in \mathbb{N}$ и $q_1, \ldots, q_k \in R$. Обозначим $r_{-1} = a$, $r_0 = b$, $r_i = r_{i-2} - q_i r_{i-1}$, для $i = 1, \ldots, k$. Выражение

$$\mathcal{D}_{a,b}(q_1, \ldots, q_k) = (r_{-1}, r_0, \ldots, r_{k-1}, r_k) \in R^{k+2}$$

будем называть *цепочкой делений* для $a, b \in R$.

Определение 3.2 Пусть a и b ненулевые элементы факториального кольца R. Цепочку делений, для которой $q_i = \text{int}\,(r_{i-2}/r_{i-1})$ для любого $i = 1, \ldots, k$, будем называть *цепочкой делений с выбором минимального по норме остатка* для $a, b \in R$.

Через $\mathcal{L}_{a,b}$ обозначим длину цепочки делений с выбором минимального по норме остатка для $a, b \in R$, если она существует. Если такой цепочки не существует, то будем считать, что $\mathcal{L}_{a,b} = \infty$.

Определение 3.3 Пусть $a, b \in R^*$. Обозначим через $\mathcal{l}_{a,b}$ длину кратчайшей цепочки делений для $a, b \in R^*$.

$$\mathcal{l}_{a,b} = \min\left(\left\{k \middle| \mathcal{D}_{a,b}(q_1, \ldots, q_k) = (r_{-1}, \ldots, r_k), r_k = 0\right\} \cap \{\infty\}\right)$$

Определение 3.4 Через $l_n(R)$ обозначим максимальную длину цепочки делений с выбором минимального по норме остатка для $a, b \in R^*$ с ограниченной нормой.

$$l_n(R) = \max\left\{\mathcal{L}_{a,b} \middle| a, b \in R^*, \upsilon(a) \leq \upsilon(b) \leq n\right\}.$$

Определение 3.5 Определим функцию $\omega : F_1 \to F_1$ следующим образом

$$\omega(\alpha) = \begin{cases} \text{fr}\left(\alpha^{-1}\right), \text{ если } \alpha \neq 0 \\ 0, \text{ если } \alpha = 0 \end{cases}$$

Определение 3.6 Будем говорить, что $(x_0, \alpha, n) \in R^* \times F_1^* \times \mathbb{N}$ – *регулярная тройка*, если существуют $p, l \in \mathbb{N}$, $p \leq n$ и $l \leq p + 1$, $\varepsilon_i \in I_R$, $b_i, c_i \in R$ для $i = 1, \ldots, l-1$, $\varepsilon \in \{0, 1\}$, для которых выполнены следующие условия $\beta_1 = \omega^{(p)}\left(\text{fr}\left((\alpha - x_0)^{-1}\right)\right)$, $\beta_{i+1} = (\varepsilon_i \beta_i + c_i)^{-1} + b_i$, $i = 1, \ldots, l-1$, $\beta_l = \alpha^{(-1)^\varepsilon}$.

Определение 3.7 Через $\mathcal{T}$ обозначим множество всех таких факториальных колец R, для которых существует $D_R \in \mathbb{N}$, что выполнено 1) для всех $x_0 \in R^*$, $\alpha \in F_1^*$ тройка $(x_0, \alpha, D_R - 1)$ регулярная; 2) если $D_R \geq 3$, то для любого $k \in [3, D_R] \cap \mathbb{N}$ и любых $x_0 \in R^*, \alpha \in F_1^*$ из равенства $\omega^{(k-2)}(\text{fr}\left((\alpha - x_0)^{-1}\right)) = 0$ следует, что тройка $(x_0, \alpha, k-2)$ регулярная.

Определение 3.8 Обозначим $[x_1 : x_2 : \cdots : x_k] = x_1 + 1/(x_2 + 1/(x_3 + 1/(\cdots + 1/x_k)))$. Будем говорить, что для $\alpha \in F$ и $k \in \mathbb{N}$ имеет место (α, k)-разрешимость, если разрешимо уравнение $\alpha = [x_1 : x_2 : \cdots : x_k]$.

Теорема 3.1 Пусть $R \in \mathcal{T}$, $a, b \in R^*$. Тогда $\mathcal{L}_{a,b} = \mathcal{l}_{a,b}$.

Пусть дано некоторое факториальное кольцо R. Рассмотрим алгоритм проверки принадлежности этого кольца классу T.

Определение 3.9 Через $\mathcal{S}$ обозначим множество всех таких факториальных колец R, что для всех $x \in R^*$ и $\alpha \in F_1^*$ выполнено $\text{int}\left((\alpha - x)^{-1}\right) \in I_R \cup \{0\}$ или $x\text{int}\left((\alpha - x)^{-1}\right) + 1 \in I_R$.

Лемма 3.3 Множество $\mathcal{S}$ содержится в $\mathcal{T}$.

Используя доказанную выше лемму, сформулируем метод проверки включения $R \in \mathcal{T}$.

Алгоритм 3.1 На вход подается факториальное кольцо R.

1. Построить множество
$$J = \left\{x \in R^* \middle| \forall \alpha \in F_1^*, \text{int}\left((\alpha - x)^{-1}\right) \in I_R \cup \{0\}\right\}$$
2. Для каждого $x_0 \in R^* \setminus J$ построить множество
$$Y(x_0) = \left\{f_{x_0}(\alpha) = \text{int}\left((\alpha - x_0)^{-1}\right) | \alpha \in F_1^*\right\}$$
3. Для каждого $x_0 \in R^* \setminus J$ построить множество
$$U(x_0) = \left(\left\{\frac{\varepsilon - 1}{x_0} | \varepsilon \in I_R\right\} \cap R\right) \cup I_R$$
4. Если $Y(x_0) \subseteq U(x_0)$ для всех $x_0 \in R^* \setminus J$, то ответ "$R \in \mathcal{T}$", иначе ответ "неизвестно"

Предложение 3.1 Если алгоритм 3.1 вернул ответ "$R \in \mathcal{T}$", то $R \in \mathcal{T}$.

Приведем общий метод проверки включения $R \in \mathcal{T}$.

Алгоритм 3.2 На вход подается факториальное кольцо R.

1. Выбрать $D_R, M \in \mathbb{N}$
2. Построить множество
$$J = \left\{x_0 \in R \middle| \text{int}\left(\frac{1}{\alpha - x_0}\right) \in I_R \cup \{0\} \forall \alpha \in F^*\right\}$$

3. Создать список L, в котором будут храниться элементы из R^i, где $i \in \{1, \ldots, D_R - 1\}$
4. Вычислить $L = R^* \setminus J$. Мы будем хранить элементы из L, в которых более двух компонент в множестве L_M
5. Выбрать элемент $(x_0, \ldots, x_l) \in L$ и удалить его из L
6. Вычислить

$$\delta = \left(\left(\ldots \left((\alpha - x_0)^{-1} - x_1 \right)^{-1} - \ldots \right)^{-1} - x_l \right)^{-1}$$

7. Построить множество $A = \left\{ b \in R \middle| b = \text{int}\,(\delta) \right\}$
8. Для каждого элемента $x_{l+1} \in A$ выполнить
   а) Вычислить $\beta_1 = \omega^{(l+1)} \left(\text{int} \left((\alpha - x_0)^{-1} \right) \right) = \text{fr} \left((\delta - x_{l+1})^{-1} \right)$
   б) Попробовать найти такие $(\varepsilon_i) \in I_R$ и $(a_i), (b_i) \in R$, что $\upsilon(a_i), \upsilon(b_i) \leq M$ и $\beta_{i+1} = \frac{1}{\varepsilon_i \beta_i + a_i} + b_i$, $\beta_{l+2} = \alpha$ или $\beta_{l+2} = \alpha^{-1}$.
   в) Если такие элементы не нашлись и $l + 1 \geq D_R - 1$, то вернуть "выберите большие D_R и M" и завершить алгоритм
   г) Если такие элементы не нашлись и $l + 1 < D_R - 1$, то добавить в множество L элемент $(x_0, \ldots, x_l, x_{l+1})$
   д) Если такие элементы нашлись, то перейти к следующему элементу в шаге 8.
9. Если множество L не пустое, то выбрать другой элемент на шаге 5.
10. Если множество L пустое и $D_R < 3$, то вернуть "$R \in \mathcal{T}$" и завершить алгоритм
11. Для всех $k \in [3, D_R]$
    а) Построить множество

$$B = \left\{ \alpha \in F^* \middle| \omega^{(k-2)} \left(\text{fr} \left((\alpha - x_0)^{-1} \right) \right) = 0 \right\}$$

    б) Для всех $\alpha_0 \in B$ попробовать найти такие $(\varepsilon_i) \in I_R$ и $(a_i), (b_i) \in R$, что $\upsilon(a_i), \upsilon(b_i) \leq M$ и $\beta_{i+1} = \frac{1}{\varepsilon_i \beta_i + a_i} + b_i$, $\beta_{k-1} = \alpha$ или $\beta_{k-1} = \alpha^{-1}$, где $\beta_1 = 0$
    в) Если такие элементы не были найдены, то вернуть "выберите большие D_R и M" и завершить алгоритм
    г) Если такие элементы были найдены и проверены все $x_0 \in L$, то вернуть "$R \in \mathcal{T}$" и завершить алгоритм

Предложение 3.2 Пусть алгоритм 3.2 вернул "$R \in \mathcal{T}$". Тогда $R \in \mathcal{T}$.

Теперь рассмотрим задачу проверки выполнимости теоремы Кронекера-Валена с другой стороны. Следующий алгоритм позволяет находить наименьший остаток при делении двух элементов $\mathcal{O}_K$.

Алгоритм 3.3 Дано числовое поле K и два элемента $a, b \in \mathcal{O}_K$. Необходимо вычислить наименьший остаток r при делении a на b.

1. Вычислить $x = \Phi(a/b) \in \Phi(K)$;
2. Вычислить $\mathrm{Orb}(x)$;
3. Выбрать произвольное действительное $k > 0$;
4. Вычислить $\Gamma(k)$;
5. Объявить переменные z' и Z', которые будут инициализированы позже;
6. Для всех $z \in \mathrm{Orb}(x)$
   а) Вычислить $\mathcal{I}_{z,k}$;
   б) Для всех $Z \in \mathcal{I}_{z,k}$, если z' и Z' не инициализированы или $\mathcal{N}(z' - Z') > \mathcal{N}(z - Z)$ положить $z' = z$ и $Z' = Z$;
7. Вычислить $\mathcal{M}_k = \mathcal{N}(z' - Z')$
8. Если $\mathcal{M}_k > k$, то положить $k = \mathcal{M}_k$ и перейти к шагу 4.
9. Вычислить $\mathrm{int}\left(\frac{a}{b}\right) = Z'\Phi((\varepsilon'_z)^{-1})$
10. Вернуть $r = a - b\mathrm{int}\left(\frac{a}{b}\right)$

Предложение 3.3 Пусть $a, b \in \mathcal{O}_K^*$. Тогда алгоритм 3.3 позволяет вычислить наименьший по норме остаток r при делении a на b за $O(1)$ арифметических операций в K.

Имея алгоритм деления с выбором минимального по норме остатка, можно сформулировать метод автоматического доказательства невыполнимости теоремы Кронекера-Валена в кольце целых алгебраических элементов числового поля K.

Алгоритм 3.4 Дано числовое поле K. Требуется доказать, что теорема Кронекера-Валена не выполняется в $\mathcal{O}_K$.

1. Взять произвольные $a, b \in \mathcal{O}_K$;
2. Вычислить цепочку делений с выбором минимального по норме остатка $\mathcal{D}_{a,b}$, используя алгоритм 3.3;
3. Найти такое $c \in \mathcal{O}_K$, что $a = bx + c$ для некоторого $x \in \mathcal{O}_K$;
4. Вычислить цепочку делений с выбором минимального по норме остатка $\mathcal{D}'_{b,c}$, используя алгоритм 3.3;
5. Если $\mathrm{len}(\mathcal{D}_{a,b}) > \mathrm{len}(\mathcal{D}'_{b,c}) + 1$, то теорема Кронекера-Валена не выполняется в $\mathcal{O}_K$.

Теорема 3.2 Пусть поле K такое, что $\mathcal{O}_K$ действительное квадратичное

норменно-евклидово кольцо. Тогда теорема Кронекера-Валена не выполняется в $\mathcal{O}_K$.

Следствие 3.1 Пусть $R = \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ – квадратичное норменно-евклидово кольцо. Теорема Кронекера-Валена выполняется в R тогда и только тогда, когда $d = -1, -2, -3, -7$.

Определение 3.12 Для $m/n \in F_1$ рассмотрим функцию

$$|m/n| = \begin{cases} \frac{\upsilon(m)}{\upsilon(n)}, & m \neq 0, (m,n) = 1 \\ 0, & m = 0 \end{cases}.$$

Обозначим $\Lambda_K = \sup_{m/n \in F_1} |m/n|$.

Теорема 3.3 Если R – евклидово кольцо относительно нормы $\upsilon(\cdot)$, то $\Lambda_R \in [0,1]$.

Если R – факториальное кольцо с мультипликативной нормой $\upsilon(\cdot)$ и $\Lambda_R \in [0,1)$, то R – евклидово относительно нормы $\upsilon(\cdot)$ и $l_n(R) \leq [\log_{\Lambda_R^{-1}} n] + 2$ для всех $n \in \mathbb{N}$, где $\log_\infty n = 0$.

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

Четвертая глава диссертации посвящена доказательству необходимых условий для параметров криптосистемы RSA для обеспечения ее криптостойкости.

Изложенный далее алгоритм аналога криптосистемы RSA был предложен в работе Петуховой и Тронина. Была показана корректность полученной криптосистемы и представлены ограничения на кольцо для ее эффективного применения. В этой части исследуется криптосистема RSA в дедекиндовых кольцах с конечным полем остатков. Целью является получение доказательств теорем, связанных с ее криптостойкостью. Например теоремы Винера, теоремы об эквивалентности факторизации и взлома криптосистемы, а так же изучение методов взлома криптосистемы.

Алгоритм 4.1 [1] Аналог криптосистемы RSA в дедекиндовых кольцах.

1. Выбрать максимальные идеалы $\mathfrak{p}, \mathfrak{q} \subset R$
2. Вычислить $\varphi(\mathfrak{N})$, где $\mathfrak{N} = \mathfrak{pq}$
3. Выбрать случайное целое $e \in [1, \varphi(\mathfrak{N})]$, $(e, \varphi(\mathfrak{N})) = 1$
4. Вычислить целое положительное d такое, что $ed \equiv 1 \pmod{\varphi(\mathfrak{N})}$

[1] Petukhova, K.A. RSA Cryptosystem for Dedekind Rings / K.A. Petukhova, S.N. Tronin // Lobachevskii Journal of Mathematics. — 2016. — V. 37. — P. 284-287.

Пара $(\mathfrak{N}, e)$ это публичный ключ A, пара $(\mathfrak{N}, d)$ секретный ключ A. Функцией шифрования называется

$$f : R/\mathfrak{N} \to R/\mathfrak{N}, f(x) \equiv x^e \pmod{\varphi(\mathfrak{N})}.$$

Функцией расшифрования называется

$$f^{-1} : R/\mathfrak{N} \to R/\mathfrak{N}, f^{-1}(x) \equiv x^d \pmod{\varphi(\mathfrak{N})}.$$

Замечание 4.1 Корректность приведенной криптосистемы гарантируется аналогом теоремы Эйлера для дедекиндовых колец.

Зная разложение на множители $\mathfrak{N} = \mathfrak{pq}$ модуля криптосистемы RSA и используя алгоритм 4.1, можно эффективно найти секретный ключ. Для того чтобы показать связь задачи факторизации и взлома криптосистемы необходимо чтобы существовал алгоритм, позволяющий найти множители идеала $\mathfrak{N}$ по известному секретному ключу.

Теорема 4.1 Пусть K – числовое поле и $\mathcal{O}_K$ его кольцо целых алгебраических элементов. Пусть $\mathcal{O}_K$ – кольцо с единственной факторизацией, $((N), e, d)$ параметры криптосистемы RSA в $\mathcal{O}_K$ и d известно. Тогда существует вероятностный алгоритм, позволяющий найти множители N за полиномиальное относительно длины бинарной записи N количество арифметических операций в $\mathbb{Z}$ с вероятностью не менее $\frac{1}{2}$.

Теорема Винера о малой секретной экспоненте утверждает, что, если секретная экспонента в криптосистеме RSA слишком маленькая относительно N, то секретную экспоненту можно эффективно вычислить. Докажем аналог теоремы Винера для случая криптосистемы RSA в дедекиндовых кольцах.

Теорема 4.2 Пусть $(\mathfrak{N}, e, d)$, $\mathfrak{N} = \mathfrak{pq}$ – параметры криптосистемы RSA в дедекиндовом кольце R. Пусть $\mathrm{Nm}(\mathfrak{q}) < \mathrm{Nm}(\mathfrak{p}) < \alpha^2\mathrm{Nm}(\mathfrak{q})$, где $\alpha > 1$, $d < \frac{1}{\sqrt{2\alpha+2}}(\mathrm{Nm}(\mathfrak{N}))^{1/4}$. Тогда существует алгоритм, позволяющий найти d за полиномиальное относительно $\log \mathrm{Nm}(\mathfrak{N})$ число бинарных операций.

Доказанная выше теорема является основой для атаки Винера на криптосистему RSA. При соблюдении определенных условий на параметры криптосистемы, можно сделать использование этой атаки невозможным. Однако существуют атаки, от которых невозможно полностью защититься.

Метод повторного шифрования является примером такой атаки. Предположим, что было перехвачено некоторое зашифрованное сообщение $y = x^e \pmod{\mathfrak{N}}$, где $x \in \mathcal{O}_K/\mathfrak{N}$ – некоторое сообщение. Построим последовательность $y_i = y^{e^i} \pmod{\mathfrak{N}}$, где $i \in \{1, 2, \ldots\}$. Используя свойства

возведения в степень и то, что $\mathcal{O}_K/\mathfrak{N}$ конечно, получаем, что существует такое $m \in \mathbb{N}$, что $y_m = y$. Тогда $y_{m-1} = x$.

Единственный способ защиты от этого метода взлома состоит в том, чтобы сделать m достаточно большим.

Теорема 4.3 Пусть $\mathfrak{N} = \mathfrak{pq}$ – модуль криптосистемы RSA в дедекиндовом кольце R. Пусть существуют простые числа r, s, $r \neq s$ и $k, l \in \mathbb{Z}$, $k, l > 0$, что $\varphi(\mathfrak{p}) = rk$, $\varphi(\mathfrak{q}) = sl$. Пусть $r-1$, $s-1$ имеют различные простые делители r_1, s_1 соответственно.

Пусть y и e – независимые равномерно распределенные случайные величины со значениями в $R/\mathfrak{N}$ и $I_{\mathbb{Z}_{\varphi(\mathfrak{N})}}$ соответственно. Обозначим

$$m_{e,y} = \min\{m \in \mathbb{N} | y_m = y\}.$$

Тогда

$$P(m_{e,y} \geq r_1 s_1) \geq (1 - r^{-1})(1 - s^{-1})(1 - r_1^{-1})(1 - s_1^{-1}).$$

Теорема 4.4 Пусть $(\mathfrak{N}, e, d)$ параметры криптосистемы RSA в дедекиндовом кольце R, где $\mathrm{Nm}(\mathfrak{p})$ и $\mathrm{Nm}(\mathfrak{q})$ имеют одинаковую битовую длину. Пусть $ed \leq (\mathrm{Nm}(\mathfrak{N}))^2$, $\mathrm{Nm}(\mathfrak{N}) \geq 3$. Пусть d известно. Тогда существует эффективный алгоритм, позволяющий найти $\mathrm{Nm}(\mathfrak{p})$ и $\mathrm{Nm}(\mathfrak{q})$.

Замечание 4.2 Если в условии теоремы 4.4 заменить неравенство $ed \leq (\mathrm{Nm}(\mathfrak{N}))^2$ на более строгое $ed \leq (\mathrm{Nm}(\mathfrak{N}))^{3/2}$, то получим, что

$$k - \overline{k} < 6(\mathrm{Nm}(\mathfrak{N}))^{-3/2}(ed - 1) < 6.$$

Следовательно, вычислив $\overline{k} = \frac{ed-1}{\mathrm{Nm}(\mathfrak{N})}$, можно перебрать все возможные k и для каждого вычислить $\varphi(\mathfrak{N})$, $\mathrm{Nm}(\mathfrak{p})$, $\mathrm{Nm}(\mathfrak{q})$.

Теорема 4.5 Пусть дедекиндово кольцо R является евклидовым относительно некоторой нормы $\upsilon(\cdot)$ и $\Lambda_R < 1$, где Λ_R задано в определении 3.12. Тогда это кольцо главных идеалов. Для простоты будем обозначать идеалы соответствующими элементами кольца.

Пусть (N, e_1, d_1) и (N, e_2, d_2) параметры криптосистемы RSA в R и $(e_1, e_2) = 1$. Пусть известны $c_1 \equiv m^{e_1} \pmod N$ и $c_2 \equiv m^{e_2} \pmod N$. Тогда существует алгоритм, позволяющий вычислить m за полиномиальное относительно $\log \upsilon(N)$ количество арифметических операций в R.

Пусть R кольцо целых алгебраических элементов числового поля $K = \mathbb{Q}(\theta)$. Будем предполагать, что поле K фиксировано и, следовательно, известен индекс $[R : \mathbb{Z}[\theta]]$. А так же разложение на простые идеалы всех

простых делителей индекса. В этом случае, используя теорему Дедекинда можно построить полиномиальное сведение задачи факторизации идеала к задаче факторизации целых чисел.

Алгоритм 4.2 Алгоритм факторизации идеала (N) числового кольца, заданного в форме 2-представления.

1. Вычислить норму идеала, равную норме элемента N.
2. Найти разложение нормы на множители используя один из известных алгоритмов для факторизации целых чисел:

$$n = \mathrm{Nm}(N) = \prod_{i=1}^{k} p_i^{\alpha_i}.$$

Тогда

$$(\mathrm{Nm}(N)) = \prod_{i=1}^{k} (p_i)^{\alpha_i}.$$

3. Найти разложение идеала (p_i) на множители, используя теорему Дедекинда:

$$(p_i) = \prod_{j=1}^{l_i} (p_i, f_{i,j}(\theta)).$$

4. Преобразовать идеалы $(p_i, f_{i,j}(\theta))$ в $\mathbb{Z}$-представление и найти равные:

$$(\mathrm{Nm}(N)) = \prod_{i=1}^{l} \mathfrak{p}_i^{\beta_i}.$$

5. Найти степени, в которых $\mathfrak{p}_i$ входит в (N), используя бинарный поиск.

Предложение 4.1 Разложить идеал (p), используя теорему Дедекинда, можно за $O((n \log n + \log p) n \log n \log\log n \log^2 p)$ бинарных операций.

Замечание 4.4 Следовательно, разложение идеала $(\mathrm{Nm}(N))$ на множители можно найти за полиномиальное относительно $\log \mathrm{Nm}(N)$ количество бинарных операций, если разложение $\mathrm{Nm}(N)$ на множители известно.

ЗАКЛЮЧЕНИЕ

Основные научные результаты диссертации

Работа посвящена исследованию свойств теоретико-числовых и криптографических алгоритмов в дедекиндовых кольцах. В частности, получены следующие результаты.

1. Доказаны критерии простоты идеалов в дедекиндовых кольцах, аналогичные критериям Эйлера и Миллера в кольце целых чисел. Показано, что полученные критерии можно использовать для построения эффективных вероятностных алгоритмов проверки идеала на простоту. Получены достаточные условия для дедекиндового кольца для того, чтобы этот алгоритм можно было модифицировать и сделать детерминированным. Получены оценки вычислительной сложности алгоритмов. Эти результаты получены в работах [3; 5; 9; 10; 11; 14] и изложены в главе 2.
2. Доказаны теоремы об экстремальных свойствах алгоритма Евклида в факториальных кольцах. Получен класс колец, в которых верна теорема Кронекера-Валена. Разработан алгоритм, позволяющий проверить принадлежность кольца этому классу колец. Построен метод автоматического доказательства невыполнимости теоремы Кронекера-Валена в числовых кольцах. Доказано, что теорема Кронекера-Валена не выполняется во всех действительных квадратичных норменно-евклидовых кольцах. Доказан аналог теоремы Ламе о длине цепочки делений с выбором минимального по норме остатка в факториальных кольцах. Эти результаты получены в работах [1; 4; 7; 8] и изложены в главе 3.
3. Доказаны теоремы накладывающие необходимые условия на параметры аналога криптосистемы RSA в дедекиндовых кольцах для обеспечения устойчивости к взлому. В частности теорема Винера о малой секретной экспоненте и теорема Кранакиса. Эти результаты получены в работах [2; 6; 12; 13] и изложены в главе 4.

Рекомендации по практическому использованию результатов

Результаты и методы диссертации могут быть использованы при проведении исследований свойств теоретико-числовых и криптографических алгоритмов в дедекиндовых кольцах или кольцах более общего вида и при чтении спецкурсов для студентов математических специальностей.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ УЧЕНОЙ СТЕПЕНИ

Статьи в научных изданиях в соответствии с Положением о присуждении ученых степеней и присвоении ученых званий в Республике Беларусь

1. Васьковский М.М., Кондратёнок Н.В. Конечные обобщенные цепные дроби в евклидовых кольцах // Вестник БГУ Серия 1 ”Физика, Математика, Информатика”. — 2013. — № 3. — С. 117-123.
2. Vaskouski M., Kondratyonok N. Analogue of the RSA-cryprosystem in quadratic unique factorization domains // Доклады Национальной Академии Наук Беларуси. — 2015. — Т. 59, № 5. — С. 18-23.
3. Vaskouski M., Kondratyonok N., Prochorov N. Primes in quadratic unique factorization domains // Journal of Number Theory. — 2016. — Vol. 168. — P. 101-116.
4. Vaskouski M., Kondratyonok N. Shortest division chains in unique factorization domains // Journal of Symbolic Computation. — 2016. — Vol. 77. — P. 175-188.
5. Васьковский М.М., Кондратёнок Н.В., Прохоров Н.П. Аналог теста Соловея-Штрассена в квадратичных евклидовых кольцах // Доклады Национальной Академии Наук Беларуси. — 2017. — Т. 61, № 5. — С. 28-32.
6. Кондратёнок Н.В. Анализ RSA-криптосистемы в абстрактных числовых кольцах // Журнал Белорусского государственного университета. Математика. Информатика. — 2020. — № 1. — С. 13-21.
7. Vaskouski M., Kondratyonok N. The Kronecker-Vahlen theorem fails in real quadratic norm-Euclidean fields // Journal of Symbolic Computation. — 2021. — Vol. 104. — P. 134-141.

Статьи в сборниках материалов научных конференций

8. Кондратёнок Н.В., Васьковский М.М. Цепные дроби в евклидовых кольцах // Материалы XVI Республиканской научной конференции студентов и аспирантов. — 2013. — Ч. 1. — С. 63-64.
9. Васьковский М.М., Кондратёнок Н.В., Прохоров Н.П. Тест Соловея-Штрассена в квадратичных евклидовых кольцах // Материалы международной научной конференции ”XII Белорусская математическая конференция”. — 2016. — Ч. 5. — С. 15-16.
10. Кондратёнок Н.В., Прохоров Н.П. Критерии простоты в квадратичных

кольцах с единственной факторизацией // Сборник статей лауреатов и авторов научных работ, получивших первую категорию XXIV Республиканского конкурса научных работ студентов. — 2017. — С. 19-20.

11. Кондратёнок Н.В., Прохоров Н.П. Аналог теоремы Кронекера-Валена и полиномиальные алгоритмы тестирования на простоту в числовых полях // Сборник статей лауреатов и авторов научных работ, получивших первую категорию XXV Республиканского конкурса научных работ студентов. — 2018. — С. 25.
12. Васьковский М.М., Кондратёнок Н.В. Построение и анализ RSA-криптосистемы в числовых полях // Сборник материалов ”Всероссийская конференция ”Алгебра и теория алгоритмов”, посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета”. — 2018. — С. 160-162
13. Кондратёнок Н.В. Свойства RSA-криптосистемы в абстрактных числовых кольцах // Материалы международной научной конференции ”XIII Белорусская математическая конференция”. — 2021. — Ч. 2. — С. 63-64.
14. Васьковский М.М., Кондратёнок Н.В. Аналог критерия Миллера в дедекиндовых кольцах с конечной нормой // Материалы международного научного конгресса по математике ”CSIST-2022”. — 2022. — Ч. 1. — С. 21-27.

РЕЗЮМЕ

Кондратёнок Никита Васильевич

Свойства теоретико-числовых и криптографических алгоритмов в дедекиндовых кольцах

Ключевые слова: дедекиндово кольцо, факториальное кольцо, евклидово кольцо, простые идеалы, тест на простоту, цепная дробь, криптосистема RSA.

Цель работы: доказательство новых критериев простоты идеалов в дедекиндовых кольцах и исследование свойств теоретико-числовых и криптографических алгоритмов в дедекиндовых кольцах.

Методы исследования: методы алгебры и алгоритмической теории чисел.

Полученные результаты и их новизна: в диссертации 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 аналога криптосистемы RSA в дедекиндовых кольцах.

Рекомендации по использованию: результаты и методы диссертации могут быть использованы при проведении исследований свойств теоретико-числовых и криптографических алгоритмов в дедекиндовых кольцах или кольцах более общего вида. Также результаты работы могут использоваться при чтении спецкурсов для студентов математических специальностей.

Область применения: результаты исследования могут быть применены в алгоритмической теории чисел, при исследовании свойств теоретико-числовых и криптографических алгоритмов.

РЭЗЮМЭ

Кандрацёнак Мікіта Васільевіч

Уласцівасці тэарэтыка-лікавых і крыптаграфічных алгарытмаў у дэдэкіндавых кольцах

Ключавыя словы: дэдэкіндава кольца, факторыяльнае кольца, эўклідава кольца, простыя ідэалы, тэст на прастату, ланцужны дроб, крыптасістэма RSA

Мэта працы: доказ новых крытэрыяў прастаты ідэалаў у дэдэкіндавых кольцах і даследаванне ўласцівасцей тэарэтыка-лікавых і крыптаграфічных алгарытмаў у дэдэкіндавых кольцах.

Метады даследавання: метады алгебры і алгарытмічнай тэорыі лікаў.

Атрыманыя вынікі і іх навізна: у дысертацыі даказаны новыя крытэры прастаты ідэалаў у дэдэкіндавых кольцах, абагульняючыя вядомыя крытэрыі Мілера і Эйлера, якія з'яўляюцца асновай для пабудовы эфектыўных алгарытмаў тэсціравання прастаты, распрацаваны новыя метады даследавання экстрэмальных уласцівасцяў алгарытму Еўкліда ў факторыяльных кольцах Ламе, упершыню даследаваны ўласцівасці і знойдзены неабходныя ўмовы крыптаўстойлівасці аналага крыптасістэмы RSA, які выкарыстоўвае ідэалы ў дэдэкіндавых кольцах.

Рэкамендацыі па выкарыстанні: вынікі і метады дысертацыі могуць быць выкарыстаны пры правядзенні даследаванняў уласцівасцяў тэарэтыка-лікавых і крыптаграфічных алгарытмаў у дэдэкіндавых кольцах або кольцах больш агульнага выгляду. Таксама вынікі працы могуць выкарыстоўвацца пры чытанні спецкурсаў для студэнтаў матэматычных спецыяльнасцей.

Вобласць ужывання: вынікі даследавання могуць быць ужытыя ў алгарытмічнай тэорыі лікаў, пры даследаванні ўласцівасцей тэарэтыка-лікавых і крыптаграфічных алгарытмаў.

SUMMARY

Kondratyonok Nikita Vasilyevich

Properties of number-theoretic and cryptographic algorithms in Dedekind domains

Keywords: Dedekind domain, factorial ring, Euclidean ring, prime ideals, primality test, continued fraction, RSA cryptosystem

Objective: proof of new ideal primality criteria in Dedekind domains and investigation of the properties of number-theoretic and cryptographic algorithms in Dedekind domains.

Research methods: methods of Algebra and Algorithmic Number Theory.

The results obtained and their novelty: new ideal primality criteria in Dedekind domains are obtained. Obtained criteria generalize the well-known Miller and Euler criteria which are the basis for constructing effective primality testing algorithms. New methods for studying the extremal properties of the Euclid algorithm in factorial rings are developed. Using developed methods analogues of Kronecker-Wahlen and Lame theorems were proved. The properties of an analogue of the RSA cryptosystem in Dedekind domains were studied and the necessary conditions for the cryptographic security of an analogue of the RSA cryptosystem in Dedekind domains were found for the first time.

Recommendations for use: the results and methods of the dissertation can be used to study the properties of number-theoretic and cryptographic algorithms in Dedekind domains or rings of a more general form. Also, the results of the work can be used when reading special courses for students of mathematical specialties.

Application area: the results of the study can be applied in algorithmic number theory, in the study of the properties of number-theoretic and cryptographic algorithms.