МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ФАКУЛЬТЕТ ПРИКЛАДНОЙ МАТЕМАТИКИ И ИНФОРМАТИКИ
Кафедра дискретной математики и алгоритмики

КОНДРАТЁНОК Никита Васильевич

СВОЙСТВА ТЕОРЕТИКО-ЧИСЛОВЫХ АЛГОРИТМОВ В АБСТРАКТНЫХ ЧИСЛОВЫХ КОЛЬЦАХ

Магистерская диссертация
специальность 1-31 80 09 «Прикладная математика и информатика»

Научный руководитель
Васьковский Максим Михайлович
доктор физико-математических наук,
доцент

Допущена к защите
«31» марта 2021 г.
Заведующий кафедрой
_____ В.М. Котов
доктор физико-математических наук, профессор

Минск, 2021

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Криптосистемы играют важную роль в жизни современного общества. Они используются в разных местах для обеспечения безопасности информации при хранении или передаче. Одной из таких криптосистем является RSA-криптосистема. Впервые она была предложена Ривестом, Шамиров и Адлеманом в 1977 году в журнале ”Communications of the ACM”. Алгоритм RSA-криптосистемы опирается на вычислительную сложность задачи факторизации натуральных чисел. Известно, что задача ”взлома” RSA-криптосистемы и факторизации натуральных чисел эквивалентны.

Известно много обобщений этой криптосистемы. Например аналог RSA-криптосистемы в кольце многочленов описан в работах [24] и [14]. В работах [11], [20], [14] изучается аналог RSA-криптосистемы в кольце гауссовых чисел. В работе [34] был предложен аналог RSA-криптосистемы в квадратичных кольцах и изучены ее свойства, связанные с безопасностью. В работе [25] предложено обобщение RSA-криптосистемы на случай произвольных абстрактных числовых колец. В качестве элементов криптосистемы предлагается брать не элементы кольца, а его идеалы.

Целью данной работы является изучение RSA-криптосистемы в абстрактных числовых кольцах. В частности, доказательство теорем, связанных с ее безопасностью. Изучение алгоритмов, необходимых для эффективной реализации криптосистемы.

Абстрактным числовых кольцом называется дедекиндово кольцо, у которого для каждого максимального идеала мощность факторкольца этого идеала конечна. Эта мощность называется нормой соответствующего идеала. Многие из известных колец являются абстрактными числовыми кольцами. Например кольцо целых чисел, гауссовых целых чисел, кольцо многочленов над полем, кольцо целых алгебраических чисел числового поля, координатные кольца.

Одним из алгоритмов, которые используются при реализации RSA-криптосистемы является алгоритм Евклида. Несмотря на то, что в криптосистеме необходима работа этого алгоритма только с целыми числами, криптосистема активно использует операцию деления с остатком. Поэтому интересной задачей является изучение аналога алгоритма Евклида в абстрактных числовых кольцах. Для формулировки аналога алгоритма Евклида используется понятие цепочки делений.

Рассмотрим некоторое кольцо K. Цепочкой делений в кольце K будем называть некоторую последовательность элементов $q_i, r_i \in K$, для которых выполнены равенства $r_i = r_{i-2} - q_i r_{i-1}, i = 1,2,\ldots,k$. При этом считаем, что

известны r_{-1}, r_0 и $r_k = 0$. Один из самых интересных вопросов при изучении цепочек деления это нахождение алгоритма вычисления q_i для минимизации k. Например, если рассмотреть $K = \mathbb{Z}$ и требовать выполнения условия $|q_i| < |q_{i-1}|$ для $i \in \mathbb{N}$, то получим алгоритм Евклида в целых числах.

Согласно работе [3], Вален и Кронекер доказали , что алгоритм Евклида с выбором минимального по норме остатка требует не больше делений, чем любой другой алгоритм Евклида, который на каждом шагу выбирает между остатками $(a \mod b)$ or $((a \mod b) - b)$. Этот результат был обобщен на случай, когда на каждом шаге выбирается любой остаток в работе Лазара [22]. Так же в ней доказан аналог теоремы Кронекера-Валена в кольце многочленов над полем. Калтофен и Роллетчек в работах [15] и [29] доказали эту теорему в специальном классе мнимых квадратичных колец. А несколько лет спустя Роллетчек в работе [30] доказал, что теорема Кронекера-Валена верна в $\mathbb{Z}[\sqrt{d}]$, $d < 0$ тогда и только тогда, когда $d \neq -11c^2$, $c \in \mathbb{N}$. Таким образом решив вопрос выполнимости теоремы Кронекера-Валена в произвольных мнимых квадратичных кольцах. В работе 1–А Васьковский и Кондратёнок доказали, что теорема Кронекера-Валена не выполняется во всех действительных квадратичных норменно-евклидовых кольцах. А именно показано, что "жадный" алгоритм Евклида не минимизирует k. В работе [8] показано, что в кольцах с бесконечной группой единиц есть ограничение сверху на длину алгоритма Евклида. Примерами таких колец могут служить действительные квадратичные норменно-евклидовы кольца. Однако доказательство не является конструктивным и привести алгоритм построения такого короткого алгоритма Евклида не представляется возможным. В работе 1–А Васьковский и Кондратёнок доказали теорему Кронекера-Валена в специальном классе факториальных колец.

Работа состоит из двух глав. Первая глава посвящена изучению RSA-криптосистемы в абстрактных числовых кольцах. Глава состоит из четырех частей. В первой части приводятся основные понятия и утверждения, которые необходимы для более глубокого понимания главы. Во второй части приводятся результаты, изложенные в работе 4–А Кондратёнка. В частности приводится аналог RSA-криптосистемы в дедекиндовых кольцах. Доказывается аналог теоремы Винера о малой секретной экспоненте. Рассматривается способ защиты от атаки повторного шифрования. Используя теорему Копперсмита, доказывается детерминированный аналог теоремы Винера. В третьей части приводится метод, позволяющий сводить факторизацию в числовых полях к факторизации в целых числах. Показано, что это сведение полиномиальное. Это позволяет утверждать, что в числовых полях RSA-криптосистема не имеет преимуществ перед ее классическим вариантом. Однако стоит отметить, что методы факторизации в произвольных дедекиндовых кольцах пока неизвестны. В четвертой части кратко излагаются

основные результаты главы.

Вторая глава посвящена изучению теоремы Кронекера-Валена в абстрактных числовых кольцах. Глава состоит из пяти частей. В первой части приводятся основные понятия и утверждения, которые необходимы для более глубокого понимания главы. Во второй части приводятся результаты, изложенные в работе 3–А Васьковского и Кондратёнка. Доказывается, что теорема Кронекера-Валена верна в специальном классе факториальных колец. В третьей части рассматривается вопрос проверки принадлежности кольца упомянутому специальному классу колец. Приводится алгоритм проверки достаточного условия принадлежности этому классу колец. Используя представленный алгоритм, приведены примеры колец из найденного множества. Чтобы показать существенность введенных ограничений, приводятся примеры колец, не подходящих под условия теорем и для которых аналог теорема Кронекера-Валена не выполняется. В четвертой части приводятся результаты, изложенные в работе 1–А Васьковского и Кондратёнка. Приводится метод доказательства невыполнимости аналога теоремы Кронекера-Валена, применимый для произвольного конечного расширения рациональных чисел. Показано, что аналог теоремы Кронекера-Валена не выполняется во всех действительных норменно-евклидовых квадратичных кольцах. В пятой части кратко излагаются основные результаты главы.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Работа, страницы: 64, главы: 2, источники: 36.

RSA-КРИПТОСИСТЕМА, АЛГЕБРАИЧЕСКОЕ ЧИСЛОВОЕ ПОЛЕ, ДЕДЕКИНДОВО КОЛЬЦО, ДЕЛЕНИЕ С ОСТАТКОМ, ИДЕАЛ, КООРДИНАТНОЕ КОЛЬЦО, МЕТОД ПОВТОРНОГО ШИФРОВАНИЯ, МЕТОДЫ АВТОМАТИЧЕСКОГО ДОКАЗАТЕЛЬСТВА, ТЕОРЕМА ВИНЕРА, ТЕОРЕМА КРОНЕКЕРА-ВАЛЕНА, ФАКТОРИАЛЬНОЕ КОЛЬЦО

Объект исследования – теоретико-числовые алгоритмы в абстрактных числовых кольцах. В частности теорема Кронекера-Валена, методы автоматического доказательства теорем, криптографические алгоритмы.

Цель работы – изучение выполнимости теоремы Кронекера-Валена в различных факториальных кольцах. Разработка метода автоматического доказательства выполнимости или невыполнимости теоремы в конкретном кольце. Так же изучение свойств RSA-криптосистемы в дедекиндовых кольцах.

Методы исследования – изучение литературы, методы теории чисел.

Результаты работы изложены в двух главах.

Первая глава посвящена изучению аналога RSA-криптосистемы в дедекиндовых кольцах. Изучена применимость метода повторного шифрования, доказан аналог теоремы Винера и других теорем, связанных с ее безопасностью. Показано, что задача факторизации идеала полиномиально сводится к задаче факторизации в целых числах.

Вторая глава посвящена теореме Кронекера-Валена. Выделен класс факториальных колец, в которых эта теорема верна. Разработан алгоритм проверки достаточного условия принадлежности факториального кольца этому классу. Используя эти алгоритмы, приведены примеры колец, для которых теорема Кронекера-Валена верна. Разработан метод доказательства невыполнимости теоремы Кронекера-Валена. Доказано, что теорема Кронекера-Валена не выполняется в действительных квадратичных норменно-евклидовых кольцах.

АГУЛЬНАЯ ХАРАКТАРЫСТЫКА ПРАЦЫ

Праца, старонкі: 64, часткі: 2, крыніцы: 36.

RSA-КРЫПТАСІСТЭМА, АЛГЕБРАІЧНЫ ЛІКАВАЕ ПОЛЕ, ДЭДЭКІНДАВА КАЛЬЦО, ДЗЯЛЕННЕ З АСТАТКАМ, ІДЭАЛ, КААРДЫНАТНАЕ КАЛЬЦО, МЕТАД ПАЎТОРНАГА ШЫФРАВАННЯ, МЕТАДЫ АЎТАМАТЫЧНАГА ДОКАЗУ, ТЭАРЭМА ВІНЕРА, ТЭАРЭМА КРОНЕКЕРА-ВАЛЕНА, ФАКТАРЫЯЛЬНАЕ КАЛЬЦО

Аб'ект даследавання - тэарэтыка-лікавыя алгарытмы ў абстрактных лікавых кольцах. У прыватнасці тэарэма Кронекера-Валена, метады аўтаматычнага доказы тэарэм, крыптаграфічныя алгарытмы.

Мэта работы - вывучэнне выканальнасць тэарэмы Кронекера-Валена ў розных факториальных кольцах. Распрацоўка метаду аўтаматычнага доказы выканальнасць або невыканальнасці тэарэмы ў канкрэтным кальцы. Гэтак жа вывучэнне уласцівасцяў RSA-крыптасістэмы ў дэдэкіндавых кольцах.

Метады даследавання - вывучэнне літаратуры, метады тэорыі лікаў.

Вынікі работы выкладзены ў двух раздзелах.

Першая частка прысвечана вывучэнню аналага RSA-крыптасістэмы ў дэдэкіндавых кольцах. Вывучана дастасавальнасць метаду паўторнага шыфравання, даказаны аналаг тэарэмы Вінера і іншых тэарэм, звязаных з яе бяспекай. Паказана, што задача факторизации ідэалу полінаміяльна зводзіцца да задачы факторизации у цэлых лічбах.

Другая частка прысвечана тэарэме Кронекера-Валена. Выдзелены клас факториальных кольцаў, у якіх гэтая тэарэма дакладная. Распрацаваны алгарытм праверкі дастатковага ўмовы прыналежнасці факториального кольцы гэтага класа. Выкарыстоўваючы гэтыя алгарытмы, прыведзены прыклады кольцаў, для якіх тэарэма Кронекера-Валена дакладная. Распрацаваны метад доказы невыканальнасці тэарэмы Кронекера-Валена. Даказана, што тэарэма Кронекера-Валена не выконваецца ў сапраўдных квадратычным норменно-эўклідавай кольцах.

GENERAL CHARACTERISTICS OF THE WORK

Paper, pages: 64, chapters: 2, sources: 36.

RSA-CRYPTOSYSTEM, ALGEBRAIC NUMBER FIELD, DEDEKIND RING, DIVISION WITH REMAINDER, IDEAL, COORDINATE RING, RE-ENCRYPTION METHOD, AUTOMATIC PROOF METHODS, WIENER THEOREM, KRONECKER-VALEN THEOREM, FACTORIAL RING

Object of research - number-theoretic algorithms in abstract number rings. In particular, the Kronecker-Walen theorem, methods of automatic theorem proving, cryptographic algorithms.

The purpose of this work is to study the satisfiability of the Kronecker-Wahlen theorem in various factorial rings. Development of a method for automatically proving the feasibility or non-feasibility of a theorem in a specific ring. Also, the study of the properties of the RSA-cryptosystem in Dedekind rings.

Research methods - study of literature, methods of number theory.

The results of the work are presented in two chapters.

The first chapter is devoted to the study of an analogue of the RSA cryptosystem in Dedekind rings. The applicability of the re-encryption method is studied, an analogue of Wiener's theorem and other theorems related to its security is proved. It is shown that the problem of factorizing an ideal is polynomially reduced to the problem of factoring in integers.

The second chapter is devoted to the Kronecker-Walen theorem. A class of factorial rings is distinguished in which this theorem is true. An algorithm for checking a sufficient condition for a factorial ring to belong to this class is developed. Using these algorithms, examples of rings are given for which the Kronecker-Walen theorem is true. A method for proving the impossibility of the Kronecker-Walen theorem is developed. It is proved that the Kronecker-Walen theorem does not hold in real quadratic norm-Euclidean rings.

ГЛАВА 1.
АНАЛОГ RSA-КРИПТОСИСТЕМЫ В АБСТРАКТНЫХ ЧИСЛОВЫХ КОЛЬЦАХ

1.1 Предварительные сведения

Рассмотрим произвольное кольцо R. Идеалом кольца R называется подкольцо, замкнутое относительно умножения на элементы из R.

Определение 1.1. Идеал $\mathfrak{p}$ называется простым, если выполняются следующие два условия

1. Для любых двух $a, b \in R$, если $ab \in \mathfrak{p}$, то $a \in \mathfrak{p}$ или $b \in \mathfrak{p}$.
2. Идеал $\mathfrak{p}$ не совпадает с R.

Определение 1.2. Идеал $\mathfrak{m}$ называется максимальным, если выполняются следующие условия

1. Это собственный идеал, т.е. $\mathfrak{m}$ собственное подмножество R.
2. Не существует собственных идеалов, для которых $\mathfrak{m}$ является собственным подмножеством.

Утверждение 1.1. *Любой максимальный идеал является простым.*

Определение 1.3. Коммутативное кольцо с единицей и без делителей нуля называется дедекиндовым, если любой собственный идеал в нем раскладывается в конечное произведение простых идеалов. Более того, можно показать, что это разложение единственно с точностью до перестановки множителей.

Определение 1.4. Абстрактным числовым кольцом называют такое дедекиндово кольцо R, что $|R/\mathfrak{m}| < \infty$ для любого максимального ненулевого идеала $\mathfrak{m}$.

Рассмотрим несколько примеров абстрактных числовых колец.

Пример 1.1. Пусть K – числовое поле. Рассмотрим кольцо $\mathcal{O}_K$, образованное алгебраическими целыми элементами этого поля. Это кольцо является абстрактным числовым кольцом. Частными случаями этого примера являются кольцо целых чисел и гауссовых чисел.

Пример 1.2. Рассмотрим кольцо многочленов от 2 переменных над полем K и обозначим его $K[x, y]$. Факторкольцо $K[x, y]/(f)$, где $f \in K[x, y]$ называется координатным кольцом.

Пример 1.3. Рассмотрим кривую $f(x,y)=0$, где $f(x,y)=y-mx-b$ – прямая. Несложно показать, что $K[x,y]/(f(x,y)) \cong K[x]$. Следовательно, это координатное кольцо является факториальным.

Пример 1.4. Рассмотрим кривую $f(x,y)=0$, где $f(x,y)=y-x^2$ – парабола. Несложно показать, что $K[x,y]/(f(x,y)) \cong K[x]$. Следовательно, это координатное кольцо является факториальным.

Пример 1.5. Рассмотрим более сложный пример. Пусть $f(x,y)=x^2+y^2-1$. Если $K=\mathbb{Q}$, то координатное кольцо $\mathbb{Q}[x,y]/(f)$ не изоморфно $K[x]$, так как первое не является факториальным кольцом. Это можно показать, рассмотрев элементы $y^2=yy$ и $1-x^2=(1-x)(1+x)$. Однако, если $K=\mathbb{C}$, то координатное кольцо $\mathbb{C}[x,y]/(f) \cong \mathbb{C}[x,x^{-1}]$ уже будет факториальным, так как это локализация факториального кольца.

Определение 1.5. Мощность множества $R/\mathfrak{m}$ называется нормой $\mathfrak{m}$ и обозначается $\mathcal{N}(\mathfrak{m})$.

Определение 1.6. Функцией Эйлера в абстрактном числовом кольце называется:

$$\varphi(\mathfrak{m}) = |(R/\mathfrak{m})^{\times}|,$$

где $(R/\mathfrak{m})^{\times}$ — группа единиц.

Утверждение 1.2. *[25] Для функции Эйлера в абстрактном числовом кольце выполнено свойство мультипликативности:*

$$\varphi\left(\prod_{i=1}^{k}\mathfrak{m}^{\alpha_i}\right)=\prod_{i=1}^{k}\varphi(\mathfrak{m}^{\alpha_i})$$

Для максимального идеала $\mathfrak{m}$ значение функции Эйлера можно вычислить по формуле:

$$\varphi(\mathfrak{m}^{\alpha})=\mathcal{N}(\mathfrak{m})^{\alpha}-\mathcal{N}(\mathfrak{m})^{\alpha-1}.$$

Утверждение 1.3 Обобщенная теорема Эйлера. *[25] Пусть R — дедекиндово кольцо, обладающее свойствами, описанными выше. Пусть $m \in R$, $\mathfrak{U} \subset R$ — идеал. Если $Rm+\mathfrak{U}=R$, то $m^{\varphi(\mathfrak{U})} \equiv 1 (mod\ \mathfrak{U})$.*

Пусть $\mathcal{O}_K$ – кольцо алгебраических целых чисел числового поля K. Известно, что $\mathcal{O}_K$ является абстрактным числовым кольцом. Обозначим через $\mathcal{O}_K^{\times}$ группу единиц кольца $\mathcal{O}_K$, через $\mathcal{O}_{K,\mathfrak{m}}=\mathcal{O}_K/\mathfrak{m}$ аддитивную группу вычетов по модулю $\mathfrak{m}$ и через $\mathcal{O}_{K,\mathfrak{m}}^{\times}$ мультипликативную группу вычетов по модулю $\mathfrak{m}$. Пусть задана некоторая норма $\mathrm{Nm}(m)$, где $m \in \mathcal{O}_K$.

Утверждение 1.4. *Пусть* $m \in \mathcal{O}_K$. *Тогда* $\mathcal{N}((m)) = |Nm(m)|$, *а так же* $(m)|(Nm(m))$.

Утверждение 1.5 Теорема Копперсмита. *Пусть* $f(x,y)$ *неприводимый многочлен от двух переменных над* $\mathbb{Z}$ *со степенью* δ *по каждой переменной отдельно. Пусть* X, Y *границы предполагаемого решения* (x_0, y_0). *Пусть* W *модуль максимального коэффициента* $f(xX, yY)$. *Если* $XY \leq W^{\frac{2}{3\delta}}$, *то существует полиномиальный относительно* $\log W$ *и* 2^δ *алгоритм, который позволяет найти все* (x_0,y_0) *такие, что* $f(x_0,y_0) = 0$, $|x_0| \leq X$ *и* $|y_0| \leq Y$.

1.2 Формулировка и анализ аналога RSA-криптосистемы

В работе [25] был предложен аналог RSA-криптосистемы в R. Так же показана корректность полученной криптосистемы. Для этого вводится определение функции Эйлера и указывается, что для нее выполнена теорема Эйлера. Показывается, что функцию Эйлера можно эффективно вычислить для максимальных идеалов. Так же формулируются ограничения, при которых можно будет легко манипулировать идеалами с использованием компьютера. Авторы показывают, что RSA-криптосистема в произвольном квадратичном кольце алгебраических целых чисел не имеет преимуществ перед RSA-криптосистемой в целых числах.

В этой части исследуется RSA-криптосистема в абстрактных числовых кольцах. Целью является получение доказательств теорем, связанных с ее криптостойкостью. Например теоремы Винера, теореме об эквивалентности факторизации и взлома криптосистемы, а так же изучение методов взлома криптосистемы.

Алгоритм 1.1 Аналог RSA-криптосистемы в дедекиндовых кольцах

1: выбираются максимальные идеалы $\mathfrak{p}$, $\mathfrak{q} \in R$
2: вычисляется $\varphi(\mathfrak{N})$, где $\mathfrak{N} = \mathfrak{pq}$
3: выбирается случайное целое $e \in [1, \varphi(\mathfrak{N})]$, $(e, \varphi(\mathfrak{N})) = 1$
4: вычисляется целое положительное d такое, что $ed \equiv 1 (\mathrm{mod}\ \varphi(\mathfrak{N}))$

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

$$\begin{gathered} f : R/\mathfrak{N} \to R/\mathfrak{N}, \\ f(x) \equiv x^e (\mathrm{mod}\ \mathfrak{N}). \end{gathered} \tag{1.1}$$

Функцией дешифровки называется

$$\begin{gathered} f^{-1} : R/\mathfrak{N} \to R/\mathfrak{N}, \\ f^{-1}(x) \equiv x^d (\mathrm{mod}\ \mathfrak{N}). \end{gathered} \tag{1.2}$$

Замечание 1.1. Корректность приведенной криптосистемы гарантируется аналогом теоремы Эйлера для абстрактных числовых колец.

Замечание 1.2. В работе [25] описаны условия, при которых применение алгоритма шифрования в абстрактном числовом кольце будет возможно на компьютере. Необходимо, чтобы для некоторых максимальных идеалов $\mathfrak{M}_1, \mathfrak{M}_2 \in R$ и $\mathfrak{U} = \mathfrak{M}_1\mathfrak{M}_2$ было известно множество $W \subset R$ такое, что:

1. Любое подмножество из $R/\mathfrak{U}$ пересекается с W в ровно одном элементе.
2. Есть вычислимая биекция между W и $\{1, \ldots, T\}$ для некоторого T.

Нетрудно заметить, что зная разложение на множители $\mathfrak{N} = \mathfrak{pq}$ для RSA-модуля можно эффективно найти секретный ключ. В некоторых случаях можно доказать обратное утверждение.

Теорема 1.1. *4–А Пусть $\mathcal{O}_K$ — кольцо с единственной факторизацией, $((N),e,d)$ параметры RSA-криптосистемы в $\mathcal{O}_K$. Если d известно, то N можно эффективно разложить на множители с вероятностью не менее $\frac{1}{2}$ за полиномиальное относительно $\log Nm(N)$ количество арифметических операций в $\mathcal{O}_K$.*

Следующая теорема является аналогом теоремы Винера о малой секретной экспоненте [35].

Теорема 1.2. *4–А Пусть $(\mathfrak{N},e,d)$, $\mathfrak{N} = \mathfrak{pq}$ — параметры RSA-криптосистемы в абстрактном числовом кольце R. Причем выполнено $\mathcal{N}(\mathfrak{q}) < \mathcal{N}(\mathfrak{p}) <$*

$\alpha^2\mathcal{N}(\mathfrak{q})$, *где* $\alpha > 1$. *Если* $d < \frac{1}{\sqrt{2\alpha+2}}(\mathcal{N}(\mathfrak{N}))^{1/4}$, *то* d *можно эффективно вычислить за полиномиальное относительно* $\log\mathcal{N}(\mathfrak{N})$ *число бинарных операций.*

Один из известных методов взлома RSA-криптосистемы это метод повторного шифрования. Он состоит в следующем. Предположим, что $x \in \mathcal{O}_{K,\mathfrak{N}}$ – некоторое сообщение. Зашифруем его и получим сообщение $y = x^e (\mathrm{mod}\,\mathfrak{N})$. Вычисляем значения элементов последовательности $y_i = y^{e^i} (\mathrm{mod}\,\mathfrak{N})$, $i = 1,2,\ldots$, пока не получим $y_m = y$. Тогда $y_{m-1} = x$. Этот метод будет работать всегда и единственной защитой от него является выбор параметров RSA-криптосистемы таким образом, чтобы m было достаточно велико.

Обозначим через $R_{\mathfrak{m}}$ и $R_{\mathfrak{m}}^{\times}$ аддитивную и мультипликативную группы вычетов по модулю $\mathfrak{m}$. Заметим, что если $\mathfrak{m} = \mathfrak{m}_1\mathfrak{m}_2$, то $R_{\mathfrak{m}}^{\times} \cong R_{\mathfrak{m}_1}^{\times} \times R_{\mathfrak{m}_2}^{\times}$.

Следующая теорема дает ответ на вопрос безопасности RSA-криптосистемы против атаки повторным шифрованием.

Теорема 1.3. *Пусть* $\mathfrak{N} = \mathfrak{pq}$ *— модуль RSA-криптосистемы в абстрактном числовом кольце* R. *Предположим, что существуют различные простые числа* r, s *и положительные целые числа* k, l *такие, что* $\varphi(\mathfrak{p}) = rk$, $\varphi(\mathfrak{q}) = sl$, *и числа* $r-1$, $s-1$ *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* $\mathbb{Z}_{\varphi(\mathfrak{N})}^*$ *соответственно. Обозначим* $m_{e,y}$*–минимальное* $m \in \mathbb{N}$ *такое, что* $y_m = y$. *Тогда выполняется неравенство*

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

где $m_{e,y}$ *это наименьшее натуральное число такое, что*

$$y^{e^{m_{e,y}}} \equiv y (mod\, \mathfrak{N}).$$

Доказательство. Оценим вероятность $\mathbb{P}\{rs|\mathrm{ord}_{R_{\mathfrak{N}}^{\times}}(y)\}$.

Так как $R_{\mathfrak{N}}^{\times} \cong R_{\mathfrak{p}}^{\times} \times R_{\mathfrak{q}}^{\times}$ и группы $R_{\mathfrak{p}}^{\times}$, $R_{\mathfrak{q}}^{\times}$ циклические, то можно записать $y = (a^i, b^j)$, где a и b примитивные элементы $R_{\mathfrak{p}}^{\times}$ и $R_{\mathfrak{q}}^{\times}$ соответственно, i и j случайные величины со значениями в $\{1,\ldots,rk\}$ и $\{1,\ldots,sl\}$ соответственно.

Заметим, что $\mathrm{ord}_{R_{\mathfrak{N}}^{\times}}(y) = \mathrm{lcm}\left(\frac{rk}{(rk,i)}, \frac{sl}{(sl,j)}\right)$. Если $r \nmid i$ и $s \nmid j$, то $\mathrm{ord}_{R_{\mathfrak{N}}^{\times}}(y) = \mathrm{lcm}\left(r\frac{k}{(k,i)}, s\frac{l}{(l,j)}\right) \vdots rs$. Таким образом получаем

$$\mathbb{P}\{rs|\mathrm{ord}_{R_{\mathfrak{N}}^{\times}}(y)\} \geq \mathbb{P}\{r \nmid i, s \nmid j\} = \frac{\varphi(r)k\varphi(s)l}{rksl} = \left(1 - \frac{1}{r}\right)\left(1 - \frac{1}{s}\right). \quad (1.3)$$

Так как $e \in \mathbb{Z}_{rs}^*$, то аналогично можно получить неравенство

$$\mathbb{P}\{r_1 s_1 | \mathrm{ord}_{\mathbb{Z}_{rs}^*}(e)\} \geq \left(1 - \frac{1}{r_1}\right)\left(1 - \frac{1}{s_1}\right). \tag{1.4}$$

Легко заметить, что $\mathrm{ord}_{R_{\mathfrak{N}}^\times}(y) | (e^{m_{e,y}} - 1)$, следовательно, имеем

$$\{rs | \mathrm{ord}_{R_{\mathfrak{N}}^\times}(y)\} \subseteq \{\mathrm{ord}_{\mathbb{Z}_{rs}^*}(e) | m_{e,y}\}. \tag{1.5}$$

Принимая во внимание $(1.3) - (1.5)$, заключаем

$$\mathbb{P}\{m_{e,y} \geq r_1 s_1\} \geq \mathbb{P}\{r_1 s_1 | m_{e,y}\} \geq \mathbb{P}\{r_1 s_1 | \mathrm{ord}_{\mathbb{Z}_{rs}^*}(e), rs | \mathrm{ord}_{R_{\mathfrak{N}}^\times}(y)\} \geq$$
$$\geq (1 - r^{-1})(1 - s^{-1})(1 - r_1^{-1})(1 - s_1^{-1}). \tag{1.6}$$

Таким образом теорема доказана. $\otimes$

Теорема 1.4. *Пусть $(\mathfrak{N}, e, d)$ параметры RSA-криптосистемы в абстрактном числовом кольце R, где $\mathcal{N}(\mathfrak{p})$ и $\mathcal{N}(\mathfrak{q})$ имеют одинаковую битовую длину. Пусть $ed \leq (\mathcal{N}(\mathfrak{N}))^2$, $\mathcal{N}(\mathfrak{N}) \geq 107$. Если d известно, то существует эффективный алгоритм, который позволяет найти $\mathcal{N}(\mathfrak{p})$ и $\mathcal{N}(\mathfrak{q})$.*

Доказательство. Из того, что $ed \equiv 1 (\mathrm{mod}\, \varphi(\mathfrak{N}))$ следует, что $ed = k\varphi(\mathfrak{N}) + 1$ для некоторого $k \in \mathbb{N}$. Предположим, что $\mathcal{N}(\mathfrak{p}) \leq \mathcal{N}(\mathfrak{q})$. Тогда $\mathcal{N}(\mathfrak{P}) \leq (\mathcal{N}(\mathfrak{N}))^{1/2} \leq \mathcal{N}(\mathfrak{q}) < 2\mathcal{N}(\mathfrak{p}) \leq 2(\mathcal{N}(\mathfrak{N}))^{1/2}$. Следовательно, имеем

$$\mathcal{N}(\mathfrak{p}) + \mathcal{N}(\mathfrak{q}) < 3(\mathcal{N}(\mathfrak{N}))^{1/2} \leq \frac{\mathcal{N}(\mathfrak{N})}{2}. \tag{1.7}$$

Из (1.7) следует, что

$$\varphi(\mathfrak{N}) = (\mathcal{N}(\mathfrak{p}) - 1)(\mathcal{N}(\mathfrak{q}) - 1) = \mathcal{N}(\mathfrak{N}) + 1 - \mathcal{N}(\mathfrak{p}) - \mathcal{N}(\mathfrak{q}) >$$
$$> \mathcal{N}(\mathfrak{N}) + 1 - \frac{\mathcal{N}(\mathfrak{N})}{2} > \frac{\mathcal{N}(\mathfrak{N})}{2}. \tag{1.8}$$

Обозначим $\overline{k} = \frac{ed-1}{\mathcal{N}(\mathfrak{N})}$. Тогда

$$k - \overline{k} = \frac{(\mathcal{N}(\mathfrak{N}) - \varphi(\mathfrak{N}))(ed-1)}{\mathcal{N}(\mathfrak{N})\varphi(\mathfrak{N})} = \frac{(\mathcal{N}(\mathfrak{p}) + \mathcal{N}(\mathfrak{q}) - 1)(ed-1)}{\mathcal{N}(\mathfrak{N})\varphi(\mathfrak{N})}. \tag{1.9}$$

Из (1.7), (1.8) и (1.9) следует, что

$$k - \overline{k} < 6(\mathcal{N}(\mathfrak{N}))^{-3/2}(ed-1). \tag{1.10}$$

Пусть $x = k - \overline{k}$. Так же выполнено $\mathcal{N}(\mathfrak{N}) - \varphi(\mathfrak{N}) = \mathcal{N}(\mathfrak{p}) + \mathcal{N}(\mathfrak{q}) - 1 < 3(\mathcal{N}(\mathfrak{N}))^{1/2}$. Следовательно $\varphi(\mathfrak{N}) \in [\mathcal{N}(\mathfrak{N}) - 3(\mathcal{N}(\mathfrak{N}))^{1/2}, \mathcal{N}(\mathfrak{N})]$. Разделим этот интервал на 6 интервалов длины $\frac{1}{2}(\mathcal{N}(\mathfrak{N}))^{1/2}$ с центрами в точках $\mathcal{N}(\mathfrak{N}) - \frac{2i-1}{4}(\mathcal{N}(\mathfrak{N}))^{1/2}$, где $i = \overline{1,6}$. Рассмотрим $i \in \{1, \ldots, 6\}$ такое, что

$$\left| \mathcal{N}(\mathfrak{N}) - \frac{2i-1}{4}(\mathcal{N}(\mathfrak{N}))^{1/2} - \varphi(\mathfrak{N}) \right| \leq \frac{1}{4}(\mathcal{N}(\mathfrak{N}))^{1/2}. \tag{1.11}$$

Пусть $g = \lceil \frac{2i-1}{4} \mathcal{N}(\mathfrak{N}) \rceil$. Тогда $|\mathcal{N}(\mathfrak{N}) - g - \varphi(\mathfrak{N})| < \frac{1}{4}(\mathcal{N}(\mathfrak{N}))^{1/2} + 1$ и $\varphi(\mathfrak{N}) = \mathcal{N}(\mathfrak{N}) - g - y$ для некоторого неизвестного y такого, что $|y| \leq \frac{1}{4}(\mathcal{N}(\mathfrak{N}))^{1/2}$. Далее имеем

$$ed - 1 = k\varphi(\mathfrak{N}) = (\lceil \overline{k} \rceil + x)(\mathcal{N}(\mathfrak{N}) - g - y). \tag{1.12}$$

Рассмотрим многочлен

$$f(x,y) = xy - (\mathcal{N}(\mathfrak{N}) - g)x + \lceil \overline{k} \rceil y - \lceil \overline{k} \rceil (\mathcal{N}(\mathfrak{N}) - g) + ed - 1. \tag{1.13}$$

У него есть корень $(x_0, y_0) = (k - \lceil \overline{k} \rceil, \mathcal{N}(\mathfrak{p}) + \mathcal{N}(\mathfrak{q}) + 1 - g)$. Имеем $\delta = 1$, где δ из теоремы Копперсмита. Определим $X = 6(\mathcal{N}(\mathfrak{N}))^{1/2}$ и $Y = \frac{1}{4}(\mathcal{N}(\mathfrak{N}))^{1/2} + 1$. Тогда $|x_0| \leq X$ и $|y_0| \leq Y$. Пусть W норма вектора коэффициентов многочлена $f(xX, yY)$. Тогда $W \geq (\mathcal{N}(\mathfrak{N}) - g)X > 3(\mathcal{N}(\mathfrak{N}))^{3/2}$. Следовательно

$$XY = \frac{3}{2}\mathcal{N}(\mathfrak{N}) + 6(\mathcal{N}(\mathfrak{N}))^{1/2} < W^{2/3} = W^{\frac{2}{3\delta}}$$

для $\mathcal{N}(\mathfrak{N}) \geq 107$.

Тогда мы можем применить теорему Копперсмита. Следовательно, мы можем найти корень (x_0, y_0) за полиномиальное относительно $\log W$ время. Корень (x_0, y_0) позволяет найти $\mathcal{N}(\mathfrak{p})$ и $\mathcal{N}(\mathfrak{q})$. $\otimes$

Приведем примеры работы криптосистемы для некоторых координатных колец.

Пример 1.6. Рассмотрим кольцо многочленов от двух переменных над $\mathbb{Z}_2$. Рассмотрим координатное кольцо

$$R = \frac{\mathbb{Z}_2(x, y)}{y - x}$$

Оно изоморфно $\mathbb{Z}_2[x]$. Известно, что это кольцо дедекиндово. Рассмотрим идеалы $(x^3 + x + 1)$ и $(x^3 + x^2 + 1)$ и найдем их норму. И $R/(x^3 + x + 1)$, и

$R/(x^3+x^2+1)$ состоит из многочленов степени не более 2. Следовательно, норма обоих идеалов равна 8.

Теперь найдем элементы $R/(x^3+x+1)(x^3+x^2+1)$

$$(x^3+x+1)(x^3+x^2+1) = x^6+x^5+x^4+x^3+x^2+x+1$$

Следовательно, $x^6 = x^5+x^4+x^3+x^2+x+1$. Следовательно, фактор-кольцо $R/(x^3+x+1)(x^3+x^2+1)$ состоит из многочленов не более чем 5 степени. Их 64, следовательно, по норме все сходится.

Заметим, что

$$\begin{aligned}
&x^6 = x^5+x^4+x^3+x^2+x+1\\
&x^7 = 1\\
&x^8 = x\\
&x^9 = x^2\\
&x^{10} = x^3\\
&x^{11} = x^4\\
&x^{12} = x^5\\
&x^{13} = x^6 = x^5+x^4+x^3+x^2+x+1\\
&x^{14} = x^7 = 1\\
&\dots
\end{aligned}$$

Следовательно, имеем

$$\begin{aligned}
&x^{7i} = 1\\
&x^{7i+1} = x\\
&x^{7i+2} = x^2\\
&x^{7i+3} = x^3\\
&x^{7i+4} = x^4\\
&x^{7i+5} = x^5\\
&x^{7i+6} = x^5+x^4+x^3+x^2+x+1
\end{aligned}$$

Вычисляем

$$\varphi_K((x^3+x+1)(x^3+x^2+1)) = 7*7 = 49$$

Выбираем случайное $e = 11$. Тогда $d = 9$.

Возьмем элемент x^4+x^2+1. Зашифруем его

$$(x^4+x^2+1)^{11} = x^2+x+1$$

Теперь расшифруем

$$(x^2+x+1)^9 = x^4+x^2+1$$

Пример 1.7. Рассмотрим кольцо многочленов от двух переменных над $\mathbb{Z}_2$. И рассмотрим координатное кольцо

$$R = \frac{\mathbb{Z}_2(x, y)}{\langle xy - 1 \rangle}.$$

Так как в этом координатном кольце $xy - 1 = 0$, то оно состоит из многочленов вида $xf(x) + yg(y) + c$. Из этого несложно заметить, что $R \cong \mathbb{Z}_2(x, x^{-1})$.

Рассмотрим идеал $(x + 1)$. Его норма 2, так как фактор кольцо $R/(x + 1)$ состоит из элементов 0 и 1.

Рассмотрим идеал $(x^2 + x + 1)$. Кольцо $R/(x^2 + x + 1)$ состоит из $x + 1$, x, 1, 0. Следовательно, норма этого идеала 4.

Теперь рассмотрим произведение этих идеалов $(x+1)(x^2+x+1) = x^3+1$. Несложно заметить, что $R/(x^3 + 1)$ состоит из многочленов 0, 1, x, $x + 1$, x^2, $x^2 + 1$, $x^2 + x$, $x^2 + x + 1$. Значит норма $(x^3 + 1)$ равна 8.

Заметим, что

$$\begin{aligned} x^{3i} &= 1 \\ x^{3i+1} &= x \\ x^{3i+2} &= x^2 \end{aligned}$$

Вычисляем

$$\varphi_K((x + 1)(x^2 + x + 1)) = 3$$

Выбираем случайное $e = 2$. Тогда $d = 2$. Возьмем элемент $x^2 + 1$. Зашифруем его

$$(x^2 + 1)^2 = x^4 + 1 = x + 1$$

Теперь расшифруем

$$(x + 1)^2 = x^2 + 1$$

1.3 Алгоритмы факторизации в абстрактных числовых кольцах

Как было сказано ранее, в работе [25] было показано, что RSA-криптосистема в произвольном квадратичном кольце алгебраических целых чисел не имеет

преимуществ перед RSA-криптосистемой в целых числах. В этой части будет показано, что аналогичное утверждение верно для произвольного кольца целых алгебраических чисел числового поля.

Рассмотрим некоторое числовое поле $K = \mathbb{Q}(\theta)$. Будем предполагать, что поле K фиксировано и, следовательно, известен индекс $[\mathcal{O}_K : \mathbb{Z}[\theta]]$. А так же разложение на простые идеалы всех простых делителей индекса.

Рассмотрим представления идеалов. Существует два способа представить идеал

1. Через целый базис.

$$\mathfrak{p} = \oplus_{i=1}^{n} \mathbb{Z}\alpha_i, \tag{1.14}$$

   где $\alpha_i \in \mathcal{O}_K$.
2. Через два элемента $\mathcal{O}_K$. Для любого $\alpha \in \mathfrak{p}$ существует $\beta \in \mathfrak{p}$ такой, что

$$\mathfrak{p} = \alpha\mathcal{O}_K + \beta\mathcal{O}_K. \tag{1.15}$$

   Будем обозначать идеалы в таком представлении через (α, β). Идеал, который генерируется одним элементом $\alpha \in \mathcal{O}_K$ будем обозначать $(\alpha) = \alpha\mathcal{O}_K$.

Утверждение 1.6 Теорема Дедекинда. *Пусть $f(T)$ минимальный многочлен алгебраического числа θ в $\mathbb{Z}[\theta]$. Для простого рационального числа p, не делящего индекс $[\mathcal{O}_K : \mathbb{Z}[\theta]]$, запишем*

$$f(T) \equiv \pi_1(T)^{e_1} \dots \pi_g(T)^{e_g} \textit{mod } p,$$

где $\pi_i(T)$ — различные монические неприводимые многочлены в $\mathbb{F}_p[T]$. Тогда

$$(p) = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_g^{e_g},$$

где $\mathfrak{p}_i = (p_i, T_i(\theta))$, $T_i(T) \equiv \pi_i(T) (\textit{mod } p)$.

Используя теорему Дедекинда, можно показать, что задача факторизации в кольце целых чисел числового поля полиномиально эквивалентна задаче факторизации целых чисел.

Сделать это можно с помощью следующего алгоритма.

1. Пусть дан идеал (N) в форме своего 2-представления.
2. Считаем норму идеала, равную норме элемента N и раскладываем норму на множители одним из известных алгоритмов для факторизации целых чисел. Например методом решета числового поля или алгоритмом Шора. Получаем разложение

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

Таким образом, мы знаем, что

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

3. Факторизуем идеал (p_i) с помощью теоремы Дедекинда 1.6 и получаем двухэлементные представления идеалов

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

4. Преобразуем полученные простые идеалы в $\mathbb{Z}$-представление и объединяем равные. Получаем представление

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

5. Используем бинарный поиск для нахождения степеней, в которых $\mathfrak{p}_i$ входит в (N).

Покажем, что алгоритм полиномиальный

Утверждение 1.7. *Для вычисления нормы идеала (N) необходимо $O(n^3 \log^2 |N|)$ бинарных операций, где $|N|$ обозначает максимальный по модулю элемент матричного представления N.*

Доказательство. Для вычисления нормы идеала (N) необходимо найти определитель матрицы, которая получается при матричном представлении элемента N. Для этого необходимо $O(n^3 \log^2 |N|)$ бинарных операций. $\otimes$

Утверждение 1.8. *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.*

Доказательство. Оценим сложность разложения многочлена на множители в $\mathbb{F}_p$. Сделать это можно с помощью вероятностной версии алгоритма Берлекэмпа за $O((n \log n + \log p) n \log n \log\log n \log^2 p)$ бинарных операций. В результате получим не более n многочленов. Тогда вычислить значения многочленом в разложении можно за $O(n \log^2 p)$.

Итого получаем, что разложить идеал (p), используя теорему Дедекинда, можно за $O((n \log n + \log p) n \log n \log\log n \log^2 p + n \log^2 p) = O((n \log n + \log p) n \log n \log\log n \log^2 p)$ бинарных операций. $\otimes$

Утверждение 1.9. *Преобразовать 2-представление идеала (p, α) из теоремы Дедекинда в $\mathbb{Z}$-представление можно $O(P(n)Q(\log p))$ бинарных операций, где $P(T)$ и $Q(T)$ некоторые полиномы.*

Доказательство. В книге [26] описан алгоритм преобразования 2-представления в $\mathbb{Z}$-представление. Необходимо найти Эрмитову нормальную форму блочной матрицы

$$\begin{pmatrix} A \\ B \end{pmatrix},$$

где $A = diag(p, \ldots, p)$, а B является матричным представлением элемента α. В 1979 году было доказано, что эрмитову нормальную форму матрицу можно найти за строго полиномиальное время [16]. Это означает, что алгоритму необходимо полиномиальное, относительно размеров матрицы, количество арифметических операций над числами не превосходящими полинома от бинарного представления элементов матрицы. Таким образом эрмитову нормальную форму можно вычислить за $O(P(n)Q(\log p))$ бинарных операций, где $P(T)$ и $Q(T)$ некоторые полиномы. $\otimes$

Замечание 1.3. Таким образом, зная разложение (p_i) на произведение простых идеалов, можно найти одинаковые идеалы и разложение $(\mathrm{Nm}(N))$ на произведение различных идеалов за $O(P(n)Q(\log|N|))$ бинарных операций, так как $k \leq \log \mathrm{Nm}(N)$ и $l_i \leq n$. Таким образом, найти разложение идеала $(\mathrm{Nm}(N))$ на произведение различных простых идеалов можно за полиномиальное относительно $\log \mathrm{Nm}(N)$ количество бинарных операций, если разложение $\mathrm{Nm}(N)$ на множители известно.

Это показывает, что аналог RSA-криптосистемы в некотором смысле не дает никакого выигрыша при использовании в кольцах алгебраических целых чисел числовых полей.

Замечание 1.4. Задача факторизации в абстрактных числовых полях является более сложной, так как нет доказательства аналога теоремы Дедекинда в абстрактных числовых кольцах.

В работе [18] приводится алгоритм факторизации идеалов в дедекиндовых кольцах. Во время факторизации идеал проходит три алгоритма: разложение на радикалы, разложение на множители с одинаковыми степенями и разложение на множители с разными степенями. Рассмотрим эти алгоритмы подробнее.

Пусть R – дедекиндово кольцо и $\mathfrak{a}$ – идеал в R. Так как R дедекиндово, то $\mathfrak{a}$ единственным образом раскладывается в произведение простых идеалов. Пусть это разложение имеет вид

$$\mathfrak{a} = \mathfrak{p}_1^{k_1} \ldots \mathfrak{p}_s^{k_s},$$

где $p_1, \ldots, p_s$ различные простые идеалы и $k_1, \ldots, k_s > 0$. Соберем вместе простые множители с одинаковой степенью. Для $j \leq m = \max\{k_1, \ldots, k_s\}$

обозначим

$$\mathfrak{g}_j = \bigcap_{k_i=j} \mathfrak{p}_i$$

Представление

$$\mathfrak{a} = \mathfrak{g}_1 \mathfrak{g}_1^2 \dots \mathfrak{g}_m^m$$

называется разложением на радикалы.

После выполнения этого разложения задача факторизации сводится к задаче факторизации идеала вида $\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_s$, где $\mathfrak{p}_1, \dots, \mathfrak{p}_s$ являются простыми идеалами. Обозначим

$$\mathfrak{h}_j = \prod_{\mathfrak{p}|\mathfrak{a}, \deg\mathfrak{p}=j} \mathfrak{p}$$

Представление

$$\mathfrak{a} = \mathfrak{h}_1 \dots \mathfrak{h}_m$$

называется разложением на множители с разными степенями.

После двух шагов получается, что задача факторизации идеала сводится к задаче факторизации радикала, который является произведением различных простых идеалов с одинаковой степенью, которая нам неизвестна. Далее можно воспользоваться алгоритмом, похожим на алгоритм Кантотра-Зассенхауса.

Несмотря на то, что алгоритм факторизации имеется, у него есть определенные ограничения. Они описаны в работе [18] и состоят в том, что надо уметь вычислять радикал идеала, сумму идеалов и частное.

1.4 Результаты

В данной главе исследован аналог RSA-криптосистемы в абстрактных числовых кольцах. В результате работы, были получены следующие результаты:

1. Приведен аналог RSA-криптосистемы в абстрактных числовых кольцах. Ключевое отличие от классической криптосистемы состоит в том, что аналог использует идеалы кольца вместо элементов.
2. Доказана теорема Винера о малой секретной экспоненте для упомянутого выше аналога RSA-криптосистемы.

3. Изучен метод взлома RSA-криптосистемы методом повторного шифрования. Доказана теорема, позволяющая защититься от этого типа атаки.
4. Доказано, что в кольцах алгебраических целых чисел числовых полей задачи взлома RSA-криптосистемы и факторизации ее модуля эквивалентны.
5. Показано, что задача факторизации идеала к кольцах алгебраических целых чисел числового поля полиномиально сводится к задаче факторизации в целых числах. Сделан вывод о том, что использование аналога RSA-криптосистемы в числовых полях не дает выигрыша по сравнению с классической RSA-криптосистемой. Однако аналогичная задача в абстрактных числовых кольцах остается открытой.

ГЛАВА 2.
ТЕОРЕМА КРОНЕКЕРА-ВАЛЕНА В АБСТРАКТНЫХ ЧИСЛОВЫХ КОЛЬЦАХ

2.1 Предварительные сведения

Пусть $\mathbb{K}$ – кольцо с единственной факторизацией. Обозначим $\mathbb{K}_*$ – кольцо без нуля.

О п р е д е л е н и е 2.1. Функция $\upsilon : \mathbb{K} \to \mathbb{N} \cup \{0, -\infty\}$ называется нормой в $\mathbb{K}$, если выполнены следующие условия:

1. $\upsilon(x) = -\infty$ тогда и только тогда, когда $x = 0$;
2. $\upsilon(xy) \geq \upsilon(y)$ для любых $x,y \in \mathbb{K}_*$;
3. если $x,y \in \mathbb{K}_*$, то $\upsilon(xy) = \upsilon(x)$ тогда и только тогда, когда $y \in \mathbb{I}$, где $\mathbb{I}$ – множество обратимых элементов $\mathbb{K}$.

Рассмотрим примеры нормы.

Пример 2.1. Рассмотрим произвольный элемент $x \in \mathbb{K}_*$. Так как $\mathbb{K}$ кольцо с единственной факторизацией, то существует единственное (с точностью до перестановки и домножения на обратимый элемент) представление

$$x = \varepsilon p_1^{\alpha_1} \cdots p_k^{\alpha_k},$$

где $\varepsilon \in \mathbb{I}$, $p_1, \ldots, p_k$ – простые элементы $\mathbb{K}$, $\alpha_1, \ldots, \alpha_k \in \mathbb{N}$, $k \geq 0$ (если $k = 0$, то $x = \varepsilon$). Тогда функция $\upsilon : \mathbb{K} \to \mathbb{N} \cup \{0, -\infty\}$, $\upsilon(x) = \sum_{i=1}^{k} \alpha_i$, $x = \varepsilon p_1^{\alpha_1} \ldots p_k^{\alpha_k} \in \mathbb{K}_*$, $\upsilon(0) = -\infty$, является нормой в $\mathbb{K}$, где $\sum_{i=1}^{k} \alpha_i = 0$ для $k = 0$.

Так же евклидова норма является нормой в смысле определения 2.1.

О п р е д е л е н и е 2.2. Пусть $\mathbb{F}$ поле частных кольца $\mathbb{K}$ с нормой υ. Функция $\mathrm{fr} : \mathbb{F} \to \mathbb{F}$ называется дробной частью в $\mathbb{F}$, если выполнены следующие условия:

1. $\mathrm{fr}(\alpha + q) = \mathrm{fr}(\alpha)$ для любых $\alpha \in \mathbb{F}$, $q \in \mathbb{K}$;
2. если $m/n \in \mathbb{F}$, $\gcd(m,n) = 1$, то $\mathrm{fr}(m/n) = r/n$, где $r \in \mathbb{K}$, $(m-r)/n \in \mathbb{K}$, и $\upsilon(r) = \min\{\upsilon(s) | s \in \mathbb{K}, (m-s)/n \in \mathbb{K}\}$.

Целой частью в $\mathbb{F}$ называется функция $\mathrm{int} : \mathbb{F} \to \mathbb{K}$, заданная формулой:

$$\mathrm{int}(\alpha) = \alpha - \mathrm{fr}(\alpha), \alpha \in \mathbb{F}.$$

Пример 2.2. Рассмотрим произвольный элемент $x \in \mathbb{F}/\mathbb{K}$, заданный следующим образом $x = \{m/n + t | t \in \mathbb{K}\}$, где m, n взаимнопростые элементы $\mathbb{K}$, $n \neq 0$. Из определения дробной части следует, что существует $t_0 \in \mathbb{K}$ такой, что $\upsilon(m + nt_0) = \min\{\upsilon(m + nt) | t \in \mathbb{K}\}$.

Определим функции $\text{fr}(x) = m/n + t_0$, $x \in \mathbb{K}$ и $\text{int}(x) = x - \text{fr}(x)$. Несложно убедиться, что $\text{fr}(\cdot)$ и $\text{int}(\cdot)$ соответственно дробная и целая части в $\mathbb{F}$ относительно нормы υ.

Далее будем считать, что рассматриваем кольцо $\mathbb{K}$, для которого задана некоторая норма υ. А так же, что для поля частных $\mathbb{F}$ заданы дробная часть $\text{fr}(\cdot)$ и целая часть $\text{int}(\cdot)$.

Определение 2.3. Пусть $a, b \in \mathbb{K}_*$. Для произвольных $k \in \mathbb{N}$ и $q_1, \ldots, q_k \in \mathbb{K}$ цепочкой деления будем называть упорядоченный набор элементов

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

где $r_{-1} = a$, $r_0 = b$, $r_i = r_{i-2} - q_i r_{i-1}, i = 1, 2, \ldots, k$. Обозначим через $\mathcal{E}_{a,b}$ множество

$$\{\mathcal{D}_{a,b}(q_1, \ldots, q_k) = (r_{-1}, \ldots, r_k) | k \in \mathbb{N}, q_1, \ldots, q_k, r_1, \ldots, r_{k-1} \in \mathbb{K}_*, r_k = 0\}.$$

В некоторых случаях возможно $\mathcal{E}_{a,b} = \emptyset$.

Определение 2.4. Пусть $a, b \in \mathbb{K}_*$. Цепочкой делений с выбором минимального по норме остатка при делении a на b называется такая цепочка делений

$$\mathcal{D}_{a,b}(q_1, \ldots, q_k) = \mathcal{g}_{a,b} \in \mathcal{E}_{a,b},$$

что $q_i = \text{int}(r_{i-2}/r_{i-1})$ для всех $i = 1, \ldots, k$. Если существует цепочка делений с выбором минимального по норме остатка при делении a на b, то обозначим через $\mathcal{L}_{a,b}$ ее длину. Если такой цепочки не существует, то положим $\mathcal{L}_{a,b} = \infty$.

Определение 2.5. Обозначим через $\mathcal{l}_{a,b}$ наименьшее положительное число k такое, что существует $\mathcal{D}_{a,b}(q_1, \ldots, q_k) \in \mathcal{E}_{a,b}$. Если $\mathcal{E}_{a,b} = \emptyset$, то положим $\mathcal{l}_{a,b} = \infty$. Положим

$$\mathcal{O}_{a,b} = \{\mathcal{D}(q_1, \ldots, q_k) \in \mathcal{E}_{a,b} | k = \mathcal{l}_{a,b}\},$$

если $\mathcal{E}_{a,b} \neq \emptyset$. Если $\mathcal{E}_{a,b} = \emptyset$, то положим $\mathcal{O}_{a,b} = \emptyset$.

Определение 2.6. Определим *длину цепочки с выбором минимального по норме остатка* следующим образом:

$$l_n(\mathbb{K}) = \max\{\mathcal{L}_{a,b} | (a,b) \in \mathbb{K}_* \times \mathbb{K}_*, n \geq \upsilon(a) \geq \upsilon(b)\}, n \in \mathbb{N}.$$

Рассмотрим пример кольца в котором не существует цепочки делений с выбором минимального по норме остатка.

Пример 2.3. Рассмотрим кольцо многочленов с целыми коэффициентами $\mathbb{K} = \mathbb{Z}[t]$. Пусть в нем некоторым образом заданы норма, дробная и целая части. Рассмотрим многочлены $a(t) = t$, $b(t) = 2$. Предположим, что существует $\mathcal{g}_{a,b}$. Это значит, что существуют многочлены $f(t)$,$g(t)$ такие, что

$$1 = \gcd(a(t),b(t)) = tf(t) + 2g(t).$$

Но это невозможно, так как при любых $g(t) \in \mathbb{Z}[t]$ равенство $1 = 2g(0)$ не выполняется. Следовательно, не существует $\mathcal{g}_{a(t),b(t)}$.

Определение 2.7. Обозначим через $\mathbb{F}_1$ множество всех правильных несократимых дробей $\mathbb{F}$, т.е.

$$\mathbb{F}_1 = \{\alpha \in \mathbb{F} | \alpha = \mathrm{fr}(\alpha)\}.$$

Обозначим $\mathbb{F}_1^* = \mathbb{F}_1 \backslash \{0\}$. Определим функцию $\omega : \mathbb{F}_1 \to \mathbb{F}_1$ следующим образом:

$$\omega(\alpha) = \begin{cases} \mathrm{fr}(\alpha^{-1}), & \alpha \neq 0, \\ 0, & \alpha = 0. \end{cases}$$

Определение 2.8. Тройка $(x_0,\alpha,n) \in \mathbb{K}_* \times \mathbb{F}_1^* \times \mathbb{N}$ называется *регулярной*, если существуют натуральные числа p и l, $p \leq n$, $l \leq p+1$, такие, что существуют $\varepsilon_i \in \mathbb{I}$, $b_i,c_i \in \mathbb{K}, i = \overline{1,l-1}$, удовлетворяющие следующим условиям

$$\begin{gathered} \beta_1 = \omega^{(p)}\left(\mathrm{fr}\left(\tfrac{1}{\alpha - x_0}\right)\right), \\ \beta_{i+1} = (\varepsilon_i \beta_i + c_i)^{-1} + b_i, i = \overline{1,l-1} \\ \beta_l = \alpha^{(-1)^\varepsilon}, \end{gathered}$$

где $\varepsilon \in \{0,1\}$, $\omega^{(p)}$ – p-кратная композиция функции ω.

Определение 2.9. Обозначим через $\mathcal{T}$ множество всех факториальных колец $\mathbb{K}$ таких, что существует $D_{\mathbb{K}} \in \mathbb{N}$ удовлетворяющее следующим условиям:

1. Для любого $x_0 \in \mathbb{K}_*, \alpha \in \mathbb{F}_1^*$, тройка $(x_0,\alpha,D_{\mathbb{K}})$ регулярная.
2. Если $D_{\mathbb{K}} \geq 3$, то для любого натурального числа $k \in [3,D_{\mathbb{K}}]$ и $x_0 \in \mathbb{K}_*, \alpha \in \mathbb{F}_1^*$ тройка $(x_0,\alpha,k-2)$ регулярная, если $\omega^{(k-2)}(\mathrm{fr}((\alpha - x_0)^{-1})) = 0$.

О п р е д е л е н и е 2.10. Будем говорить, что теорема Кронекера-Валена выполняется в $\mathbb{K}$, если для любых $a, b \in \mathbb{K}$ любая цепочка с выбором минимального по норме остатка для a и b имеет наименьшую длину среди всех цепочек делений для a и b.

Будем говорить, что теорема Кронекера-Валена не выполняется в $\mathbb{K}$, если существуют $a, b \in \mathbb{K}$ и две цепочки делений $\mathcal{D}_{a,b}$ и $\mathcal{D}'_{a,b}$ такие, что $\mathcal{D}_{a,b}$ – цепочка с выбором минимального по норме остатка и $\text{len}(\mathcal{D}_{a,b}) > \text{len}(\mathcal{D}'_{a,b})$.

О п р е д е л е н и е 2.11. Обозначим

$$\Lambda_{\mathbb{K}} = \sup_{a/b \in \mathbb{F}_1^*} \inf_{q \in \mathbb{K}} \frac{\upsilon(a - bq)}{\upsilon(b)}$$

2.2 Теорема Кронекера-Валена в классе $\mathcal{T}$

Обозначим

$$[x_1 : x_2 : \ldots : x_k] := x_1 + \cfrac{1}{x_2 + \cfrac{1}{x_3 + \cfrac{1}{\ddots + \cfrac{1}{x_k}}}} \tag{2.1}$$

Для $\alpha \in \mathbb{F}_1$ и $k \in \mathbb{N}$ уравнение $[x_1 : x_2 : \ldots : x_k] = \alpha$ будем называть (α, k)-разрешимым, если существуют $x_1, \ldots, x_k \in \mathbb{K}$ такие, что $\alpha = [x_1 : x_2 : \ldots : x_k]$.

Лемма 2.1. *Пусть $\mathbb{K} \in \mathcal{T}$, $\alpha \in \mathbb{F}_1$ и $k \in \mathbb{N}$. Уравнение 2.1 является (α, k)-разрешимым тогда и только тогда, когда $\omega^{(k-1)}(\alpha) = 0$.*

Д о к а з а т е л ь с т в о. Заметим, что для $\alpha = 0$ или $k = 1$ утверждение очевидно. Далее будем полагать, что $\alpha = m/n \neq 0$, $\gcd(m,n) = 1$ и $k \geq 2$.

Рассмотрим случай $k = 2$. Имеем уравнение

$$\frac{m}{n} = x_1 + \frac{1}{x_2} = \frac{x_1 x_2 + 1}{x_2}.$$

Следовательно, выполнено $m \equiv \varepsilon (\text{mod } n)$ для некоторого $\varepsilon \in \mathbb{I}$. Пусть $m = qn + \varepsilon$, $q \in \mathbb{K}$, тогда $m/n = \text{fr}(m/n) = \text{fr}(q + \varepsilon/n) = \text{fr}(\varepsilon/n) = \varepsilon/n$. Тогда $\omega(\alpha) = \text{fr}(n/\varepsilon) = 0$. В обратную сторону доказывается аналогично.

Заметим, что 2.1 (α,k)-разрешимо тогда и только тогда, когда существует $z \in \mathbb{K}$ такой, что 2.1 $((\alpha - z)^{-1},k-1)$-разрешимо. Следовательно, мы должны доказать, что для любого k выполнено: $\omega^{(k-1)}(\alpha) = 0$ тогда и только тогда, когда существует $z \in \mathbb{K}$ такой, что $\omega^{(k-2)}(\text{fr}((\alpha - z)^{-1})) = 0$.

Предположим, что $\omega^{(k-1)}(\alpha) = 0$, тогда по определению имеем $\omega^{(k-2)}(\text{fr}(\alpha^{-1})) = 0$.

Теперь докажем в обратную сторону. Для начала докажем для всех $k \leq D_{\mathbb{K}}$, где $D_{\mathbb{K}}$ из определения множества $\mathcal{T}$. Если $D_{\mathbb{K}} \leq 2$, то утверждение уже доказано. Предположим, что $D_{\mathbb{K}} \geq 3$.

Доказательство проведем с помощью индукции по k. База индукции – лемма верна для $k = 1, 2$. Предположим, что утверждение верно для всех $k < k'$ и докажем, что оно выполнено для k'. Согласно условию, существует $z \in \mathbb{K}$ такой, что $\omega^{(k'-2)}(\text{fr}((\alpha - z)^{-1})) = 0$. Если $z = 0$, то из определения ω следует, что $\omega^{(k'-1)}(\alpha) = 0$. Далее предполагаем, что $z \neq 0$. Тогда из условия (2) определения множества $\mathcal{T}$ следует, что тройка $(z, \alpha, k' - 2)$ регулярная. Следовательно, существует натуральные числа p и l, $p \leq k' - 2$, $l \leq p + 1$, такие, что существуют обратимые элементы $\varepsilon_i \in \mathbb{I}$, $\varepsilon \in \{0,1\}$ и элементы $b_i,c_i \in \mathbb{K}$ $(i = 1,\ldots,l-1)$, для которых выполнено:

$$\begin{gathered} \beta_1 = \omega^{(p)}(\text{fr}((\alpha - z)^{-1})), \\ \beta_{i+1} = (\varepsilon_i\beta_i + c_i)^{-1} + b_i, i = \overline{1,l-1}, \\ \beta_l = \alpha^{(-1)^{\varepsilon}}. \end{gathered} \tag{2.2}$$

Из равенств $\omega^{(k'-2)}(\text{fr}((\alpha - z)^{-1})) = 0$ и $\beta_1 = \omega^{(p)}(\text{fr}((\alpha - z)^{-1}))$ следует, что $\omega^{(k'-p-2)}(\beta_1) = 0$. Тогда, предположению индукции, 2.1 $(\beta_1, k' - p - 1)$-разрешимо.

Из 2.2 следует, что для любых $i = 1,\ldots,l-1$ и $j \in \mathbb{N}$ уравнение 2.1 (β_i,j)-разрешимо тогда и только тогда, когда 2.1 $(\beta_{i+1},j+1)$-разрешимо. Следовательно, 2.1 $(\alpha^{(-1)^{\varepsilon}}, k' - p + l - 2)$-разрешимо. Так как $k' - p + l - 2 \leq k' - 1 < k$, то по предположению индукции получаем, что $\omega^{(k'-p+l-3)}(\text{fr}(\alpha^{(-1)^{\varepsilon}})) = 0$. Тогда, используя определение ω получаем, что $\omega^{(k'-2)}(\text{fr}(\alpha^{(-1)^{\varepsilon}})) = 0$. Если в последнем равенстве $\varepsilon = 1$, то имеем $0 = \omega^{(k'-2)}(\text{fr}(\alpha^{(-1)})) = \omega^{(k'-2)}(\omega(\alpha)) = \omega^{(k'-1)}(\alpha)$. Если $\varepsilon = 0$, то $0 = \omega^{(k'-2)}(\text{fr}(\alpha)) = \omega^{(k'-2)}(\alpha)$, следовательно, $\omega^{(k-1)}(\alpha) = 0$. Таким образом доказали лемму для всех $k \leq D_{\mathbb{K}}$.

Теперь докажем для $k > D_{\mathbb{K}}$. Аналогично индукцией по k. База индукции — лемма верна для $k \leq D_{\mathbb{K}}$. Предположим, что утверждение верно для всех $k < k'$ и докажем, что оно выполнено для k'. Согласно условию, существует $z \in \mathbb{K}$ такой, что $\omega^{(k'-2)}(\text{fr}((\alpha - z)^{-1})) = 0$. Если $z = 0$, то, по определению ω, мы имеем $\omega^{(k'-1)}(\alpha) = 0$. Предположим, что $z \neq 0$. Тогда из условия (1) определения множества $\mathcal{T}$, получаем, что тройка $(z, \alpha, D_{\mathbb{K}})$ регулярная. Далее

доказательство почти дословно повторяет случай $k \leq D_{\mathbb{K}}$. Таким образом лемма доказана. $\otimes$

Лемма 2.2. *Пусть $\mathbb{K}$ кольцо с единственной факторизацией. Тогда для любых двух элементов $(a,b) \in \mathbb{K}_* \times \mathbb{K}_*$ выполнено*

$$\mathcal{L}_{a,b} = \min\{k \in \mathbb{N} | \omega^{(k-1)}(\mathrm{fr}(a/b)) = 0\},$$

где $\min \emptyset = \infty$.

Доказательство. Рассмотрим произвольные $a, b \in \mathbb{K}_*$. Предположим, что $\mathcal{L}_{a,b} < \infty$. Пусть

$$\mathcal{g}_{a,b} = \mathcal{D}_{a,b}(q_1, \ldots, q_k) = (r_{-1}, r_0, r_1, \ldots, r_{k-1}, r_k),$$

где $r_{-1} = a, r_0 = b, r_k = 0, r_i \neq 0$ для любого $i = \overline{1,k-1}$.

Из равенств

$$\frac{a}{b} = q_1 + \frac{r_1}{b}, \frac{b}{r_1} = q_2 + \frac{r_2}{r_1}, \ldots, \frac{r_{k-3}}{r_{k-2}} = q_{k-1} + \frac{r_{k-1}}{r_{k-2}}, \frac{r_{k-2}}{r_{k-1}} = q_k$$

и определения ω и цепочки деления с выбором минимального по норме остатка следует, что выполнены следующие равенства

$$\omega\left(\mathrm{fr}\left(\frac{a}{b}\right)\right) = \mathrm{fr}\left(\frac{b}{r_1}\right), \omega^{(2)}\left(\mathrm{fr}\left(\frac{a}{b}\right)\right) = \mathrm{fr}\left(\frac{r_1}{r_2}\right), \ldots,$$
$$\omega^{(k-1)}\left(\mathrm{fr}\left(\frac{a}{b}\right)\right) = \mathrm{fr}\left(\frac{r_{k-2}}{r_{k-1}}\right) = 0. \quad (2.3)$$

Следовательно, $\omega^{(k-1)}(\mathrm{fr}(a/b)) = 0$. Из того, что $\omega^{(j-1)}(\mathrm{fr}(a/b)) = r_j/r_{j-1} \neq 0$ для любого $j = 1, \ldots, k-1$ следует, что $\mathcal{L}_{a,b} = k = \min\{n \in \mathbb{N} | \omega^{(n-1)}(\mathrm{fr}(a/b)) = 0\}$.

Пусть $\mathcal{L}_{a,b} = \infty$. Предположим, что существует $k \in \mathbb{N}$ такое, что $\omega^{(k-1)}(\mathrm{fr}(a/b)) = 0$. Выберем наименьшее натуральные k с этим свойством.

Пусть $\mathrm{int}(a/b) = q_1, \mathrm{fr}(a/b) = r_1/b$. Если $r_1 = 0$, то $\mathcal{L}_{a,b} = 1$, что является противоречием. Следовательно, $r_1 \neq 0$. Из определения ω следует, что $\omega^{(k-2)}(\mathrm{fr}(b/r_1)) = 0$. Пусть $\mathrm{int}(b/r_1) = q_2, \mathrm{fr}(b/r_1) = r_2/r_1$. Если $r_2 = 0$, то $\mathcal{L}_{a,b} = 2$, что является противоречием. Следовательно, $r_2 \neq 0$ и $\omega^{(k-3)}(\mathrm{fr}(r_1/r_2)) = 0$. Аналогично строим элементы $r_3, \ldots, r_k$, $q_3, \ldots, q_k$ такие, что $\mathrm{int}(r_{i-2}/r_{i-1}) = q_i, \mathrm{fr}(r_{i-2}/r_{i-1}) = r_i/r_{i-1}$ для всех $i = \overline{3,k}$ и $\omega^{(0)}(\mathrm{fr}(r_{k-2}/r_{k-1})) = r_k/r_{k-1} = 0$. Получаем, что $r_k = 0$. Это противоречит тому, что $\mathcal{L}_{a,b} = \infty$. Таким образом, утверждение доказано. $\otimes$

Теорема 2.1. *Пусть* $\mathbb{K} \in \mathcal{T}$. *Тогда цепочка делений с выбором минимального по норме остатка является минимальной, т.е.* $\mathcal{L}_{a,b} = \ell_{a,b}$ *для любых* $a,b \in \mathbb{K}_*$.

Доказательство. Пусть $(a,b) \in \mathbb{K}_* \times \mathbb{K}_*$. Предположим, что $\ell_{a,b} = k < \infty$. Пусть

$$\mathcal{D}_{a,b}(q_1,\ldots,q_k) = (r_{-1},r_0,r_1,\ldots,r_{k-1},r_k) \in \mathcal{O}_{a,b},$$

где $r_{-1} = a, r_0 = b, r_k = 0, r_i \neq 0$ для всех $i = \overline{1,k-1}$.

Тогда по определению имеем множество равенств

$$\begin{aligned} r_{-1} &= a \\ r_0 &= b \\ r_i &= r_{i-2} - q_i r_{i-1}, i = \overline{1,k}. \end{aligned}$$

Разделим последнее равенство на r_{i-1} и поменяем местами слагаемые и получим

$$\begin{aligned} \frac{a}{b} &= q_1 + \frac{r_1}{b} \\ \frac{b}{r_1} &= q_2 + \frac{r_2}{r_1} \\ &\cdots \\ \frac{r_{k-2}}{r_{k-1}} &= q_k + \frac{r_k}{r_{k-1}} = q_k \end{aligned}$$

Из этого получаем, что $a/b = [q_1 : q_2 : \cdots : q_k]$. Следовательно, уравнение 2.1 $(a/b,k)$-разрешимо. Это равносильно тому, что 2.1 $(\mathrm{fr}(a/b),k)$-разрешимо. Тогда, по лемме 2.1, выполнено $\omega^{(k-1)}(\mathrm{fr}(a/b)) = 0$. Используя лемму 2.2 получаем

$$\mathcal{L}_{a,b} = \min\{r \in \mathbb{N} | \omega^{(r-1)}(\mathrm{fr}(a/b)) = 0\} \leq k = \ell_{a,b}.$$

Следовательно, $\mathcal{L}_{a,b} = \ell_{a,b}$.

Если $\ell_{a,b} = \infty$, то $\mathcal{E}_{a,b} = \emptyset$. Следовательно, $\mathcal{L}_{a,b} = \infty$. Таким образом теорема доказана. $\otimes$

Теорема 2.2. *Следующие утверждения являются верными:*

1. *Если* $\mathbb{K}$ *евклидово кольцо относительно нормы* υ, *то* $\Lambda_{\mathbb{K}} \in [0,1]$.
2. *Если* $\mathbb{K}$ *– кольцо с единственной факторизацией, заданной нормой* υ *и* $\Lambda_{\mathbb{K}} \in [0,1)$, *то* $\mathbb{K}$ *евклидово относительно нормы* υ *и выполнено следующее неравенство*

$$l_n(\mathbb{K}) \leq [\log_{\Lambda_{\mathbb{K}}^{-1}} n] + 2$$

для любого $n \in \mathbb{N}$, *где* $\log_\infty n = 0$.

Доказательство. Пусть $\mathbb{K}$ — евклидово кольцо относительно нормы υ. Тогда для любых a и $b \in \mathbb{K}_*$ существует q и $r \in \mathbb{K}$ такие, что $a = bq + r$ и $\upsilon(r) < \upsilon(b)$. Тогда $\upsilon(a - bq) < \upsilon(b)$, из чего следует утверждение первого пункта.

Теперь докажем вторую часть теоремы. Предположим, что $\Lambda_{\mathbb{K}} \in [0,1)$. Возьмем произвольный $a/b \in \mathbb{F}_1^*$. Согласно предположению и определению $\Lambda_{\mathbb{K}}$, имеем

$$\inf_{q \in \mathbb{K}} \frac{\upsilon(a - bq)}{\upsilon(b)} < 1.$$

Возьмем $q = \text{int}(a/b)$, $r = b\text{fr}(a/b)$. Тогда $a = bq + r$ и $\upsilon(r) \leq \Lambda_{\mathbb{K}}\upsilon(b)$. Если $\upsilon(b) = 0$, то b обратимый элемент в $\mathbb{K}$ и, следовательно, $r = 0$. Если $\upsilon(b) > 0$, то $\upsilon(r) \leq \Lambda_{\mathbb{K}}\upsilon(b) < \upsilon(b)$. Так как $\upsilon(r) < \upsilon(b)$, то кольцо $\mathbb{K}$ евклидово относительно нормы υ.

Зафиксируем некоторое $n \in \mathbb{N}$. Рассмотрим произвольные $(a,b) \in \mathbb{K}_* \times \mathbb{K}_*$ такие, что $\gcd(a,b) = 1$ и $n \geq \upsilon(a) \geq \upsilon(b)$. Так как кольцо евклидово, то $\mathcal{E}_{a,b} \neq \emptyset$, а так же существует $\mathcal{g}_{a,b} = \mathcal{D}_{a,b}(q_1, \ldots, q_k) = (r_{-1}, r_0, r_1, \ldots, r_{k-1}, r_k)$. Заметим, что $\gcd(r_{i-1}, r_i) = 1$ для всех $i = 1, \ldots, k$. Так как $\text{fr}(r_{i-2}/r_{i-1}) = r_i/r_{i-1} \neq 0$, $i = 1, \ldots, k-1$, то

$$|r_i/r_{i-1}| = \upsilon(r_i)/\upsilon(r_{i-1}) \leq \Lambda_{\mathbb{K}}$$

для $i = 1, \ldots, k-1$. Следовательно,

$$\upsilon(r_i) \leq \upsilon(b)\Lambda_{\mathbb{K}}^i \leq n\Lambda_{\mathbb{K}}^i$$

для $i = 1, \ldots, k-1$. Так как $r_{k-2} \notin \mathbb{I} \cup \{0\}$, то $1 \leq \upsilon(r_{k-2}) \leq n\Lambda_{\mathbb{K}}^{k-2}$. Следовательно, $k \leq \log_{\Lambda_{\mathbb{K}}^{-1}} n + 2$. Итого, $l_n(\mathbb{K}) \leq [\log_{\Lambda_{\mathbb{K}}^{-1}} n] + 2$. $\otimes$

Таким образом аналог теоремы Кронекера-Валена верен для всех колец из класса $\mathcal{T}$.

2.3 Алгоритм проверки принадлежности кольца классу $\mathcal{T}$

Опишем метод проверки включения $\mathbb{K} \in \mathcal{T}$.

Определение 2.12. Обозначим через $\mathcal{S}$ множество факториальных колец $\mathbb{K}$ такое, что для любых $x \in \mathbb{K}_*$ и $\alpha \in \mathbb{F}_1^*$ выполнено одно из условий:

1. $\text{int}((\alpha - x)^{-1}) \in \mathbb{I} \cup \{0\}$;
2. $x\,\text{int}((\alpha - x)^{-1}) + 1 \in \mathbb{I}$.

Предложение 2.1. *Выполнено включение $\mathcal{S} \subseteq \mathcal{T}$.*

Доказательство. Предположим, что $\mathbb{K} \in \mathcal{S}$. Положим $D_{\mathbb{K}} = 1$. Надо доказать. что для любых $x_0 \in \mathbb{K}_*, \alpha \in \mathbb{F}_1^*$ тройка $(x_0,\alpha,D_{\mathbb{K}})$ регулярная. Выберем $p = 1$ в определении регулярной тройки. Обозначим $b = \text{int}((\alpha - x)^{-1})$.

Предположим, что выполнено первое условие определения множества $\mathcal{S}$. Это значит, что $b \in \mathbb{I} \cup \{0\}$. Тогда

$$\beta_1 = \omega(\text{fr}((\alpha - x)^{-1})) = \omega((\alpha - x)^{-1} - b) = \text{fr}\left(\frac{\alpha - x}{1 - b\alpha + bx}\right) = \\ = \frac{\alpha - x}{1 - b\alpha + bx} - c$$

для некоторого $c \in \mathbb{K}$.

Предположим, что $b = 0$. Тогда

$$\beta_1 = \alpha - x - c$$
$$\beta_2 = (\beta_1 + x + c)^{-1} = \alpha^{-1}$$

Предположим, что $b \in \mathbb{I}$. Тогда $\beta_1 = \frac{b^{-1}}{1-b\alpha+bx} - b^{-1} - c$ и $\beta_2 = \alpha = (-b^2\beta_1 - b - b^2c)^{-1} + b^{-1} + x$.

$$\beta_1 = \frac{\alpha - x}{1 - b\alpha + bx} - c = \frac{b^{-1}}{1 - b\alpha + bx} - b^{-1} - c$$
$$\beta_2 = (-b^2\beta_1 - b - b^2c)^{-1} + b^{-1} + x = \alpha$$

Предположим, что выполнено второе условие определения множества $\mathcal{S}$. Это значит, что $xb + 1 \in \mathbb{I}$. Аналогично получаем, что

$$\beta_1 = \omega(\text{fr}((\alpha - x)^{-1})) = \omega((\alpha - x)^{-1} - b) = \text{fr}\left(\frac{\alpha - x}{1 - b\alpha + bx}\right) = \\ = \frac{\alpha - x}{1 - b\alpha + bx} - c$$

для некоторого $c \in \mathbb{K}$. Положим

$$\beta_2 = (\beta_1(xb+1)^2 + c(xb+1)^2 + x(xb+1))^{-1} + b(xb+1)^{-1} = \\ = (\beta_1(xb+1) + c(xb+1) + x)^{-1}(xb+1)^{-1} + b(xb+1)^{-1} = \\ = \left(\frac{(\alpha - x)(xb+1)}{1 - b\alpha + bx} + x\right)^{-1}(xb+1)^{-1} + b(xb+1)^{-1} = \\ = \left(\frac{bx\alpha + \alpha - bx^2 - x + x - bx\alpha + bx^2}{1 - b\alpha + bx}\right)^{-1}(xb+1)^{-1} + b(xb+1)^{-1} = \\ = \left(\frac{\alpha}{1 - b\alpha + bx}\right)^{-1}(xb+1)^{-1} + b(xb+1)^{-1} = \\ = (xb+1)^{-1}\left(\frac{1 - b\alpha + bx}{\alpha} + b\right) = \alpha^{-1}$$

Следовательно, тройка $(x_0,\alpha,D_{\mathbb{K}})$ регулярная и предложение доказано. $\otimes$

Алгоритм 2.1 Алгоритм проверки условия $\mathbb{K} \in \mathcal{S}$

1: $\mathbb{J} \leftarrow \{x \in \mathbb{K}_* | \text{int}((\alpha - x)^{-1}) \in \mathbb{I} \cup \{0\}\ \forall \alpha \in \mathbb{F}_1^*\}$.
2: Для $x_0 \in \mathbb{K}_* \setminus \mathbb{J}$ вычислить $\mathbb{Y}(x_0)$ – множество значений функции $f_{x_0}(\alpha) = \text{int}((\alpha - x_0)^{-1}), \alpha \in \mathbb{F}_1^*$.
3: Для $x_0 \in \mathbb{K}_* \setminus \mathbb{J}$ вычислить $\mathbb{U}(x_0) \leftarrow \{\frac{\varepsilon-1}{x_0} \in \mathbb{K} | \varepsilon \in \mathbb{I}\} \cup \mathbb{I}$.
4: **if** $\mathbb{Y}(x_0) \subseteq \mathbb{U}(x_0)$ для любого $x_0 \in \mathbb{K}_* \setminus \mathbb{J}$ **then**
5: **return** "Да", $\mathbb{K} \in \mathcal{S}$
6: **else**
7: **return** "Неизвестно"
8: **end if**

Замечание 2.1. Алгоритм корректен. Предположим, что ответ "Да". Рассмотрим произвольный $x_0 \in \mathbb{K}$. Если $x_0 \in \mathbb{J}$, то первое условие из определения выполнено. Предположим, что $x_0 \notin \mathbb{J}$. Тогда $x_0 \in \mathbb{K}_* \setminus \mathbb{J}$. Рассмотрим множества $\mathbb{Y}(x_0)$ и $\mathbb{U}(x_0)$. Предположим, что $y \in \mathbb{Y}(x_0)$, тогда $y = \text{int}((\alpha - x_0)^{-1})$. С другой стороны $y \in \mathbb{U}(x_0)$, тогда или $y \in \mathbb{I}$ и первое условие определения выполнено, или $y = \frac{\varepsilon-1}{x_0}$. Тогда

$$\frac{\varepsilon - 1}{x_0} = \text{int}((\alpha - x_0)^{-1}).$$

В этом случае выполнено второе условие из определения множества S.

Используя полученный алгоритм можно получить примеры факториальных колец $\mathbb{K}$ из класса $\mathcal{S}$.

Пример 2.4. Пусть $\mathbb{K} = \mathbb{Z}$. Норма задана функцией $\upsilon(a) = |a|$, $a \in \mathbb{Z}_*$. Дробная часть $\text{fr}(\alpha) = \alpha - [\alpha + 1/2]$, $\alpha \in \mathbb{Q}$.

1. $\mathbb{J} = \{x \in \mathbb{Z} \big| |x| > 1\}$;
2. $\mathbb{Y}(1) = \{-2, -1\}$, $\mathbb{Y}(-1) = \{1,2\}$;
3. $\mathbb{U}(1) = \{-2, -1,0,1\}$, $\mathbb{U}(-1) = \{-1,0,1,2\}$;
4. $\mathbb{Y}(1) \subseteq \mathbb{U}(1)$, $\mathbb{Y}(-1) \subseteq \mathbb{U}(-1)$.

Следовательно, $\mathbb{Z} \in \mathcal{S}$.

Пример 2.5. Пусть $\mathbb{K} = \mathbb{P}[t]$, где $\mathbb{P}$ – поле. Норма задана функцией $\upsilon(f) = \deg f$, $f \in \mathbb{P}[t]$. Дробная часть $\text{fr}(m(t)/n(t)) = r(t)/n(t)$, $m(t) \equiv r(t) (\text{mod}\, n(t))$, $\deg r < \deg n$, $m(t)/n(t) \in \mathbb{P}(t)$.

1. $\mathbb{J} = \mathbb{K}_*$;
2. $\mathbb{K}_* \setminus \mathbb{J} = \emptyset$;

Следовательно, $\mathbb{P}[t] \in \mathcal{S}$.

Пример 2.6. Пусть $\mathbb{K}$ это координатное кольцо $\mathbb{Q}[i][x,y]/(x^2+y^2+1)$. Известно, что это кольцо изоморфно $\mathbb{Q}[i][t,t^{-1}]$, где отображение задано следующим образом

$$X \to \cos\theta \to \frac{e^{ix}+e^{-ix}}{2} \to \frac{t+t^{-1}}{2}$$
$$Y \to \sin\theta \to \frac{-ie^{ix}+ie^{-ix}}{2} \to \frac{-it+it^{-1}}{2}$$

Так же известно, что $Q[i][t,t^{-1}]$ – факториальное.

Обратимыми элементами в этом кольце являются одночлены вида αt^k, где $\alpha \in \mathbb{Q}[i]$, $k \in \mathbb{Z}$. Введем норму в этом кольце следующим образом

$$\upsilon(x) = \upsilon\left(\sum_{i=k_1}^{k_2} \alpha_i t^i\right) = k_2 - k_1$$

где $\alpha_i \in \mathbb{Q}[i]$, если $x \neq 0$ и $\upsilon(0) = -\infty$. Проверим критерии. Рассмотрим два элемента кольца

$$x = \sum_{i=k_1}^{k_2} \alpha_i t^i$$
$$y = \sum_{i=l_1}^{l_2} \beta_i t^i$$

При умножении максимальная степень будет равна k_2+l_2, а минимальная k_1+l_1. Тогда $\upsilon(xy) = k_2+l_2-k_1-l_1 \geq k_2-k_1$. Это равенство будет выполняться только если $l_2-l_1=0$. А это будет означать, что $y \in \mathbb{I}$.

Покажем, что $\text{fr}(\alpha) = \varepsilon^{-1}\text{fr}(\varepsilon\alpha)$ для $\varepsilon \in \mathbb{I}$, $\alpha \in \mathbb{K}$. Предположим, что $\text{fr}\left(\frac{m}{n}\right) = \frac{r}{n}$. Это означает, что $n|(m-r)$ и r имеет минимальную норму из возможных. Так как норма не меняется при умножении на обратимый элемент, то εr будет иметь минимальную норму, а так же $n|(\varepsilon m - \varepsilon r)$. Следовательно, имеем $\text{fr}(\alpha) = \varepsilon^{-1}\text{fr}(\varepsilon\alpha)$ для $\varepsilon \in \mathbb{I}$, $\alpha \in \mathbb{K}$. Тогда $\text{int}(\alpha) = \varepsilon^{-1}\text{int}(\varepsilon\alpha)$ для $\varepsilon \in \mathbb{I}$, $\alpha \in \mathbb{K}$.

Заметим, что умножив $\text{int}((\alpha - x)^{-1})$ на некоторый обратимый элемент можно сделать так, что α принадлежит полю частных кольца многочленов, а x это многочлен. Тогда этот пример будет аналогичным примеру с многочленами. Следовательно, для данного координатного кольца выполнен аналог теоремы Кронекера-Валена.

Пример 2.7. Пусть $\mathbb{K} = \mathbb{Z}[t]$, $\upsilon(f) = \deg f$, $f \in \mathbb{Z}[t]$. Определим дробную часть в $\mathbb{F} = \mathbb{Z}(t)$ следующим образом. Рассмотрим отображение $\mathcal{A} : \mathbb{F}/\mathbb{K} \to \mathbb{F}$:

$$\mathcal{A}(\mathbb{A}) = m(t)/n(t),$$

где $\mathbb{A} = \{m(t)/n(t) + q(t) | q(t) \in \mathbb{Z}[t]\}$. Для произвольных $\mathbb{A} \in \mathbb{F}/\mathbb{K}$, $\alpha \in \mathbb{A}$ положим

$$\begin{gathered}\text{int}(\alpha) = r(t),\\ \text{fr}(\alpha) = \mathcal{A}(\mathbb{A}) - r(t),\end{gathered}$$

где $r(t) \in \mathbb{Z}[t]$ и для любого $p(t) \in \mathbb{Z}[t]$

$$\lim_{t\to+\infty} \left| \frac{\mathcal{A}(\mathbb{A}) - r(t)}{\mathcal{A}(\mathbb{A}) - p(t)} \right| \leq 1.$$

Докажем, что

$$\mathbb{J} \supseteq \{f \in \mathbb{Z}[t] | \deg f > 0 \text{ или } |f(t)| \equiv |x_0| > 2\}.$$

Рассмотрим произвольные $\mathbb{A} \in \mathbb{F}/\mathbb{K}$ и $\alpha = m(t)/n(t) \in \mathbb{A}$, $\alpha = \text{fr}(\alpha)$.

Имеем два случая. Предположим, что $\deg m > \deg n$. Из того, что $\alpha = \text{fr}(\alpha)$ и определения дробной части следует, что

$$1 \geq \lim_{t\to+\infty} \left| \frac{\frac{m(t)}{n(t)}}{\frac{m(t)}{n(t)} - p(t)} \right| = \lim_{t\to+\infty} \left| \frac{m(t)}{m(t) - n(t)p(t)} \right|.$$

Следовательно, получаем, что для любых $p(t) \in \mathbb{Z}[t]$ выполнено $\deg m(t) \leq \deg(m(t) - n(t)p(t))$. Предположим, что $\text{int}((\alpha - x_0)^{-1}) = r(t) \not\equiv 0$ для некоторого $x_0(t) \in \mathbb{Z}[t]$. Тогда

$$\begin{gathered}\text{fr}((\alpha - x_0)^{-1}) = (\alpha - x_0)^{-1} - r =\\ = \left(\frac{m}{n} - x_0\right)^{-1} - r = \frac{n}{m - x_0 n} - r =\\ = \frac{n - r(m - nx_0)}{m - nx_0}.\end{gathered}$$

Из того, что $\deg n < \deg m \leq \deg(m - nx_0)$ следует, что $\deg(n - r(m - nx_0)) > \deg n$. Однако выше показано, что $\deg(n - r(m - nx_0)) < \deg n$, исходя из определения дробной части. Получаем противоречие. Следовательно, если $\deg m > \deg n$, то для любого $x_0 \in \mathbb{Z}[t]$ выполнено $\text{int}((\alpha - x_0)^{-1}) = 0$.

Теперь предположим, что $\deg m \leq \deg n$. Предположим, что $\text{int}((\alpha - x_0)^{-1}) = r(t) \not\equiv 0$ для некоторого $x_0 \in \mathbb{Z}[t]$, $\deg x_0 > 0$. Тогда $\deg(m - nx_0) > \deg n$. Следовательно, имеем $\deg(n - r(m - nx_0)) > \deg n$. А это противоречит определению дробной части. Следовательно, если $\deg m \leq \deg n$, то для любого $x_0 \in \mathbb{Z}[t]$, $\deg x_0 > 0$ выполнено $\text{int}((\alpha - x_0)^{-1}) = 0$.

Предположим, что $\text{int}((\alpha - x_0)^{-1}) = r(t) \not\equiv 0$ для некоторого $x_0 = c \in \mathbb{Z} \setminus \{0, \pm 1, \pm 2\}$. Если $\deg m < \deg n$, то $\deg n < \deg(n - r(m - nc))$ или

$r = const$. Первый вариант противоречит определению дробной части. Если $r = const$, то $\lim_{t\to+\infty}\left|\frac{n(t)-r(m(t)-n(t)c)}{n(t)}\right| = |1+rc| \geq 2$, но это противоречит определению дробной части. Таким образом имеем $\deg m = \deg n$. Учитывая то, что $\alpha = \mathrm{fr}(\alpha)$ и $\deg m = \deg n$ получаем $\lim_{t\to+\infty}\left|\frac{m(t)}{n(t)}\right| \leq 0.5$. Если $\deg r > 0$, то $\deg n < \deg(n-r(m-nc))$, но это противоречие. Таким образом $r = const$ и

$$\lim_{t\to+\infty}\left|\frac{n(t)-r(m(t)-n(t)c)}{n(t)}\right| \geq |1+rc| - |r|/2 \geq \tag{2.4}$$

$$\geq |r|(|c|-1/2) - 1 \geq \frac{3}{2}, \tag{2.5}$$

но это противоречит определению дробной части.

Таким образом $\mathbb{J} \supseteq \{f \in \mathbb{Z}[t] | \deg f > 0$ или $|f(t)| \equiv |x_0| > 2\}$. Если $x_0 \equiv \pm 2$, то $\mathrm{int}((\alpha - x_0)^{-1}) = r(t) \not\equiv 0$ тогда и только тогда, когда $\deg m = \deg n$ и $r(t) \equiv \pm 1$, откуда следует, что $\pm 2 \in \mathbb{J}$. Несложно показать, что $0, \pm 1 \notin \mathbb{J}$.

Тогда $\mathbb{K}_*\backslash\mathbb{J} \subseteq \{\pm 1\}$. Вычисляем $\mathbb{Y}(1) = \{-2, -1\}$, $\mathbb{Y}(-1) = \{1,2\}$ и $\mathbb{U}(1) = \{-2, -1,0,1\}$, $\mathbb{U}(-1) = \{-1,0,1,2\}$.

Следовательно, $\mathbb{Z}[t] \in \mathcal{S}$.

Пример 2.8. Пусть $\mathbb{K}$ евклидово кольцо такое, что для любых $a,b \in \mathbb{K}$ или $a|b$, или $b|a$. В этом случае $\mathbb{F} = \mathbb{K} \cup \{1/a | a \in \mathbb{K}_*\backslash\mathbb{I}\}$.

Докажем, что $\mathbb{J} = \mathbb{K}_*$. Рассмотрим произвольный $\alpha \in \mathbb{F}_1^*$, тогда существует $b \in \mathbb{K}_*\backslash\mathbb{I}$ такой, что $\alpha = 1/b$. Пусть $x \in \mathbb{K}_*$. Покажем, что $\mathrm{int}((\alpha - x)^{-1}) = (\alpha - x)^{-1}$. Имеем $(\alpha - x)^{-1} = \frac{b}{1-bx}$. Предположим, что $\mathrm{fr}(\frac{b}{1-bx}) \neq 0$, что эквивалентно утверждению, что $\frac{b}{1-bx} = \frac{1}{c}$ для некоторого $c \in \mathbb{K}_*\backslash\mathbb{I}$. Так как b и $1-bx$ взаимнопростые, то $b \in \mathbb{I}$. Следовательно, имеем $\alpha - x = b^{-1} - x \in \mathbb{K}$, это означает, что $\alpha \in \mathbb{K}$, но это противоречит условию $\alpha \in \mathbb{F}_1^*$. Таким образом имеем $x\ \mathrm{int}((\alpha - x)^{-1}) + 1 = \frac{1}{1-bx}$. Предположим, что $1 - bx \in \mathbb{K}_*\backslash\mathbb{I}$. Так как b и $1 - bx$ взаимнопростые, то $b|(1 - bx)$. Следовательно, $b \in \mathbb{I}$. Из последнего следует, что $\alpha - x = b^{-1} - x \in \mathbb{K}$, но это противоречит условию $\alpha \in \mathbb{F}_1^*$. Итого получаем $1 - bx \in \mathbb{I}$. Следовательно, $x\ \mathrm{int}((\alpha - x)^{-1}) + 1 \in \mathbb{I}$.

Тогда $\mathbb{K}_*\backslash\mathbb{J} = \emptyset$. Следовательно, $\mathbb{K} \in \mathcal{S}$.

Рассмотрим пример факториального кольца, не лежащего в $\mathcal{S}$, но лежащего в $\mathcal{T}$.

Замечание 2.2. Пусть $d \neq 1$ целое число свободное от квадратов. Через $\mathbb{Z}[\sqrt{d}]$ будем обозначать кольцо алгебраических целых чисел квадратичного поля $\mathbb{Q}[\sqrt{d}]$. Известно, что (see, e.g., [29])

$$\mathbb{Z}[\sqrt{d}] = \begin{cases} \left\{a + b\sqrt{d} | a,b \in \mathbb{Z}\right\}, & \text{если } d \not\equiv 1(\mathrm{mod}\ 4) \\ \left\{\frac{a+b\sqrt{d}}{2} \middle| a,b \in \mathbb{Z}, a \equiv b(\mathrm{mod}\ 2)\right\}, & \text{если } d \equiv 1(\mathrm{mod}\ 4). \end{cases}$$

Пусть норма в $\mathbb{Z}[\sqrt{d}]$ определена следующим образом:

$$\upsilon(a+b\sqrt{d}) = |a^2 - db^2| \text{ для } a+b\sqrt{d} \in \mathbb{Z}[\sqrt{d}] \setminus \{0\}, a, b \in \mathbb{Q}, \quad \upsilon(0) = -\infty. \tag{2.6}$$

Пусть дробная часть в $\mathbb{Q}[\sqrt{d}]$ для $d < 0$ определена следующим образом:

$$\text{fr}(q_1 + q_2\sqrt{d}) = q_1 - [q_1 + 1/2] + (q_2 - [q_2 + 1/2])\sqrt{d}, \tag{2.7}$$

где q_1, $q_2 \in \mathbb{Q}$, $[x] = \max\{k \in \mathbb{Z} | k \leq x\}$.

Пример 2.9. Пусть $\mathbb{K} = \mathbb{Z}[i]$. Пусть норма в $\mathbb{Z}[i]$ и дробная часть в $\mathbb{Q}[i]$ заданы соотношениями 2.6 и 2.7.

Покажем, что кольцо $\mathbb{Z}[i]$ не принадлежит $\mathcal{S}$. Выберем $\alpha = \frac{9-4i}{20}$, $x = 1$. Тогда $\text{int}((\alpha - x)^{-1}) = -2 + i \notin \mathbb{I} \cup \{0\}$ и $x\ \text{int}((\alpha - x)^{-1}) + 1 = -1 + i \notin \mathbb{I}$.

Покажем, что $\mathbb{K} \in \mathcal{T}$. Заметим, что $\mathbb{F}_1 = \{z \in \mathbb{C} | Re(z), Im(z) \in \mathbb{Q} \cap [-1/2, 1/2[\}$. Положим $D_{\mathbb{K}} = 3$ в определении множества $\mathcal{T}$.

Проверим первое условие из определения $\mathcal{T}$. Рассмотрим произвольные $x_0 \in \mathbb{Z}[i] \setminus \{0\}$ и $\alpha \in \mathbb{F}_1^*$. Обозначим $b = \text{int}((\alpha - x_0)^{-1})$. Пусть p — число из первого условия определения $\mathcal{T}$. Если $\upsilon(x_0) > 5$, то при $p = 1$ имеем $\beta_1 = \alpha$. Если $b \in \mathbb{I} \cup \{0\}$, то для $p = 1$ имеем $\beta_1 = \text{fr}((\alpha - x_0)/(bx_0 + 1 - \alpha))$, тогда $\beta_2 = \alpha$. Далее предполагаем, что $b \notin \mathbb{I} \cup \{0\}$ и $\upsilon(x_0) \leq 5$. Заметим, что $\upsilon(x_0) \in \{1, 2\}$. Достаточно рассмотреть только случаи $x_0 = 1$ и $x_0 = 1 + i$ (так как для любого x_0 таком, что $\upsilon(x_0) \in \{1, 2\}$ существует элемент $\varepsilon \in \mathbb{I}$ такой, что $x_0 = \varepsilon$ или $x_0 = (1 + i)\varepsilon$).

Пусть $x_0 = 1 + i$, тогда $b = -1 + i$. Положим $p = 1$, и получим

$$\beta_1 = \text{fr}((\alpha - (1 + i))/(\alpha(1 - i) - 1)),\ \beta_2 = \alpha^{-1}.$$

Пусть $x_0 = 1$, тогда $b \in \{-2, -1 \pm i, -2 \pm i\}$.

Если $b = -2$, то для $p = 1$ имеем

$$\beta_1 = \text{fr}((\alpha - 1)/(2\alpha - 1)),\ \beta_2 = \alpha^{-1}.$$

Если $b = -1 \pm i$, то для $p = 1$ имеем

$$\beta_1 = \text{fr}((\alpha - 1)/(\alpha(1 \mp i) \pm i)),\ \beta_2 = \alpha^{-1}.$$

Пусть $b = -2 + i$. Рассмотрим элемент

$$\beta = \omega(\text{fr}((\alpha - 1)^{-1})) = \text{fr}((\alpha - 1)/(\alpha(2 - i) - (1 - i))).$$

Заметим, что

$$\gamma = \text{int}((\alpha - 1)/(\alpha(2 - 1) - (1 - i))) \in \{1 + i, 1 + 2i, 2 + i, 2 + 2i\}.$$

Если $\gamma = 1 + i$, то

$$\beta = (1 - \alpha(2 + i))/(\alpha(2 - i) - (1 - i)).$$

Положим $p = 2$, тогда имеем

$$\beta_1 = \omega^{(2)}(\text{fr}((\alpha - 1)^{-1})) = \text{fr}((\alpha(2 - i) - (1 - i))/(1 - \alpha(2 + i))),$$
$$\beta_2 = \alpha/(1 - \alpha(2 + i)),$$
$$\beta_3 = \alpha^{-1}.$$

Если $\gamma = 1 + 2i$, то

$$\beta = ((2 + i) - \alpha(3 + 3i))/(\alpha(2 - i) - (1 - i)).$$

Положим $p = 2$, тогда имеем

$$\beta_1 = \omega^{(2)}(\text{fr}((\alpha - 1)^{-1})) = \text{fr}((\alpha(2 - i) - (1 - i))/((2 + i) - \alpha(3 + 3i))),$$
$$\beta_2 = \alpha/(1 - \alpha(2 + i)),$$
$$\beta_3 = \alpha^{-1}.$$

Если $\gamma = 2 + i$, то

$$\beta = ((2 - i) - 4\alpha)/(\alpha(2 - i) - (1 - i)).$$

Положим $p = 2$, тогда имеем

$$\beta_1 = \omega^{(2)}(\text{fr}((\alpha - 1)^{-1})) = \text{fr}((\alpha(2 - i) - (1 - i))/((2 - i) - 4\alpha)),$$
$$\beta_2 = \alpha/(1 - \alpha(2 + i)),$$
$$\beta_3 = \alpha^{-1}.$$

Если $\gamma = 2 + 2i$, то

$$\beta = (3 - \alpha(5 + 2i))/(\alpha(2 - i) - (1 - i)).$$

Положим $p = 3$, тогда имеем

$$\beta_1 = \omega^{(3)}(\text{fr}((\alpha - 1)^{-1})) = \text{fr}((3 - \alpha(5 + 2i))/(2 - 2i - \alpha(5 - 2i))),$$
$$\beta_2 = \alpha/(1 - \alpha(2_i),$$
$$\beta_3 = \alpha^{-1}.$$

Случай $b = -2 - i$ аналогичен случаю $b = -2 + i$.

Проверим второе условие определения множества $\mathcal{T}$. Рассмотрим произвольные $x_0 \in \mathbb{Z}[i] \setminus \{0\}$ и $\alpha \in \mathbb{F}_1^*$ такие, что $\omega(\text{fr}((\alpha - x_0)^{-1})) = 0$. Так как во всех случаях, кроме $x_0 = 1$, $b = -2 \pm i$, можно взять $D_{\mathbb{K}} = 2$ вместо $D_{\mathbb{K}} = 3$, то необходимо рассмотреть только случай $x_0 = 1$, $b = -2 \pm i$. Пусть $b = -2 + i$, тогда из условия $\omega(\text{fr}((\alpha - x_0)^{-1})) = 0$ следует, что $\alpha \in \{1/(2 + i),(2 + i)/(3 + 3i),(2 - i)/4,3/(5 + 2i)\}$. Для первого, второго и третьего элемента выполнено $\omega^{(2)}(\alpha) = 0$. Для четвертого элемента условие $\alpha = \text{fr}(\alpha)$ не выполняется. Случай $b = -2 - i$ аналогичен случаю $b = -2 + i$. Следовательно, $\mathbb{K} = \mathbb{Z}[i]$ не принадлежит классу $\mathcal{S}$, но принадлежит классу $\mathcal{T}$.

Покажем, что существует факториальное кольцо $\mathbb{K}$ такое, что $\mathbb{K} \notin \mathcal{T}$ и цепочка делений с выбором минимального по норме остатка не является кратчайшей.

Пример 2.10. Пусть $\mathbb{K} = \mathbb{Z}[\sqrt{-11}]$, где норма и дробная часть заданы соотношениями 2.6 и 2.7. Заметим, что множество

$$\{6, -2i\sqrt{11}, 6, -3 + i\sqrt{11}, -1 - i\sqrt{11}, 2, 0\}$$

образует цепочку делений с выбором минимального по норме остатка для пары $(a,b) = (6, -2i\sqrt{11})$. Тогда $\mathcal{L}_{a,b} = 5$. С другой стороны существует цепочка делений

$$\{6, -2i\sqrt{11}, -5 + i\sqrt{11}, 3 + i\sqrt{11}, 2, 0\},$$

из которой следует, что $\mathcal{l}_{a,b} \leq 4 \leq \mathcal{L}_{a,b}$. Следовательно, теорема 2.1 не выполняется. Предположим, что $\mathbb{Z}[i\sqrt{11}] \in \mathcal{T}$, но тогда по теореме 2.1 получаем, что для любой пары $(c,d) \in \mathbb{K}_* \times \mathbb{K}_*$ выполнено $\mathcal{l}_{c,d} = \mathcal{L}_{c,d}$. Получаем противоречие с приведенным примером. Аналогично можно показать, что лемма 2.1 не выполняется для $\mathbb{Z}[\sqrt{-11}]$.

Рассмотрим пример, показывающий, что условия теоремы 2.2 не могут быть упрощены.

Пример 2.11. Пусть $\mathbb{K} = \mathbb{P}[t]$ с нормой и дробной частью как в примере 2.5

Пусть n произвольное натуральное число. Определим последовательность

$$g_{k+2}(t) = tg_{k+1}(t) + g_k(t), k \geq 1, g_1(t) = 1, g_2(t) = t.$$

Заметим, что $\deg g_k = k - 1$. Пусть $a(t) = g_{n+1}(t), b(t) = g_n(t)$, тогда $\mathcal{L}_{a(t),b(t)} = n$. Из того, что $l_n(\mathbb{P}[t]) \leq n$ следует, что $l_n(\mathbb{P}[t]) = n$.

Для произвольного $n \in \mathbb{N}$ существует элемент $\alpha \in \mathbb{F}_1$, для которого $|\alpha| = n/(n+1)$. Следовательно, $\Lambda_{\mathbb{K}} \geq 1$. Так как $\mathbb{P}[t]$ евклидово, то по теореме 2.2 имеем $\Lambda_{\mathbb{K}} \leq 1$ и $l_n(\mathbb{P}[t]) \leq n$. Итого получаем, что $\Lambda_{\mathbb{K}} = 1$. Следовательно, условие $\Lambda_{\mathbb{K}} \in [0,1)$ в теореме 2.2 не может быть заменено условием $\Lambda_{\mathbb{K}} \in [0,1]$.

2.4 Теорема Кронекера-Валена в кольце алгебраических целых чисел числового поля

В этой части будет приведен метод вычисления наименьшего по норме остатка. Используя его, будет приведен общий метод доказательства

невыполнимости теоремы Кронекера-Валена в некотором фиксированном кольце K специального вида. Затем, используя полученный метод, покажем, что теорема Кронекера-Валена не выполняется во всех действительных квадратичных норменно-евклидовых кольцах.

Пусть $\mathbb{Z}_K$ – кольцо алгебраических целых чисел числового поля K. И пусть $(e_i)_{1\leq i\leq n}$ – базис $\mathbb{Z}_K$. Обозначим через r_1 количество действительных векторов, а через $2r_2$ количество вещественных. Тогда $n = r_1 + 2r_2$. Обозначим через $N_{K/\mathbb{Q}}$ обычную норму. Через $\mathbb{Z}_K^\times$ обозначим группу единиц K, а ее ранг $r = r_1+r_2-1$. Далее в этой части будем полагать, что $\mathbb{Z}_K$ евклидово по отношению к норме $N_{K/\mathbb{Q}}$.

Определение 2.13. Евклидовым минимумом $\xi \in K$ будем называть неотрицательное действительное число

$$m_K(\xi) = \inf_{z\in\mathbb{Z}_K} \left|N_{K/\mathbb{Q}}(\xi - z)\right|$$

Через $(\sigma_i)_{1\leq i\leq n}$ обозначим вложение K и $\mathbb{C}$. Предполагаем, что σ_i для $1 \leq i \leq r_1$ является действительным, а для $r_1 < i < r_1 + r_2$ мнимым и $\sigma_{i+r_2} = \overline{\sigma_i}$. Введем функцию $\Phi(x) : K \to \mathbb{R}^n$ следующим образом

$$\Phi(x) = (\sigma_1(x), \ldots, \sigma_{r_1}(x), \mathcal{R}\sigma_{r_1+1}(x), \ldots, \mathcal{R}\sigma_{r_1+r_2}(x), \mathcal{I}\sigma_{r_1+1}(x), \ldots, \mathcal{I}\sigma_{r_1+r_2}(x))$$

Удобнее вместо K использовать $\Phi(K)$ как в [23]. Для этого необходимо определить произведение в $\mathbb{R}^n$. Сделаем это через Φ: для $x = (x_i)_{1\leq i\leq n}$ и $y = (y_i)_{1\leq i\leq n}$ обозначим $xy = (\omega_i)_{1\leq i\leq n}$ где

$$\omega_i = \begin{cases} x_i y_i & \text{если } 1 \leq i \leq r_1, \\ x_i y_i - x_{i+r_2} y_{i+r_2} & \text{если } r_1 < i \leq r_1 + r_2, \\ x_{i-r_2} y_i - x_i y_{i-r_2} & \text{если } r_1 + r_2 < i \leq n. \end{cases}$$

Через H обозначим $\mathbb{R}^n$ вместе с произведением, определенным выше. Обозначим через $\mathcal{N} : H \to \mathbb{R}$ норму в H. По определению считаем, что

$$\mathcal{N} : x = (x_i)_{1\leq i\leq n} \longmapsto \prod_{i=1}^{r_1} x_i \prod_{i=r_1+1}^{r_1+r_2} (x_i^2 + x_{i+r_2}^2).$$

Заметим, что для любых $x, y \in H$ выполнено $\mathcal{N}(xy) = \mathcal{N}(x)\mathcal{N}(y)$. А так же для любых $\xi \in K$ выполнено $N_{K/\mathbb{Q}}(\xi) = \mathcal{N}(\Phi(\xi))$. Следовательно, H можно рассматривать как замыкание K относительно введенной нормы. Определим неоднородный минимум для $x \in H$.

Определение 2.14. Для $x \in H$ неоднородным минимумом будем называть неотрицательное число

$$m_{\overline{K}}(x) = \inf_{z\in\mathbb{Z}_K} |\mathcal{N}(x - \Phi(z))|.$$

Очевидно, что $m_K(\xi) = m_{\overline{K}}(\Phi(\xi))$ для любого $\xi \in K$.

Утверждение 2.1. *[23] Для любого $\varepsilon \in \mathcal{O}_K^{\times}$, $Z \in \Phi(\mathcal{O}_K)$ выполнено*

$$m_{\overline{K}}(\Phi(\varepsilon)x - Z) = m_{\overline{K}}(x).$$

Будем предполагать, что $r \geq 1$, т.е. группа $\mathcal{O}_K^{\times}$ бесконечна и образована r фундаментальными единицами и корнями единицы в K. Будем обозначать их через $\{\varepsilon_1, \ldots, \varepsilon_r\}$ и считать, что они известны. Обозначим ν – генератор корней из единицы в K порядка l.

Определим фундаментальную область $\mathcal{F}$ поля K как

$$\mathcal{F} = \left\{ \sum_{i=1}^{n} x_i \Phi(e_i) : x_i \in \mathbb{Q} \cap [0,1), e_i \in \{\varepsilon_1, \ldots, \varepsilon_r\} \right\}$$

Обозначим через $\mathrm{Orb}(x)$ орбиту элемента $x \in H$, т.е. множество элементов $\mathcal{F}$, полученных из x домножением на единицы и переведенных в фундаментальную область с помощью $\Phi(\mathcal{O}_K)$.

$$\mathrm{Orb}(x) = \left\{ \Phi(\varepsilon)x - z \in \mathcal{F} | \varepsilon \in \mathbb{Z}_K^{\times}, z \in \mathbb{Z}_K \right\}$$

Из утверждения 2.1 следует, что функция $m_{\overline{K}}$ принимает одно значение на всех элементах орбиты. Из [23] следует, что для любого элемента $x \in H$ орбита $\mathrm{Orb}(x)$ конечна тогда и только тогда, когда $x \in \Phi(K)$.

Пусть дана точка $\xi \in K$ и необходимо вычислить множество $\mathrm{Orb}(\Phi(\xi))$. Определим следующую операцию

$$x = \sum_{i=1}^{n} q_i e_i \longmapsto \overline{x} = \sum_{i=1}^{n} (q_i - \lfloor q_i \rfloor) e_i.$$

Обозначим

$$\mathcal{O}(\xi) = \{\overline{\varepsilon\xi} : \varepsilon \in \mathcal{O}_K^{\times}\}.$$

Для каждого $1 \leq i \leq r$ существует положительное число m такое, что $\overline{\varepsilon_i}^m \overline{\xi} = \overline{\xi}$. Обозначим l_i наименьшее такое число. Далее будем полагать, что l_i известны для K.

С этими обозначениями, из [23] следует, что

$$\mathcal{O}(\xi) = \left\{ \overline{\nu}^m \prod_{i=1}^{r} \overline{\varepsilon_i}^{m_i} \overline{\xi} : 0 \leq m < l, 0 \leq m_i < l_i, 1 \leq i \leq r \right\} \tag{2.8}$$

Получаем, что выполнено $\mathrm{Orb}(\Phi(\xi)) = \{\Phi(\zeta) : \zeta \in \mathcal{O}(\xi)\}$ для любого $\xi \in K$.

Определение 2.15. Для всех $1 \leq i \leq n$ обозначим

$$\Gamma_i = \prod_{j=1}^{r} \max\left\{|\sigma_i(\varepsilon_j)|, \frac{1}{|\sigma_i(\varepsilon_j)|}\right\}.$$

А так же определим

$$\Gamma(k) = \begin{cases} \left(\prod\limits_{j=1}^{n-1} \Gamma_j\right)^{\frac{1}{n}} k^{\frac{1}{n}} \text{ если } K \text{ действительное,} \\ \left(\prod\limits_{j=1}^{r_1} \Gamma_j \prod\limits_{j=1}^{r_1+r_2-1} \Gamma_j\Gamma_{j+r_2}\right)^{\frac{1}{n}} k^{\frac{1}{n}} \text{ иначе,} \end{cases}$$

где $k > 0$.

Далее будем полагать, что z_i, $i \in \{1, \ldots, n\}$, $z \in H$ обозначает i-ую координату элемента z в базисе $(e_i)_{1 \leq i \leq n}$.

Утверждение 2.2. *[23] Пусть $x \in \Phi(K)$ и $k > 0$. Для каждого $z \in Orb(x)$ обозначим*

$$\mathcal{I}_{z,k} = \{Z \in \Phi(\mathcal{O}_K) : |z_i - Z_i| \leq \Gamma(k) \forall i, 1 \leq i \leq n\},$$
$$\mathcal{M}_k = \min_{z \in Orb(x)} \min_{Z \in \mathcal{I}_{z,k}} |\mathcal{N}(z - Z)|. \tag{2.9}$$

Тогда, если $\mathcal{M}_k \leq k$, то $m_{\overline{K}}(x) = \mathcal{M}_k$.

Далее будем использовать определения деления с выбором минимального по норме остатка и цепочки делений. В этой части работы будем представлен алгоритм нахождения цепочки делений с выбором минимального по норме остатка для произвольных $a, b \in \mathcal{O}_K$, а так же приведена оценка его вычислительной трудоемкости. Заметим, что задача нахождения минимального по норме остатка при делении a на b эквивалентна задаче нахождения такого $q \in \mathcal{O}_K$, что $|\mathcal{N}(\Phi(a/b - q))|$. Для нахождения такого q будем использовать утверждение 2.2.

Определение 2.16. Для $x \in H$ обозначим через $x_{\mathbb{Z}} \in \mathcal{O}_K$ такой элемент, что

$$\inf_{z \in \mathcal{O}_K} |\mathcal{N}(x - \Phi(z))| = |\mathcal{N}(x - \Phi(x_{\mathbb{Z}}))|.$$

Утверждение 2.3. *Пусть $x \in \Phi(K)$ и $k > 0$. Для $z \in Orb(x)$ рассмотрим $\mathcal{I}_{z,k}$ и $\mathcal{M}_k$, определенные в утверждении 2.2. Предположим, что $\mathcal{M}_k \leq k$. Предположим, что $z' \in Orb(x)$ и $Z' \in \mathcal{I}_{z',k}$ такие элементы, что $\mathcal{M}_k = |\mathcal{N}(z' - Z')|$. Тогда можно вычислить $x_{\mathbb{Z}}$ за $O(1)$ арифметических операций в K.*

Доказательство. Из утверждения 2.2 следует, что

$$m_{\overline{K}}(x) = \mathcal{M}_k.$$

Используя определение $m_{\overline{K}}(x)$ и условие этого утверждения, получаем, что

$$\inf_{z \in \mathcal{O}_K} |\mathcal{N}(x - \Phi(z))| = |\mathcal{N}(z' - Z')|.$$

Из того, что $z' \in \mathrm{Orb}(x)$ следует, что существует $\varepsilon \in \mathcal{O}_K^\times$ такое, что $z' = \Phi(\varepsilon)x$. Предположим, что мы знаем такие m и m_i что $\varepsilon = \nu^m \prod_{i=1}^r \varepsilon_i^{m_i}$. Так как m и m_i ограничены l и l_i, то можно вычислить $\Phi(\varepsilon^{-1})$ за $O(1)$ арифметических операций. Так как $\mathcal{N}(x) = \mathcal{N}(\Phi(\varepsilon)x)$ для всех $x \in H$ и $\varepsilon \in \mathcal{O}_K^\times$ выполнено следующее равенство

$$\inf_{z \in \mathcal{O}_K} |(x - \Phi(z))| = |\mathcal{N}(x - Z'\Phi(\varepsilon^{-1}))|.$$

Таким образом, получаем, что $x_{\mathbb{Z}} = Z'\Phi(\varepsilon^{-1})$, где $z' = \Phi(\varepsilon)x$. $\otimes$

Замечание 2.3. Для произвольного $x \in \Phi(K)$ и $z \in \mathrm{Orb}(x)$ будем предполагать, что известно $\varepsilon_z \in \mathcal{O}_K^\times$ такое, что $z = \Phi(\overline{\varepsilon_z \Phi^{-1}(x)})$, и более того можно вычислить ε_z^{-1} за $O(1)$ арифметических операций.

Используя доказанные выше утверждения, получаем следующий алгоритм.

Алгоритм 2.2 Вычисление наименьшего по норме остатка

Дано: числовое поле K, два элемента $a, b \in \mathcal{O}_K$

Результат: наименьший общий остаток r при делении a на b

1: $x \in \Phi(K) \leftarrow \Phi(a/b)$
2: вычислить Orb(x), используя 2.8
3: выбрать произвольное действительное $k > 0$
4: вычислить $\Gamma(k)$
5: объявить переменные z' и Z', которые будут инициализированы позже
6: **for all** $z \in Orb(x)$ **do**
7: вычислить $\mathcal{I}_{z,k}$ используя 2.9
8: **for all** $Z \in \mathcal{I}_{z,k}$ **do**
9: **if** z' и Z' не инициализированы или $\mathcal{N}(z' - Z') > \mathcal{N}(z - Z)$ **then**
10: $z' \leftarrow z$
11: $Z' \leftarrow Z$
12: **end if**
13: **end for**
14: **end for**
15: $\mathcal{M}_k \leftarrow \mathcal{N}(z' - Z')$
16: **if** $\mathcal{M}_k > k$ **then**
17: $k \leftarrow \mathcal{M}_k$
18: перейти к шагу 4
19: **end if**
20: $x_{\mathbb{Z}} \leftarrow Z'\Phi(\varepsilon_z'^{-1})$
21: **return** $r = a - bx_{\mathbb{Z}}$

Оценим вычислительную сложность этого алгоритма.

Утверждение 2.4. *Для любых $a, b \in \mathcal{O}_K \setminus \{0\}$ наименьший по норме остаток r при делении a на b можно найти, используя алгоритм 2.4, за $O(1)$ арифметических операций в K.*

Доказательство. Из того, что

$$|\text{Orb}(x)| \leq l \prod_{i=1}^{r} l_i$$

следует, что множество Orb(x) можно найти за $O(1)$ арифметических операций в K. Так же мощность множества $\mathcal{I}_{z,k}$ ограничена некоторой константой, зависящей только от $\Gamma(k)$. Заметим, что $\Gamma(k)$ на зависит от a/b. Так как функция $k \to \mathcal{M}_k$ неубывающая, из Утверждения 2.2 следует, что цикл необходимо будет повторить не более двух раз. Таким образом, можно заключить, что наименьший по норме остаток при делении a на b можно найти за $O(1)$ арифметических операций в K. $\otimes$

В этой части работы будет представлен метод автоматического доказательства невыполнимости теоремы Кронекера-Валена в фиксированном поле K. Метод доказательства приведен в алгоритме 2.4.

Алгоритм 2.3 Общий метод доказательства невыполнимости теоремы Кронекера-Валена

1: взять произвольные $a, b \in \mathbb{Z}_K$
2: используя Алгоритм 2.4 вычислить цепочку делений с выбором минимального по норме остатка $\mathcal{D}_{a,b}$
3: найти $c \in \mathbb{Z}_K$ такое, что $a = bx + c$ для некоторого $x \in \mathbb{Z}_K$ (без ограничений на $N_{K/\mathbb{Q}}(c)$)
4: используя Алгоритм 2.4 вычислить цепочку делений с выбором минимального по норме остатка $\mathcal{D}'_{b,c}$
5: **if** $\text{len}(\mathcal{D}_{a,b}) > \text{len}(\mathcal{D}'_{b,c}) + 1$ **then**
6: теорема Кронекера-Валена не выполняется в K
7: **else**
8: неизвестно
9: **end if**

Применим этот метод в частном случае. Предположим, что K действительное квадратичное норменно-евклидово поле. В методе будем рассматривать такие целые элементы a и b, которые являются рациональными, т.е. $a, b \in \mathbb{Z}$. А так же будем искать c используя остаток при делении a на b на $\mathbb{Z}$. Модифицированный метод приведен в алгоритме 2.4.

Алгоритм 2.4 Специальный метод доказательства невыполнимости теоремы Кронекера-Валена

1: взять произвольные $a, b \in \mathbb{Z}$
2: используя Алгоритм 2.4 вычислить цепочку делений с выбором минимального по норме остатка $\mathcal{D}_{a,b}$
3: $c \leftarrow a\%b$
4: используя Алгоритм 2.4 вычислить цепочку делений с выбором минимального по норме остатка $\mathcal{D}'_{b,c}$
5: **if** $\text{len}(\mathcal{D}_{a,b}) > \text{len}(\mathcal{D}'_{b,c}) + 1$ **then**
6: теорема Кронекера-Валена не выполняется в K
7: **else**
8: неизвестно
9: **end if**
10: $c \leftarrow a\%b - b$
11: используя Алгоритм 2.4 вычислить цепочку делений с выбором минимального по норме остатка $\mathcal{D}''_{b,c}$
12: **if** $\text{len}(\mathcal{D}_{a,b}) > \text{len}(\mathcal{D}''_{b,c}) + 1$ **then**
13: теорема Кронекера-Валена не выполняется в K
14: **else**
15: неизвестно
16: **end if**

Реализуем этот алгоритм на R и применим его для всех действительных квадратичных норменно-евклидовых полей.

Теорема 2.3. *Пусть K действительное квадратичное норменно-евклидово поле. Тогда теорема Кронекера-Валена не выполняется в K.*

Доказательство. Известно, что существует ровно 16 полей $K = \mathbb{Q}(\sqrt{d})$, удовлетворяющих условиям теоремы, со значениями d из множества $\{2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73\}$. Приведем контрпримеры для всех $\mathbb{Q}(\sqrt{d})$.

$\mathcal{O}_{\mathbb{Q}[\sqrt{2}]}$. Цепочка делений с выбором минимального по норме остатка:

$$\{50, 29, -8, -11 - 8\sqrt{2}, -7 - 5\sqrt{2}, 0\}$$

Более короткая цепочка делений:

$$\{50, 29, 21, 19601 - 13860\sqrt{2}, 0\}$$

$\mathcal{O}_{\mathbb{Q}[\sqrt{3}]}$. Цепочка делений с выбором минимального по норме остатка:

$$\{52, 38, 14, 24 + 14\sqrt{3}, 14 + 8\sqrt{3}, 0\}$$

Более короткая цепочка делений:

$$\{52, 38, -24, 2702 - 1560\sqrt{3}, 0\}$$

$\mathcal{O}_{\mathbb{Q}[\sqrt{5}]}$. Цепочка делений с выбором минимального по норме остатка:

$$\{58, 39, 17101 - 10569\frac{1+\sqrt{5}}{2},$$
$$-1974 + 1220\frac{1+\sqrt{5}}{2}, -377 + 233\frac{1+\sqrt{5}}{2}, 0\}$$

Более короткая цепочка делений:

$$\{58, 39, 19, 1, 0\}$$

$\mathcal{O}_{\mathbb{Q}[\sqrt{6}]}$. Цепочка делений с выбором минимального по норме остатка:

$$\{50, 33, -2425 + 990\sqrt{6}, -9602 + 3920\sqrt{6}, -485 + 198\sqrt{6}, 0\}$$

Более короткая цепочка делений:

$$\{50, 33, 17, -1, 0\}$$

$\mathcal{O}_{\mathbb{Q}[\sqrt{7}]}$. Цепочка делений с выбором минимального по норме остатка:

$$\{50, 23, -5355 + 2024\sqrt{7}, -20830 + 7873\sqrt{7}, 2024 - 765\sqrt{7}, 0\}$$

Более короткая цепочка делений:

$$\{50, 23, 4, -1, 0\}$$

$\mathcal{O}_{\mathbb{Q}[\sqrt{11}]}$. Цепочка делений с выбором минимального по норме остатка:

$$\{50, 34, -902 + 272\sqrt{11}, -252 + 76\sqrt{11}, -398 + 120\sqrt{11}, 0\}$$

Более короткая цепочка делений:

$$\{50, 34, 16, 2, 0\}$$

$\mathcal{O}_{\mathbb{Q}[\sqrt{13}]}$. Цепочка делений с выбором минимального по норме остатка:

$$\{52, 19, -355666 + 154451\frac{1+\sqrt{13}}{2},$$
$$-128511 + 55807\frac{1+\sqrt{13}}{2}, -98644 + 42837\frac{1+\sqrt{13}}{2}, 0\}$$

Более короткая цепочка делений:

$$\{52, 19, -5, -1, 0\}$$

$\mathcal{O}_{\mathbb{Q}[\sqrt{17}]}$. Цепочка делений с выбором минимального по норме остатка:

$$\{51, 14, 11153 - 4354\frac{1+\sqrt{17}}{2},$$
$$3038 - 1186\frac{1+\sqrt{17}}{2}, 333 - 130\frac{1+\sqrt{17}}{2}, 0\}$$

Более короткая цепочка делений:

$$\{51, 14, -5, -1, 0\}$$

$\mathcal{O}_{\mathbb{Q}[\sqrt{19}]}$. Цепочка делений с выбором минимального по норме остатка:

$$\{70, 29, -6194 + 1421\sqrt{19}, 3012 - 691\sqrt{19}, -170 + 39\sqrt{19}, 0\}$$

Более короткая цепочка делений:

$$\{70, 29, 12, -57799 + 13260\sqrt{19}, 0\}$$

$\mathcal{O}_{\mathbb{Q}[\sqrt{21}]}$. Цепочка делений с выбором минимального по норме остатка:

$$\{50, 33, 36845 - 13200\frac{1+\sqrt{21}}{2},$$
$$14738 - 5280\frac{1+\sqrt{21}}{2}, 7369 - 2640\frac{1+\sqrt{21}}{2}, 0\}$$

Более короткая цепочка делений:

$$\{50, 33, 17, -1, 0\}$$

$\mathcal{O}_{\mathbb{Q}[\sqrt{29}]}$. Цепочка делений с выбором минимального по норме остатка:

$$\{54, 21, 201 - 63\frac{1+\sqrt{29}}{2}, 96 - 30\frac{1+\sqrt{29}}{2}, -9 + 3\frac{1+\sqrt{29}}{2}, 0\}$$

Более короткая цепочка делений:

$$\{54, 21, 12, -3, 0\}$$

$\mathcal{O}_{\mathbb{Q}[\sqrt{33}]}$. Цепочка делений с выбором минимального по норме остатка:

$$\{50, 27, 58999613 - 17495460\frac{1+\sqrt{33}}{2},$$
$$- 30811543 + 9136706\frac{1+\sqrt{33}}{2}, -2623473 + 777952\frac{1+\sqrt{33}}{2}, 0\}$$

Более короткая цепочка делений:

$$\{50, 27, -4, -1, 0\}$$

$\mathcal{O}_{\mathbb{Q}[\sqrt{37}]}$. Цепочка делений с выбором минимального по норме остатка:

$$\{51, 23, -2525 + 713\frac{1+\sqrt{37}}{2},$$
$$471 - 133\frac{1+\sqrt{37}}{2}, 1027 - 290\frac{1+\sqrt{37}}{2}, 0\}$$

Более короткая цепочка делений:

$$\{51, 23, 5, -1027 + 290\frac{1+\sqrt{37}}{2}, 0\}$$

$\mathcal{O}_{\mathbb{Q}[\sqrt{41}]}$. Цепочка делений с выбором минимального по норме остатка:

$$\{51, 33, -12093 + 3267\frac{1+\sqrt{41}}{2},$$
$$-47628 + 12867\frac{1+\sqrt{41}}{2}, 454959 - 122910\frac{1+\sqrt{41}}{2}, 0\}$$

Более короткая цепочка делений:

$$\{51, 33, 18, -3, 0\}$$

$\mathcal{O}_{\mathbb{Q}[\sqrt{57}]}$. Цепочка делений с выбором минимального по норме остатка:

$$\{51, 31, -11, -2, -1, 0\}$$

Более короткая цепочка делений:

$$\{51, 31, 20, 131 + 40\frac{1+\sqrt{57}}{2}, 0\}$$

$\mathcal{O}_{\mathbb{Q}[\sqrt{73}]}$. Цепочка делений с выбором минимального по норме остатка:

$$\{57, 32, -7, -580996 + 121751\frac{1+\sqrt{73}}{2},$$
$$2548249 - 534000\frac{1+\sqrt{73}}{2}, 0\}$$

Более короткая цепочка делений:

$$\{57, 32, 25, -943 - 250\frac{1+\sqrt{73}}{2}, 0\}$$

$\otimes$

Следствие 2.1. Пусть $K = \mathbb{Q}[\sqrt{d}]$ – квадратичное норменно-евклидово поле. Теорема Кронекера-Валена выполняется в K тогда и только тогда, когда $d = -1, -2, -3, -7$.

Доказательство. Если $d >= 0$, то утверждение следует из теоремы 2.3. Если $d < 0$, то утверждение следует из работы [30]. $\otimes$

2.5 Результаты

В данной главе исследована теорема Кронекера-Валена в абстрактных числовых кольцах. В результате работы, были получены следующие результаты:

1. Доказана теорема Кронекера-Валена в специальном классе факториальных колец.
2. Разработан алгоритм проверки достаточного условия принадлежности этому классу колец. Используя этот алгоритм, приведены примеры колец из найденного множества.
3. Разработан метод доказательства невыполнимости аналога теоремы Кронекера-Валена, применимый для произвольного конечного расширения рациональных чисел.
4. Используя упомянутый выше метод, доказано, что аналог теоремы Кронекера-Валена не выполняется во всех действительных норменно-евклидовых квадратичных кольцах. В совокупности с известными результатами это дает ответ о выполнимости теоремы Кронекера-Валена для всех квадратичных норменно-евклидовых кольцах.

ЗАКЛЮЧЕНИЕ

В работе был исследован аналог RSA-криптосистемы и алгоритм Евклида в абстрактных числовых кольцах. В результате работы, были получены следующие результаты:

1. Приведен аналог RSA-криптосистемы в абстрактных числовых кольцах. Ключевое отличие от классической криптосистемы состоит в том, что аналог использует идеалы кольца вместо элементов. Доказана теорема Винера о малой секретной экспоненте для упомянутого выше аналога RSA-криптосистемы. Так же доказан детерминированный аналог этой теоремы. Изучен метод взлома RSA-криптосистемы методом повторного шифрования. Доказана теорема, позволяющая защититься от этого типа атаки. Доказано, что в кольцах с единственной факторизацией задачи взлома RSA-криптосистемы и факторизации ее модуля эквивалентны. Указанный результат был получен в работе 4–А и изложен в главе 1.
2. Показано, что задача факторизации идеала к кольцах алгебраических целых элементов числового поля полиномиально сводится к задаче факторизации в целых числах. Сделан вывод о том, что использование аналога RSA-криптосистемы в числовых полях не дает выигрыша по сравнению с классической RSA-криптосистемой. Однако для нечисловых полей аналогичных результатов нет и их получение не является тривиальной задачей. Указанный результат изложен в главе 1.
3. Доказана теорема Кронекера-Валена в специальном классе абстрактных числовых колец. Разработан алгоритм проверки достаточного условия принадлежности этому классу колец. Используя представленный алгоритм, приведены примеры колец из найденного множества. Указанный результат был получен в работе 3–А и изложен в главе 2.
4. Разработан метод доказательства невыполнимости аналога теоремы Кронекера-Валена, применимый для произвольного конечного расширения рациональных чисел. Используя этот метод, доказано, что аналог теоремы Кронекера-Валена не выполняется во всех действительных норменно-евклидовых квадратичных кольцах. В совокупности с известными результатами это дает ответ о выполнимости теоремы Кронекера-Валена для всех квадратичных норменно-евклидовых кольцах. Указанный результат был получен в работе 1–А и изложен в главе 2.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. *Васьковский М.М.* Полиномиальная эквивалентность вычисления функции эйлера RSA-модуля и поиска секретного ключа в квадратичных евклидовых кольцах / М.М. Васьковский // Материалы международного научного конгресса по информатике: Информационные системы и технологии. — 2016. — С. 427-430.
2. *Agarwal S.* A New GCD Algorithm for Quadratic Number Rings with Unique Factorization / S. Agarwal, G.S. Frandsen. // LATIN 2006: Theoretical Infor matics. — 2006. — P. 30–42.
3. *Bach E.* Explicit bounds for primality testing and related problems / E. Bash. // Mathematics of Computation. — 1990. — P. 355–380.
4. *Brunyate A., Clark P.L.* Extending the Zolotarev-Frobenius approach to quadratic reciprocity / A. Brunyate, P.L. Clark // The Ramanujan Journal. — 2015. — V. 37. — P. 25-50.
5. *Cerri Jean-Paul.* Euclidean minima of totally real number fields: algorithmic determination // Mathematics of computation. — 2007. — V. 76. — P. 1547–1575.
6. *Cohen H.* A Course in Computational Algebraic Number Theory // Springer. — 1996.
7. *Cohen H.* Advanced topics in computational number theory // Springer. — 1999.
8. *Cooke G.E.* On the construction of division chains in algebraic number rings, with applications to sl2 / G.E.Cooke, P.L.Weinberger // Comm. Algebra. — 1975. — P.481–524.
9. *Coppersmith D.* Small solutions to polynomial equations, and low exponent rsa vulnerabilities / D. Coppersmith // J. Cryptology. — 1997. — V. 10. — P. 233–260.
10. *Coron J.S.* Deterministic polynomial-time equivalence of computing the rsa secret key and factoring / J.S. Coron, A. May. // J. Cryptology. — 2007. — V. 20. — P. 3950.
11. *Elkamchouchi H.* Extended RSA Cryptosystem and Digital Signature Schemes in the Domain of Gaussian Integers / H. Elkamchouchi, K. Elshenawy, H. Sha ban. // Proceedings of the 8th International conference on communication sys tems. — 2002. — P. 91–95.
12. *Gekke E.* Lectures on the Theory of Algebraic Numbers / E. Gekke. // GITTL. — 1940.
13. *Glukhov M.M.* Introduction to Number Theoretical Methods in Cryptography / M.M. Glukhov, I.A. Kruglov, A.B. Pichkur, A.V. Cheremushkin // Saint-Peters burg: Lan'. — 2011.

14. *El-Kassar A.N.* Modified RSA in the Domains of Gaussian Integers and Polynomials over Finite Fields / A.N. El-Kassar, R.A. Haraty, Y.A. Awad. // Proceedings of the ISCA 18th International conference on computer applications in industry and engineering. — 2005. — P. 298–303.
15. *Kaltofen E.* Arithmetic in quadratic fields with unique factorization / E. Kaltofen, H. Rolletschek. // EUROCAL '85 — 1985. — V. 204 — P. 279–288.
16. *Kannan R.* Polynomial Algorithms for Computing the Smith and Hermite Normal Forms of an Integer Matrix / R. Kannan, A. Bachem // SIAM Journal on Computing. — 1979. — P. 499–507.
17. *Koblitz N.* Course in Number Theory and Cryptography. / N. Koblitz // Springer-Verlag New York. — 1994.
18. *Darkey-Mensah M.K., Koprowski P.* Intrinsic factorization of ideals in dedekind domains / M.K. Darkey-Mensah, P. Koprowski // ACM Communications in Computer Algebra — 2019. — V. 53. — P. 107–109
19. *Derksen H., Kemper G.* Computational Invariant Theory / H. Derksen, G. Kemper // Encyclopaedia of Mathmatical Sciences. — 2010. — V. 130.
20. *Koval A.* Analysis of RSA over Gaussian Integers Algorithm / A. Koval, B. Verkhovsky. // 5th international conference on information technology: new generations. — 2008. — P. 101–105.
21. *Kranakis E.* Primality and Cryptography / E. Kranakis. // Teubner. — 1986.
22. *Lazard D.* Le meilleur algorithme d'Euclide pour $K[X]$ et Z / D. Lazard. // C. R. Acad. Sci. Paris Sér. A-B. — 1977. — V.284. — № 1. — P. A1–A4.
23. *Lezowski P.* Computation of the euclidean minimum of algebraic number fields / P. Lezowski. // Mathematics of Computation, American Mathematical Society 83. — 2014. — P.1397–1426.
24. *Li B.* Generalizations of RSA Public Key Cryptosystem. / B. Li. // IACR, Cryptology ePrint Arc. — 2005.
25. *Petukhova K.A.* RSA Cryptosystem for Dedekind Rings / K.A. Petukhova, S.N. Tronin // Lobachevskii Journal of Mathematics. — 2016. — V. 37. — P. 284–287.
26. *Pohst M.E.* Computational algebraic number theory / M.E. Pohst // Basel; Boston; Berlin: Birkhauser. — 1993.
27. *Rivest R.L.* A method for obtaining digital signatures and public-key cryptosystems / R.L. Rivest, A. Shamir, L. Adleman. // Communications of the ACM. — 1978. — V. 21. — P. 120–126.
28. *Rodosskii K.A.* Euclidean Algorithm. / K.A. Rodosskii. // Moscow: Nauka. — 1988.
29. *Rolletschek H.* On the number of divisions of the Euclidean algorithm applied to Gaussian integers / H. Rolletschek // J. Symbolic Comput. — 1986. — V. 2. — № 3. — P. 261–291.
30. *Rolletschek H.* Shortest division chains in imaginary quadratic number fields /

H. Rolletschek // J. Symbolic Comput. — 1990. — V. 9. — № 3. — P. 321–354.
31. *Selfridge J.L.* Euclidean Quadratic Fields / J.L. Selfridge, C.B. Lacampagne, R.B. Eggleton. // Amer. Math. Monthly. — 1992. — V. 99. — № 9. — P. 829–837.
32. *Vaskouski M.* Finite generalized continued fractions in euclidean domains / M. Vaskouski, N. Kondratyonok // Vestnik BSU. — 2013. — P. 117–123.
33. *Vaskouski M.* Shortest division chains in unique factorization domains / M. Vaskouski, N. Kondratyonok. // Journal of Symbolic Computation. — 2016. — V. 77. — P. 175–188.
34. *Vaskouski M.* Primes in quadratic unique factorization domains / M. Vaskouski, N. Kondratyonok, N. Prochorov. // Journal of number theory. — 2016. — V. 168. — P. 101–116.
35. *Wiener M.J.* Cryptanalysis of short RSA secret exponents / M.J. Wiener. // IEEE Trans. Inform. Theory. — 1990. — V. 36. — P. 553–558.
36. *Weinberger P.J.* On euclidean rings of algebraic integers / P.J. Weinberger // Proc. Sympos. Pure Math. — 1973. — V. 24. — P. 321-332.

Список публикаций автора по теме

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

8–А. Васьковский М.М. Построение и анализ RSA-криптосистемы в числовых полях / М.М. Васьковский, Н.В. Кондратёнок // ”Всероссийская конференция ”Алгебра и теория алгоритмов”, посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета” — г. Иваново, 21-24 марта 2018 г.

9–А. Васьковский М.М. Тест Соловея-Штрассена в квадратичных евклидовых кольцах / М.М. Васьковский, Н.В. Кондратёнок, Н.П. Прохоров // Материалы международной научной конференции ”XII Белорусская математическая конференция” — Сентябрь 5-10, 2016. — Часть 5. — С. 15-16

10–А. Кондратёнок Н.В. Критерии простоты в квадратичных кольцах с единственной факторизацией / Н.В. Кондратёнок, Н.П. Прохоров // Сборник статей лауреатов и авторов научных работ, получивших первую категорию XXIV Республиканского конкурса научных работ студентов. — 2017. — С. 19-20.

11–А. Кондратёнок Н.В. Цепные дроби в евклидовых кольцах / Н.В. Кондратёнок, М.М. Васьковский // Материалы XVI Республиканской научной конференции студентов и аспирантов — Март 25-27, 2013. — Часть 1. — С. 63-64.

ПРИЛОЖЕНИЕ А

Приведем реализацию, изложенного в работе метода на языке R. Для начала приведем вспомогательные функции, реализующие арифметику в квадратичном кольце.

```
library(data.table)

Sum <- function(x, y){
  res<-list()
  res[["a"]]<-x[["a"]]+y[["a"]]
  res[["b"]]<-x[["b"]]+y[["b"]]
  res[["theta"]]<-x[["theta"]]
  return(res)
}

Prod <- function(x, y){
  res<-list()
  if (x[["theta"]] %% 4 != 1) {
  res[["a"]]<-x[["a"]]*y[["a"]]+x[["b"]]*y[["b"]]*x[["theta"]]
    res[["b"]]<-x[["a"]]*y[["b"]]+x[["b"]]*y[["a"]]
  } else {
    res[["a"]]<-x[["a"]]*y[["a"]]+x[["b"]]*y[["b"]]*(x[["theta"
       ]]-1)/4
    res[["b"]]<-x[["a"]]*y[["b"]]+x[["b"]]*y[["a"]]+x[["b"]]*y[["b"
       ]]
  }
  res[["theta"]]<-x[["theta"]]
  return(res)
}

IsEqual <- function(x, y){
  eps<-10^{-6}
  return(as.logical(abs(x[["a"]]-y[["a"]])<eps & abs(x[["b"]]-y[["b
     "]])<eps & x[["theta"]]==y[["theta"]]))
}

IsEquiv <- function(x, y, m){ # m is rational integer
  res<-Sum(x, Inverse(y))
  res[["a"]]<-round(res[["a"]])
  res[["b"]]<-round(res[["b"]])
  return(as.logical(res[["a"]]%%m==0 & res[["b"]]%%m==0))
}

Norm <- function(x){
  if (x[["theta"]] %% 4 != 1) {
    return(
```

```
      x[["a"]]*x[["a"]]+x[["b"]]*x[["b"]]*(-x[["theta"]])
    )
  } else {
    return(
      ((2*x[["a"]]+x[["b"]])*(2*x[["a"]]+x[["b"]])+x[["b"]]*x[["b"
        ]]*(-x[["theta"]]))/4
    )
  }
}

NormIdeal <- function(x){
  return(abs(Norm(x)))
}

GetAdjoint <- function(x){
  if (x[["theta"]] %% 4 != 1) {
    res<-x
    res[["b"]]<--res[["b"]]
    return(res)
  } else {
    res<-x
    res[["a"]]<-res[["a"]]+res[["b"]]
    res[["b"]]<--res[["b"]]
    return(res)
  }
}

Div <- function(x, y){
  res<-Prod(x, GetAdjoint(y))
  res[["a"]]<-res[["a"]]/Norm(y)
  res[["b"]]<-res[["b"]]/Norm(y)
  return(res)
}

Unit <- function(theta){
  res<-list()
  if (theta==2){
    res[["a"]]<-1
    res[["b"]]<-1
    res[["theta"]]<-theta
  } else if (theta==3) {
    res[["a"]]<-2
    res[["b"]]<-1
    res[["theta"]]<-theta
  } else if (theta==5) {
    res[["a"]]<-0
    res[["b"]]<-1
    res[["theta"]]<-theta
  } else if (theta==6) {
    res[["a"]]<-5
```

```
    res[["b"]]<-2
    res[["theta"]]<-theta
  } else if (theta==7) {
    res[["a"]]<-8
    res[["b"]]<-3
    res[["theta"]]<-theta
  } else if (theta==11) {
    res[["a"]]<-10
    res[["b"]]<-3
    res[["theta"]]<-theta
  } else if (theta==13) {
    res[["a"]]<-1
    res[["b"]]<-1
    res[["theta"]]<-theta
  } else if (theta==17) {
    res[["a"]]<-3
    res[["b"]]<-2
    res[["theta"]]<-theta
  } else if (theta==19) {
    res[["a"]]<-170
    res[["b"]]<-39
    res[["theta"]]<-theta
  } else if (theta==21) {
    res[["a"]]<-2
    res[["b"]]<-1
    res[["theta"]]<-theta
  } else if (theta==29) {
    res[["a"]]<-2
    res[["b"]]<-1
    res[["theta"]]<-theta
  } else if (theta==33) {
    res[["a"]]<-19
    res[["b"]]<-8
    res[["theta"]]<-theta
  } else if (theta==37) {
    res[["a"]]<-5
    res[["b"]]<-2
    res[["theta"]]<-theta
  } else if (theta==41) {
    res[["a"]]<-27
    res[["b"]]<-10
    res[["theta"]]<-theta
  } else if (theta==57) {
    res[["a"]]<-131
    res[["b"]]<-40
    res[["theta"]]<-theta
  } else if (theta==73) {
    res[["a"]]<-943
    res[["b"]]<-250
    res[["theta"]]<-theta
```

```
138   }
139   return(res)
140 }
141 
142 IntUnit <-function(theta){
143   res<-list()
144   res[["a"]]<-1
145   res[["b"]]<-0
146   res[["theta"]]<-theta
147   return(res)
148 }
149 
150 NegIntUnit <-function(theta){
151   res<-list()
152   res[["a"]]<--1
153   res[["b"]]<-0
154   res[["theta"]]<-theta
155   return(res)
156 }
157 
158 Inverse <- function(x){
159   res<-list()
160   res[["a"]]<--x[["a"]]
161   res[["b"]]<--x[["b"]]
162   res[["theta"]]<-x[["theta"]]
163   return(res)
164 }
165 
166 FractionalPartRational <- function(x, y){
167   res<-list()
168   res[["a"]]<-x[["a"]]-floor(x[["a"]]/y)*y
169   res[["b"]]<-x[["b"]]-floor(x[["b"]]/y)*y
170   res[["theta"]]<-x[["theta"]]
171   return(list(x=res, y=y))
172 }
173 
174 Abs <- function(x){
175   if (x[["theta"]] %% 4 != 1) {
176     return(abs(x[["a"]]+x[["b"]]*sqrt(x[["theta"]])))
177   } else {
178     return(abs(x[["a"]]+x[["b"]]*(1+sqrt(x[["theta"]]))/2))
179   }
180 }
181 
182 GammaConst <- function(theta){
183   return(max(Abs(Unit(theta)), 1/Abs(Unit(theta))))
184 }
185 
186 Round <- function(a){
187   res<-list()
```

```
  res[["a"]]<-round(a[["a"]])
  res[["b"]]<-round(a[["b"]])
  res[["theta"]]<-round(a[["theta"]])
  return(res)
}
```

Теперь рассмотрим части представленного метода. Функция "GetOrbit" реализует алгоритм нахождения орбиты элемента a/b. Она принимает a и b и возвращает список элементов орбиты.

```
GetOrbit <- function(a, b){
  base.unit<-Unit(a[["theta"]])
  norm.b<-Norm(b)
  initial.frac.part<-FractionalPartRational(Prod(a, GetAdjoint(b)),
      norm.b)
  curr.iteration<-initial.frac.part[["x"]]
  curr.degree<-0

  orbit.a<-curr.iteration[["a"]]
  orbit.b<-curr.iteration[["b"]]
  orbit.sign<-1
  orbit.degree<-curr.degree

  while (!IsEquiv(x=initial.frac.part[["x"]],
                  y=FractionalPartRational(Prod(curr.iteration,
                     base.unit), norm.b)[["x"]],
                  m=norm.b)){
    curr.iteration<-FractionalPartRational(Prod(curr.iteration,
       base.unit), norm.b)[["x"]]
    curr.degree<-curr.degree + 1
    orbit.a<-c(orbit.a, curr.iteration[["a"]])
    orbit.b<-c(orbit.b, curr.iteration[["b"]])
    orbit.sign<-c(orbit.sign, 1)
    orbit.degree<-c(orbit.degree, curr.degree)
  }

  base.neg_unit<-Prod(Unit(a[["theta"]]), NegIntUnit(a[["theta"]]))
  initial.frac.part<-FractionalPartRational(Prod(a, GetAdjoint(b)),
      norm.b)
  curr.iteration<-initial.frac.part[["x"]]
  curr.degree<-0

  orbit.a<-c(orbit.a, curr.iteration[["a"]])
  orbit.b<-c(orbit.b, curr.iteration[["b"]])
  orbit.sign<-c(orbit.sign, -1)
  orbit.degree<-c(orbit.degree, curr.degree)

  while (!IsEquiv(x=initial.frac.part[["x"]],
                  y=FractionalPartRational(Prod(curr.iteration,
                     base.neg_unit), norm.b)[["x"]],
```

```
                    m=norm.b)){
    curr.iteration<-FractionalPartRational(Prod(curr.iteration,
       base.neg_unit), norm.b)[["x"]]
    curr.degree<-curr.degree + 1
    orbit.a<-c(orbit.a, curr.iteration[["a"]])
    orbit.b<-c(orbit.b, curr.iteration[["b"]])
    orbit.sign<-c(orbit.sign, -1)
    orbit.degree<-c(orbit.degree, curr.degree)
  }
  orbit.a<-orbit.a/norm.b
  orbit.b<-orbit.b/norm.b

  df.res<-data.frame(a=c(orbit.a), b=c(orbit.b), theta=a[["theta"
     ]], sign=c(orbit.sign), degree=c(orbit.degree))
  return(df.res)
}
```

Функция ”Dist” находит минимальное расстояние между данной точкой и точками на некоторой ограниченной сетке.

```
Dist <- function(x.a, x.b, x.theta, lower.a, upper.a, lower.b,
   upper.b){
  df.value<-expand.grid(a=seq(from=lower.a, to=upper.a, by=1),
          b=seq(from=lower.b, to=upper.b, by=1))

  x<-list()
  x[["a"]]<-x.a
  x[["b"]]<-x.b
  x[["theta"]]<-x.theta

  y<-list()
  y[["a"]]<-df.value$a
  y[["b"]]<-df.value$b
  y[["theta"]]<-x.theta

  df.value$dist<-NormIdeal(Sum(x, Inverse(y)))
  df.value<-df.value[df.value$dist==min(df.value$dist),]
  return(list(nearest.a=df.value$a[1], nearest.b=df.value$b[1],
     dist=df.value$dist[1]))
}
```

Функция ”FindNearest” вычисляет множество $\mathcal{I}_{z,k}$ для каждого элемента орбиты и находит элементы, дающие минимальное расстояние.

```
FindNearest <- function(a, b){
  eps<-10^{-6}
  orbit.a<-GetOrbit(a, b)
  max.dist<-sqrt(GammaConst(theta=a[["theta"]]))
  if (a[["theta"]] %% 4 != 1) {
    orbit.a$x<-orbit.a$a+sqrt(a[["theta"]])*orbit.a$b
    orbit.a$y<-orbit.a$a-sqrt(a[["theta"]])*orbit.a$b
  } else {
```

```
    orbit.a$x<-orbit.a$a+(1+sqrt(a[["theta"]]))*orbit.a$b/2
    orbit.a$y<-orbit.a$a+(1-sqrt(a[["theta"]]))*orbit.a$b/2
  }

  orbit.a$lower.x<-orbit.a$x-max.dist
  orbit.a$upper.x<-orbit.a$x+max.dist
  orbit.a$lower.y<-orbit.a$y-max.dist
  orbit.a$upper.y<-orbit.a$y+max.dist

  if (a[["theta"]] %% 4 != 1) {
    orbit.a$lower.a<-ceiling((orbit.a$lower.x+orbit.a$lower.y)/2)
    orbit.a$upper.a<-floor((orbit.a$upper.x+orbit.a$upper.y)/2)
    orbit.a$lower.b<-ceiling((orbit.a$lower.x-orbit.a$upper.y)/2/
       sqrt(a[["theta"]]))
    orbit.a$upper.b<-floor((orbit.a$upper.x-orbit.a$lower.y)/2/sqrt
       (a[["theta"]]))
  } else {
    orbit.a$lower.a<-ceiling(
      (orbit.a$lower.x+orbit.a$lower.y - (orbit.a$lower.x-orbit.a$
         lower.y)/sqrt(a[["theta"]]))/2)
    orbit.a$upper.a<-floor(
      (orbit.a$upper.x+orbit.a$upper.y - (orbit.a$upper.x-orbit.a$
         upper.y)/sqrt(a[["theta"]]))/2)
    orbit.a$lower.b<-ceiling((orbit.a$lower.x-orbit.a$upper.y)/sqrt
       (a[["theta"]]))
    orbit.a$upper.b<-floor((orbit.a$upper.x-orbit.a$lower.y)/sqrt(a
       [["theta"]]))
  }
  FindNearestOne <- function(x){
    Z<-Dist(x.a=orbit.a$a[x], x.b=orbit.a$b[x], x.theta=a[["theta"
       ]],
            lower.a=orbit.a$lower.a[x], upper.a=orbit.a$upper.a[x],
            lower.b=orbit.a$lower.b[x], upper.b=orbit.a$upper.b[x])
    return(Z)
  }

  QQ<-lapply(c(1:length(orbit.a[,1])), FUN=FindNearestOne)
  QQ<-rbindlist(QQ)
  orbit.a<-cbind(orbit.a, QQ)

  orbit.a<-orbit.a[orbit.a$dist<min(orbit.a$dist)+eps,]
  orbit.a<-orbit.a[orbit.a$degree==min(orbit.a$degree),]

  z<-list()
  z[["a"]]<-orbit.a$a[1]
  z[["b"]]<-orbit.a$b[1]
  z[["theta"]]<-a[["theta"]]

  Z<-list()
  Z[["a"]]<-orbit.a$nearest.a[1]
```

```
  Z[["b"]]<-orbit.a$nearest.b[1]
  Z[["theta"]]<-a[["theta"]]

  n<-orbit.a$degree[1]
  sgn<-orbit.a$sign[1]
  nearest.dist<-orbit.a$dist[1]

  return(list(z=z, Z=Z, nearest.dist=nearest.dist, n=n, sgn=sgn))
}
```

Функция ”DivMod” реализует алгоритм деления с выбором минимального по норме остатка.

```
DivMod <- function(a, b){
  base.unit<-Unit(a[["theta"]])
  a.b<-Div(a, b)
  res<-FindNearest(a=a, b=b)
  diff.Z<-Sum(res[["Z"]], Inverse(res[["z"]]))
  n.abs<-abs(res[["n"]])
  for (i in 1:n.abs){
    if (n.abs>0){
      if (res[["n"]]<0){
        diff.Z<-Prod(diff.Z, base.unit)
      }else{
        diff.Z<-Div(diff.Z, base.unit)
      }
    }
  }
  if (res[["sgn"]]==-1){
    diff.Z<-Inverse(diff.Z)
  }
  q<-Round(Sum(a.b, diff.Z))
  r<-Sum(a, Inverse(Prod(b, q)))
  return(list(q=q, r=r))
}
```

Функция ”Euclidean” реализует алгоритм нахождения цепочки делений с выбором минимального по норме остатка.

```
Euclidean <- function(a, b){
  res<-list()
  eps<-10^{-6}
  Z<-DivMod(a,b)
  steps<-1
  a.new<-b
  b.new<-Z[["r"]]
  res[["1"]]<-a
  res[["2"]]<-b
  res[["3"]]<-b.new
  while (NormIdeal(b.new)>eps){
    Z<-DivMod(a.new, b.new)
    a.new<-b.new
```

```
    b.new<-Z[["r"]]
    steps<-steps+1
    res[[as.character(steps+2)]]<-b.new
  }
  res<-rbindlist(res)
  return(list(steps=steps, res=res))
}
```

Далее приведен пример кода, использующий функции выше. Он перебирает различные целые числа и пытается найти такие, которые нужны методу.

```
global_theta<-19
found = FALSE

a<-list()
a[["a"]]<-70
a[["b"]]<-0
a[["theta"]]<-global_theta

b<-list()
b[["a"]]<-29
b[["b"]]<-0
b[["theta"]]<-global_theta

Z<-Euclidean(a=a, b=b)

c<-list()
c[["a"]]<-b[["a"]]
c[["b"]]<-0
c[["theta"]]<-global_theta

d<-list()
d[["a"]]<-a[["a"]] %% b[["a"]]
d[["b"]]<-0
d[["theta"]]<-global_theta

Z1<-Euclidean(a=c, b=d)

e<-list()
e[["a"]]<-b[["a"]]
e[["b"]]<-0
e[["theta"]]<-global_theta

f<-list()
f[["a"]]<-a[["a"]] %% b[["a"]] - b[["a"]]
f[["b"]]<-0
f[["theta"]]<-global_theta

Z2<-Euclidean(a=e, b=f)
```

```
39
40 print(c("z z1", Z[["steps"]], Z1[["steps"]]))
41 if (Z[["steps"]] - Z1[["steps"]] > 1) {
42     print("found")
43     print(Z)
44     print(Z1)
45 }
46
47 print(c("z z2", Z[["steps"]], Z2[["steps"]]))
48 if (Z[["steps"]] - Z2[["steps"]] > 1) {
49     print("found")
50     print(Z)
51     print(Z2)
52 }
```