МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ФАКУЛЬТЕТ ПРИКЛАДНОЙ МАТЕМАТИКИ И ИНФОРМАТИКИ

Кафедра дискретной математики и алгоритмики

ПРОХОРОВ
Николай Петрович

ПОЛИНОМИАЛЬНЫЕ АЛГОРИТМЫ ТЕСТИРОВАНИЯ ПРОСТОТЫ В АЛГЕБРАИЧЕСКИХ ЧИСЛОВЫХ ПОЛЯХ

Дипломная работа

Научный руководитель:
кандидат физ.-мат. наук,
доцент М.М. Васьковский

Допущена к защите
”____” _____ 2019 г.
Зав. кафедрой дискретной математики и алгоритмики
доктор физ.-мат. наук, профессор В.М. Котов

Минск, 2019

ОГЛАВЛЕНИЕ

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Работа, страницы: 60, главы: 4, источники: 32.

ДЕДЕКИНДОВО КОЛЬЦО, АБСТРАКТНОЕ ЧИСЛОВОЕ КОЛЬЦО, ИДЕАЛ, ПРОСТОЙ ИДЕАЛ, АЛГОРИТМ ТЕСТИРОВАНИЯ НА ПРОСТОТУ, ВЕРОЯТНОСТНЫЙ ТЕСТ, ДЕТЕРМИНИРОВАННЫЙ ТЕСТ, КОЛЬЦО ЦЕЛЫХ АЛГЕБРАИЧЕСКИХ ЭЛЕМЕНТОВ КОНЕЧНОГО РАСШИРЕНИЯ, КООРДИНАТНОЕ КОЛЬЦО, ПРЕДСТАВЛЕНИЕ ИДЕАЛА

Объект исследования — идеалы абстрактных числовых колец, критерии простоты идеалов абстрактных числовых колец, операции и тестирование на простоту над идеалами колец целых алгебраических элементов конечных расширений поля $\mathbb{Q}$ и координатных колец несингулярных кривых.

Метод исследования — методы алгоритмической и алгебраической теории чисел, коммутативной и линейной алгебры.

Цель работы — получение критериев простоты в абстрактных числовых кольцах, исследование и построение алгоритмов тестирования на простоту в кольцах целых алгебраических элементов конечных расширений поля $\mathbb{Q}$ и координатных кольцах несингулярных кривых.

Результат работы — доказаны аналоги критериев Миллера и Эйлера в абстрактных числовых кольцах, исследован вероятностный аналог теста Миллера-Рабина в произвольных абстрактных числовых кольцах, а также в более конкретных случаях – кольцах целых алгебраических элементов конечных расширений поля $\mathbb{Q}$ и координатных кольцах несингулярных кривых. Также построен детерминированный полиномиальный аналог теста Миллера-Рабина в случае факториального кольца целых алгебраических элементов и предположении выполнимости расширенной гипотезы Римана.

АГУЛЬНАЯ ХАРАКТАРЫСТЫКА ПРАЦЫ

Праца, старонкі: 60, часткі: 4, крыніцы: 32.

ДЭДЭКІНДАВА КАЛЬЦО, АБСТРАКТНАЕ ЛІКАВАЕ КАЛЬЦО, ІДЭАЛ, ПРОСТЫ ІДЭАЛ, АЛГАРЫТМ ТЭСЦІРАВАННЯ НА ПРАСТАТУ, ІМАВЕРТНАСНЫ ТЭСТ, ДЭТЭРМІНАВАНЫ ТЭСТ, КАЛЬЦО ЦЕЛЫХ АЛГЕБРАІЧНЫХ ЭЛЕМЕНТАЎ КАНЧАТКОВАГА ПАШЫРЭННЯ, КААРДЫНАТНАЕ КАЛЬЦО, ПРАДСТАЎЛЕННЕ ІДЭАЛА.

Аб'ект даследавання — ідэалы абстрактных лікавых калец, крытэрыі прастаты ідэалаў абстрактных лікавых калец, аперацыш і тэсціраванне на прастату над ідэаламі калец цэлых алгебраічных элементаў канчатковых пашырэнняў поля $\mathbb{Q}$ і каардынатных калец несінгулярных крывых.

Метад даследавання — метады алгебраічнай і алгарытмічнай тэорыі лікаў, каммутатыўнай і лінейная алгебры.

Мэта працы — атрыманне крытэрыяў прастаты ў абстрактных лікавых кольцах, даследванне і збудаванне алгарытмаў тэсціравання на прастату ў кольцах цэлых алгебраічных элементаў канчатковых пашырэнняў поля $\mathbb{Q}$ і каардынатных калец несінгулярных крывых.

Вынік працы — даказаны аналагі крытэрыяў Міллера і Эйлера ў абстрактных лікавых кольцах, даследван імавертнастны аналаг теста Міллера-Рабіна ў адвольных абстактных лікавых кольцах, а таксама ў больш дакладных выпадках – кольцах цэлых алгебраічных элементаў канчатковых пашырэнняў $\mathbb{Q}$ і каардынатных кольцах несінгулярных крывых. Таксама збудаваны дэтэрмініраваны палінаміальны аналаг тесту Міллера-Рабіна ў выпадку фактарыяльнага кальца цэлых алгебраічных элементаў і меркавання аб выкананасці пашыраннай гіпотэзы Рымана.

GENERAL CHARACTERISTICS OF WORK

Paper, pages: 60, chapters: 4 sources: 32.

DEDKIND DOMAIN, ABSTRACT NUMBER RING, IDEAL, PRIME IDEAL, ALGORITHM FOR PRIMALITY TESTING, DETERMINISTIC TEST, RING OF INTEGER ALGEBRAIC ELEMENTS OF FINITE EXTENSION, COORDINATE RING, REPRESENTATION OF IDEAL.

Object of study — ideals of abstract number rings, criteria for primality of ideals in abstract number rings, operations and primality testing for ideals in rings of integer algebraic elements of final extensions of field $\mathbb{Q}$ and coordinate rings of nonsingular curves.

Method of study — methods of algebraic and algorithmic number theory, commutative and linear algebra.

Purpose of the work — obtaining primality criteria in abstract number rings, investigating and constructing primality testing algorithms in rings of integer algebraic elements of finite extensions of field $\mathbb{Q}$ and coordinate rings of nonsingular curves.

Result of the work — analogues of Miller and Euler criteria were proved in abstract number rings, probabilistic analogue of Miller-Rabin test in arbitrary abstract number ring was investigated, also, it was investigated in more concrete cases – rings of integer algebraic elements of finite extensions of field $\mathbb{Q}$ and coordinate rings of nonsingular curves. Also, deterministic polynomial analog of Miller-Rabin test was constructed in case of factorial ring of integer algebraic elements and assumption that Extended Riemann Hypothesis holds.

ВВЕДЕНИЕ

Со второй половины XX века алгоритмическая теория чисел начинает активно развивается, что, в частности, было связано с развитием информатики и криптографии, а также приложениями теории чисел в указанных сферах. Был получен ряд существенных результатов связанных со свойствами целых простых чисел, критериями простоты и алгоритмами проверки чисел на простоту.

В 1976 году Г. Миллером[1] был предложен критерий и построен первый полиномиальный алгоритм тестирования чисел на простоту в предположении верности расширенной гипотезы Римана. Несколько позже алгоритм был модифицирован Эриком Бахом[3]. Наконец, в 1980 году М. Рабин[2] на основе критерия Миллера предложил полиномиальный вероятностный алгоритм тестирования чисел на простоту, который в настоящее время является самым эффективным вероятностным безусловным алгоритмом тестирования на простоту, который позволяет определять с вероятностью близкой к 1 при достаточном числе итераций является ли число простым. Также существует ряд других алгоритмов проверки на простоту, например тест Соловея-Штрассена[4], тест Адельмана-Померанса-Румели[5], который является одним из наиболее эффективных детерминированных алгоритмов проверки на простоту. В 2002 году было конструктивно доказано[6], что задача проверки на простоту принадлежит классу $\mathcal{P}$. Данные результаты представляют большой интерес как с теоретической точки зрения, так и с практической: при генерации ключей ряда криптосистем(например RSA, Рабина) требуется уметь быстро решать задачи проверки числа на простоту.

В частях 1-4 настоящей работы рассматриваются вопросы о построении критериев простоты и алгоритмов проверки на простоту в абстрактных числовых кольцах. Целями текущей работы являются доказательство критериев простоты идеалов абстрактных числовых колец, исследование и построение алгоритмов тестирования на простоту в кольцах целых алгебраических элементов конечных расширений поля $\mathbb{Q}$ и координатных колец несингулярных кривых.

Вопросы о простых идеалах различных ранее рассматривались в ряде работ. Например, в [7] приводится необходимое и достаточное условие простоты, в [16] были построены критерии простоты, а в [19] алгоритмы проверки

на простоту в квадратичных факториальных кольцах, в статье [20] был построен полиномиальный алгоритм проверки идеалов на простоту основанный на AKS. В статьях [17], [18] были исследованы свойства аналогов чисел Кармайкла в кольцах целых.

Важным классом колец, которые обобщают свойства колец целых чисел, являются кольца числовые абстрактные кольца, которые возникают, в ряде областей математике, например алгебре, теории чисел и алгебраической геометрии.

В первой главе рассматриваются и вводятся необходимые понятия и определения, ряд вспомогательных утверждений, формулируется постановка задачи. В частности, формулируется понятие идеалов, их свойств, дедекиндовых и абстрактных числовых колец, приводятся их основные примеры.

Во второй главе доказываются аналоги критериев Миллера и Эйлера в абстрактных числовых кольцах, а также исследуется применимость вероятностного аналога теста Миллера-Рабина в произвольных абстрактных числовых кольцах, приводится оценка вероятности успеха.

В третьей главе нами был исследован аналог теста Миллера-Рабина в кольцах целых алгебраических элементов конечных расширений поля $\mathbb{Q}$. Для этого были изучены способы представления идеалов в указанных кольцах, арифметические и модулярные операции. Далее были получены усиленные аналоги критериев Эйлера и Миллера в предположении выполнимости расширенной гипотезы Римана, на основе них был построен детерминированный аналог теста Миллера.

В четвёртой главе был исследован аналог теста Миллера-Рабина в координатных кольцах несингулярных кривых. Сначала он был построен для частого случая координатного кольца – кольца многочленов от одной переменной. Далее были исследованы приложения базиса Грёбнера для выполнения операций необходимых для тестирования идеалов в координатных кольцах на простоту.

Одним из основных преимуществ полученных результатов является их универсальность, так как критерии простоты были получены для произвольных абстрактных числовых колец, тесты также могут быть прменены для широкого набора колец. Также стоит отметить, хорошие показатели теоретической сложности и вероятности успехов полученных алгоритмов.

Отметим, что данные результаты интересны как с точки зрения теоретической алгебраической и алгоритмической теории чисел, так и для ряда приложений, например, для генерации ключей RSA в Дедекиндовых кольцах.

ГЛАВА 2.
ПРЕДВАРИТЕЛЬНЫЕ СВЕДЕНИЯ

2.1 Идеалы

О п р е д е л е н и е 2.1. Далее под кольцом мы будем понимать коммутативное ассоциативное кольцо с единицей, под областью целостности – коммутатичное ассоциативное кольцо с единицей и без делителей нуля.

О п р е д е л е н и е 2.2. Идеалом $\mathfrak{I}$ кольца R будем называть подкольцо, такое что $ab \in \mathfrak{I}$ для любых $a \in R$ и $b \in \mathfrak{I}$. Далее идеалы, как правило, будем обозначать готическими буквами.

О п р е д е л е н и е 2.3. Идеалы R и $(0) = \{0\}$ будем называть несобственными идеалами, все остальные идеалы – собственными.

Определение идеала позволяет ввести отношение сравнимости по его модулю[29].

О п р е д е л е н и е 2.4. Будем говорить, что два элемента $a, b \in R$ сравнимы по модулю идеала $\mathfrak{I}$ и записывать $a \equiv b (\mathrm{mod}\, \mathfrak{I})$, если $a - b \in \mathfrak{I}$. Данное отношение является отношением эквивалентности.

Примером идеалов кольца могут служить следующие конструкции[29]:

Утверждение 2.1. *Для любого подмножества $S \subset R$ совокупность всех конечных линейных комбинаций*

$$a_1 x_1 + \cdots + a_n x_n, \;\; x_1, \ldots, x_m \in S, a_1, \ldots, a_m \in R,$$

является наименьшим идеалом, содержащим S. Далее такой идеал будем обозначать (S). Идеал порождённый одним элементом $u \in R$ будем обозначать (u) и называть главным идеалом.

О п р е д е л е н и е 2.5. Область целостности, в которой всякий идеал является главным будем называть кольцом главных идеалов.

Примером кольца главных идеалов являются Евклидовы кольца[29]:

О п р е д е л е н и е 2.6. Область целостности будем называть Евклидовым кольцом, если существует Евклидова функция $d : R\backslash\{0\} \to \mathbb{N}_0$, что для любых $a, b \in R, b \neq 0$ имеется представление $a = bq + r$, для которого $d(r) < d(b)$ или $r = 0$.

Утверждение 2.2. *Всякое евклидово кольцо является областью главных идеалов.*

На множестве идеалов можно ввести следующие операции[30]:

О п р е д е л е н и е 2.7. Суммой идеалов $\mathfrak{I}$ и $\mathfrak{J}$ кольца R будем называть минимальный идеал кольца R, который одновременно содержит идеалы $\mathfrak{I}$ и $\mathfrak{J}$.

Произведением идеалов $\mathfrak{I}$ и $\mathfrak{J}$ кольца R будем называть идеал $\{ab|a \in \mathfrak{I}, b \in \mathfrak{J}\}$.

Следующие типы идеалов служат обощением простых натуральных чисел[30]:

О п р е д е л е н и е 2.8. Идеал $\mathfrak{I}$ кольца R называется максимальным, если любой идеал $\mathfrak{J}$, такой что $\mathfrak{I} \subset \mathfrak{J}$, совпадает либо с $\mathfrak{I}$, либо с R.

Идеал $\mathfrak{I}$ кольца R называется простым, если $\mathfrak{I} \neq R$ и, если $ab \in \mathfrak{I}$, то $a \in \mathfrak{I}$ или $b \in \mathfrak{I}$.

Утверждение 2.3. *Каждый максимальный идеал является простым, но обратное верно не всегда.*

Существуют следующие критерии для простоты и максимальности идеалов[30]:

Утверждение 2.4. *Идеал $\mathfrak{I}$ кольца R ялвляется простым тогда и только тогда, когда фактор-кольцо $R/\mathfrak{I}$ является областью целостности.*

Идеал $\mathfrak{I}$ кольца R является максимальным тогда и только тогда, когда фактор-кольцо $R/\mathfrak{I}$ является полем.

Для идеалов верен следующий аналог Китайской теоремы об остатках[30]:

О п р е д е л е н и е 2.9. Идеалы $\mathfrak{I}$ и $\mathfrak{J}$ кольца R будем называть взаимнопростыми, если $\mathfrak{I} + \mathfrak{J} = R$.

Утверждение 2.5. *Пусть* $\mathfrak{I}_1, \mathfrak{I}_2, \ldots, \mathfrak{I}_n$ *являются попарно взаимнопростыми идеалами кольца* R*, тогда*

$$R/(\mathfrak{I}_1\mathfrak{I}_2\cdots\mathfrak{I}_n) \simeq (R/\mathfrak{I}_1) \times (R/\mathfrak{I}_2) \times \ldots (R/\mathfrak{I}_n).$$

$$(R/(\mathfrak{I}_1\mathfrak{I}_2\cdots\mathfrak{I}_n))^\times \simeq (R/\mathfrak{I}_1)^\times \times (R/\mathfrak{I}_2)^\times \times \ldots (R/\mathfrak{I}_n)^\times.$$

Важными классами колец являются дедекиндовы и нётеровы кольца[30]:

Определение 2.10. Кольцо R называется дедекиндовым, если в нём выполнен аналог основной теоремы арифметики для идеалов, а именно, любой собственный идеал раскладывается в произведение простых идеалов единственным образом, с точностью до порядка сомножителей.

Определение 2.11. Кольцо R называется нётеровым, если любой идеал является конечнопредставленным, то есть может быть записан как конечная сумма главных идеалов.

Верно следующее утверждение[30]:

Утверждение 2.6. *Дедекиндово кольцо является нётеровым, причём любой идеал может быть порождён не более чем двумя элементами.*

Далее под кольцом вычетов по модулю будем подразумевать $R/\mathfrak{I}$, мультипликативную группу данного кольца будем обозначать за $(R/\mathfrak{I})^\times$.

Также через $R^\times$ будем обозначать мультипликативную группу кольца, а через R^* обозначим $R \setminus \{0\}$.

Далее введём аналоги символов Лежандра и Якоби. Пусть $\mathfrak{p}$ – простой идеал, тогда будем считать, что $\left[\frac{a}{\mathfrak{p}}\right]$ равно 1, если a является квадратичным вычетом по модулю $\mathfrak{p}$, то есть существует $b \in R$, что $b^2 \equiv a (\mathrm{mod}\, \mathfrak{p})$, в противном случае будем считать, что $\left[\frac{a}{\mathfrak{p}}\right]$ равен -1. Аналог символа Якоби определим как

$$\left[\frac{a}{\mathfrak{n}}\right] = \left[\frac{a}{\mathfrak{p}_1}\right]\left[\frac{a}{\mathfrak{p}_2}\right]\cdots\left[\frac{a}{\mathfrak{p}_r}\right],$$

где $a = \mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_r$ и $\mathfrak{p}_i$ – простые.

2.2 Абстрактные числовые кольца

Определение 2.12. Область целостности R будем называть абстрактным числовым кольцом, если R является дедекиндовым, а также для любого ненулевого идеала $\mathfrak{I}$ фактор-кольцо $R/\mathfrak{I}$ конечно.

Замечание 2.1. Исходя из Утверждений 2.3 и 2.4 любой простой идеал в абстрактном числовом кольце является максимальным и наоборот, так как конечная область целостности является полем.

Также, исходя из Утверждения 2.6, абстрактное числовое кольцо является Нётеровым, то есть любой идеал является конечнопорождённым.

Также в абстрактном числовом кольце можно ввести понятия нормы и аналога функции Эйлера для идеалов:

Определение 2.13. Нормой ненулевого идеала $\mathfrak{I}$ абстрактного числового кольца R будем называть $|R/\mathfrak{I}|$ и обозначать $\mathrm{Nm}(\mathfrak{I})$, а функцией Эйлера будем называть $|(R/\mathfrak{I})^\times|$ и обозначать $\varphi(\mathfrak{I})$ или $\varphi_R(\mathfrak{I})$.

В абстрактном числовом кольце верны следующие свойства:

Утверждение 2.7. *Норма является полностью мультипликативной функцией, то есть для любых ненулевых идеалов $\mathfrak{I}$ и $\mathfrak{J}$ верно*

$$\mathrm{Nm}(\mathfrak{I}\mathfrak{J}) = \mathrm{Nm}(\mathfrak{I})\mathrm{Nm}(\mathfrak{J}).$$

Функция Эйлера является мультипликативной функцией, то есть для любых ненулевых взаимнопростых идеалов $\mathfrak{I}$ и $\mathfrak{J}$ верно

$$\varphi(\mathfrak{I}\mathfrak{J}) = \varphi(\mathfrak{I})\varphi(\mathfrak{J}).$$

Исходя из теоремы Лагранжа можно получить аналог теоремы Эйлера[7]:

Утверждение 2.8. *Для любого идеала $\mathfrak{n}$ и $a \in (R/\mathfrak{n})^\times$ выполнено*

$$a^{\varphi(\mathfrak{n})} \equiv 1 (\mathrm{mod}\, \mathfrak{n}).$$

Также верна следующая формула для вычисления аналога функции Эйлера[]:

Утверждение 2.9. *Пусть* $\mathfrak{p} = \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_r^{\alpha_r}$, *где* $\mathfrak{p}_i$ - *простые идеалы и* $\alpha_i \in \mathbb{N}$. *Тогда*

$$\varphi_K(\mathfrak{p}) = (\mathfrak{p}_1^{\alpha} - \mathfrak{p}_1^{\alpha-1}) \cdots (\mathfrak{p}_r^{\alpha_r} - \mathfrak{p}_r^{\alpha_r-1}). \tag{2.1}$$

Наиболее важными примерами абстрактных числовых колец для данной работы являются следующие примеры:

Замечание 2.2.

1. Пусть K – поле, такое что $\mathbb{Q} \subset K \subset \mathbb{R}$ и K конечномерно как векторное пространство над $\mathbb{Q}$. Такое поле будем называть конечным расширением поля $\mathbb{Q}$. Далее рассмотрим множество целых алгебраических элементов K, то есть тех, которые являются корнями приведённых многочленов с целыми коэффициентами. Множество таких элементов обозначим за $\mathcal{O}_K$. Вместе с естественными операциями сложения и умножения оно образует абстрактное числовое кольцо.
2. Пусть $\mathbb{F}$ является конечным полем и $f \in \mathbb{F}[x,y]$, причём f является несингулярным, то есть в любой точке $(x_0, y_0) \in \mathbb{F} \times \mathbb{F}$ формальные производные $\partial f/\partial x$ и $\partial f/\partial y$ одновременно не обращаются в ноль. Далее рассмотрим фактор-кольцо $C_f = \mathbb{F}[x, y]/(f)$, которое будем называть координатным кольцом кривой $f = 0$. Данное кольцо удовлетворяет условиям абстрактного координатного кольца.

2.3 Постановка задачи

В данной работе нами будут исследоваться критерии простоты идеалов в абстрактных числовых кольцах. В частности, мы будем обобщать критерии известные для самого просто абстрактного числового кольца – кольца целых чисел на более широкий класс колец.

Далее нами будут исследованы алгоритмы тестирования на простоту основанные на полученных критериях. Интерес будут представлять в первую очередь полиномиальные, как вероятностные, так и детерминированные тесты простоты. Применимость и свойства данных алгоритмов будет исследована как для случая произвольного абстрактного числового кольца, так и для более конкретных примеров описанных выше.

ГЛАВА 3.
КРИТЕРИИ ПРОСТОТЫ

В данной главе нами будут получены некоторые ктрерии простоты идеалов в абстрактных числовых кольцах. Далее мы исследуем возможность и эффективность применения вероятностных тестов на основе данных критериев.

3.1 Аналог критерия Эйлера

Следующая теорема является аналогом критерия Эйлера:

Теорема 3.1. *Пусть* $\mathfrak{n}$ *– ненулевой идеал нечётной нормы в абстрактном числовом кольце* R*. Тогда* $\mathfrak{n}$ *является простым тогда и только тогда, когда для любого* $a \in (R/\mathfrak{n})^\times$ *выполнено сравнение* $a^{(\mathrm{Nm}(\mathfrak{n})-1)/2} \equiv \left[\frac{a}{\mathfrak{n}}\right] (\mathrm{mod}\, \mathfrak{n})$.

Доказательство.

Для начала докажем необходимое условие. Предположим, что $\mathfrak{n}$ является ненулевым простым идеалом нечётной нормы в кольце R. Рассмотрим произвольный элемент $a \in (R/\mathfrak{n})^\times$. Получаем, что требуется показать, что a – квадратичный вычет по модулю $\mathfrak{n}$ тогда и только тогда, когда выполнено сравнение

$$a^{(\mathrm{Nm}(\mathfrak{n})-1)/2} \equiv 1 (\mathrm{mod}\, \mathfrak{n}). \tag{3.1}$$

Согласно Утверждению 2.4 существует g – некоторый первообразный корень(порождающий элемент $(\mathbb{R}/\mathfrak{n})^\times$) по модулю $\mathfrak{n}$. Так как $\mathrm{Nm}(\mathfrak{n})$ нечётно, то a является квадратичным вычетом по модулю $\mathfrak{n}$ тогда и только тогда, когда существует чётное число $t \in \{0,1,\ldots,\mathrm{Nm}(\mathfrak{n})-1\}$, такое что $a \equiv g^t (\mathrm{mod}\, \mathfrak{n})$. Последнее равносильно соотношению (3.1).

Далее докажем достаточное условие. Пусть далее $\mathfrak{n}$ является ненулевым идеалом нечётной нормы, причём для любого элемента $a \in (R/\mathfrak{n})^\times$ верно сравнение $a^{(\mathrm{Nm}(\mathfrak{n})-1)/2} \equiv \left[\frac{a}{\mathfrak{n}}\right] (\mathrm{mod}\, \mathfrak{n})$.

Рассмторим каноническое разложение идеала $\mathfrak{n}$ на простые сомножители: $\mathfrak{n} = \prod_{i=1}^{r} \mathfrak{p}_i^{\alpha_i}$, где $\mathfrak{p}_i$ ненулевые простые идеалы нечётной нормы и $\alpha_i \in \mathbb{N}$. Пусть также $\mathrm{Nm}(\mathfrak{p}_j) = q_j^{f_j}$, где q_j является простым натуральным числом.

Рассмотрим следующие возможные два случая.

Случай 1. Пусть в данном случае существует $i \in \{1,\dots,r\}$, такое что $\alpha_i > 1$. Рассмотрим $a \in (R/\mathfrak{n})^\times$ элемент порядка $q_j l$ (такой элемент существует исходя из Утверждения 2.5 и теоремы Коши для абелевых групп[7]). Исходя из сравнения (3.1) получаем $q_j|(\mathrm{Nm}(N)-1)$, что приводит к противоречию.

Случай 2. Пусть в данном случае верно, что $\alpha_i = 1$ для любого $i \in \{1,\dots,r\}$, $r \geq 2$. Рассмотрим $b \in (R/\mathfrak{p}_1)^\times$ – произвольный квадратичный невычет(такой существует, так как можно считать, что $\mathrm{Nm}(\mathfrak{p}_1) \geqslant 5$). Исходя из Утверждения 2.5 найдётся элемент $a \in (R/\mathfrak{n})^\times$ такой, что выполнено $a \equiv b(\mathrm{mod}\,\mathfrak{p}_1)$, $a \equiv 1(\mathrm{mod}\,\mathfrak{p}_2\dots\mathfrak{p}_r)$. ОТсюда получаем, $\left[\frac{a}{\mathfrak{n}}\right] = -1$. Значит $a^{(\mathrm{Nm}(\mathfrak{n})-1)/2} \equiv -1(\mathrm{mod}\,\mathfrak{n})$. Исходя из последнего сравнения получаем противоречие с $a \equiv 1(\mathrm{mod}\,\mathfrak{p}_2)$.

Таким образом, доказано что идеал $\mathfrak{n}$ является простым в R.

$\otimes$

3.2 Аналог критерия Миллера

Следующая теорема является аналогом критерия Миллера:

Теорема 3.2. *Пусть $\mathfrak{n}$ – ненулевой идеал нечётной нормы абстрактного числового кольца R. Тогда следующие утверждения эквивалентны*

1. $\mathfrak{n}$ *простой идеал;*
2. $\forall a,(a,\mathfrak{n}) = 1, a^u \not\equiv 1(\mathrm{mod}\,\mathfrak{n}) : \exists k \in \{0,\dots,t-1\}$, *такое что* $a^{2^k u} \equiv -1(\mathrm{mod}\,\mathfrak{n})$, *где* $\mathrm{Nm}(\mathfrak{n}) - 1 = 2^t u,(u,2) = 1$.

Доказательство.

Для начала докажем необходимое условие. Пусть $\mathfrak{n}$ ненулевой простой идеал нечётной нормы. Отметим, что тогда $\varphi_K(\mathfrak{n}) = \mathrm{Nm}(\mathfrak{n}) - 1 = 2^t u$, $(u,2) = 1$. Рассмотрим элемент $a \in \mathbb{R}$, такой что $(a,\mathfrak{n}) = 1$ и $a^u \not\equiv 1(\mathrm{mod}\,\mathfrak{n})$. Из теоремы Лагранжа [29] для группы $(R/\mathfrak{n})^\times$ следует, что верно выражение $a^{\varphi(\mathfrak{n})} \equiv a^{\mathrm{Nm}(\mathfrak{n})-1} \equiv a^{2^t u} \equiv 1(\mathrm{mod}\,\mathfrak{n})$. Отсюда

$$(a^u - 1)(a^u + 1)(a^{2u} + 1)\dots(a^{2^{t-1}u} + 1) \equiv 0(\mathrm{mod}\,\mathfrak{n}). \tag{3.2}$$

Так как $a^u - 1 \not\equiv 0(\mathrm{mod}\,\mathfrak{n})$, то из равенства (3.2) следует существование такого $k \in \{0,\dots,t-1\}$, что $a^{2^k u} \equiv -1(\mathrm{mod}\,\mathfrak{n})$.

Докажем достаточное условие. Допустим, что $\mathfrak{n}$ не является простым идеалом. Рассмотрим каноническое разложение $\mathfrak{n}$ в произведение простых сомножителей: $\mathfrak{n} = \prod_{i=1}^{r} \mathfrak{p}_i^{\alpha_i}$, где $\mathfrak{p}_i$ являются различными простыми идеалами нечётной нормы, $\alpha_i \in \mathbb{N}$. Пусть также $\mathrm{Nm}(\mathfrak{p}_j) = q_j^{f_j}$, где q_j простое натуральное число.

Рассмотрим возможные два случая:

Случай 1. Пусть в этом случае существует $j \in \{1, \ldots, r\}$, такое что $\alpha_j > 1$.

Следуя схеме доказательства Теоремы 3.1 получаем существование $a \in (R/\mathfrak{n})^\times$ порядка $q_j l$. Исходя из того, что $u \not\equiv 0 (\mathrm{mod}\, q_j)$, получаем $a^u \not\equiv 1 (\mathrm{mod}\, \mathfrak{n})$. Значит найдётся число $k \in \{1, \ldots, t-1\}$, такое что выполнено $a^{2^{k+1}u} \equiv 1 (\mathrm{mod}\, \mathfrak{n})$. Получаем, $2^{k+1}u \equiv 0 (\mathrm{mod}\, q_j)$. Из последнего выражения следует, что $\mathrm{Nm}(\mathfrak{n}) - 1 \equiv 0 (\mathrm{mod}\, q_j)$, что приводит к противоречию.

Случай 2. Пусть в данном случае $\alpha_j = 1$ для любого $j \in \{1, \ldots, r\}$, $r \geq 2$. Исходя из аналога Китайской теоремы об остатках 2.5 и того факта, элемент -1 имеет порядок 2 в каждой группе $(R/\mathfrak{p}_j)^\times$, получаем существование по крайней мере $2^r - 1 \geq 3$ элемента $\mathcal{O}_{K,\mathfrak{n}}^\times$ порядка 2. Рассмотрим $a \not\equiv \pm 1 (\mathrm{mod}\, \mathfrak{n})$, произвольный элемент порядка 2 в группе $(R/\mathfrak{n})^\times$. Так как число u нечётно, то $a^u = a \not\equiv \pm 1 (\mathrm{mod}\, \mathfrak{n})$. Значит, найдётся $k \in \{0, \ldots, t-1\}$, такое что $a^{2^k u} \equiv -1 (\mathrm{mod}\, \mathfrak{n})$. Последнее сравнение противоречит тому, что $a^u \not\equiv \pm 1 (\mathrm{mod}\, \mathfrak{n})$ и a имеет порядок 2 в $(R/\mathfrak{n})^\times$.

Во всех случаях было получено противоречие, значит, идеал $\mathfrak{n}$ является простым.

$\otimes$

3.3 Тесты на простоту в произвольном абстрактном числовом кольце

На основе вышедоказанного аналога критерия Миллера можно получить следующий алгоритм тестирования на простоту в произвольном абстрактном числовом кольце.

Алгоритм 1. Пусть $\mathfrak{n}$ нетривиальный идеал нечётной нормы. Мы хотим определить является ли элемент $\mathfrak{n}$ простым в R.

1. Вычислить $\mathrm{Nm}(\mathfrak{n})$ и определить неотрицательные числа $u,t \in \mathbb{N}$, $(u,2) = 1$, такие что $\mathrm{Nm}(\mathfrak{n}) - 1 = 2^t u$.
2. Выбрать произвольное $a \in R$. Если $a = 0$, то ответ – 'неизвестно', иначе перейти к следующему шагу алгоритма.
3. Вычислить вычет $r_0 \equiv a^u (\mathrm{mod}\, \mathfrak{n})$. Если $r_0 = 1$, то ответ – 'неизвестно', иначе положить $k = 0$ и перейти к следующему шагу алгоритма.
4. Если $k < t$ и $r_k = -1$, то ответ – 'неизвестно'. Если $k < t$ и $r_k \neq -1$, то увеличить k на 1, вычислить $r_{k+1} \equiv r_k^2 (\mathrm{mod}\, \mathfrak{n})$ и повторить шаг 4. Если $k = t$, то ответ – '$\mathfrak{n}$ не является простым'.

Если был получен ответ 'неизвестно', то мы можем повторить итерацию данного алгоритма (шаги 2 – 4) с другим значением a.

Замечание 3.1. Отметим, что данный алгоритм не является полноценным алгоритмом, так как многие необходимые операции, например арифметические операции над элементами кольца, модулярные операции, вычисление нормы идеала, могут быть нетривиальными в ряде колец, тем не менее такая схема может быть использована для тестирования в произвольном абстрактном числовом кольце.

Алгоритм 2. Пусть $\mathfrak{n}$ нетривиальный идеал нечётной нормы. Мы хотим определить является ли элемент $\mathfrak{n}$ простым в R.

1. Вычислить $\mathrm{Nm}(\mathfrak{n})$.
2. Выбрать произвольное $a \in R$. Если $a = 0$, то ответ – 'неизвестно', иначе перейти к следующему шагу алгоритма.
3. Вычислить $d = ((a), \mathfrak{n})$. Если $d \notin R^\times$, то ответ – '$\mathfrak{n}$ не является простым'.
4. Вычислить вычет $r_0 = a^{(\mathrm{Nm}(\mathfrak{n})-1)/2} \bmod \mathfrak{n}$.
5. Вычислить $r_1 = \left[\frac{a}{\mathfrak{n}}\right] \bmod \mathfrak{n}$.
6. Если $r_0 \equiv r_1 (\mathrm{mod}\, \mathfrak{n})$ то ответ – 'неизвестно'. В противном случае ответ – '$\mathfrak{n}$ не является простым'.

Если был получен ответ 'неизвестно', то мы можем повторить итерацию данного алгоритма (шаги 2 – 4) с другим значением a.

Замечание 3.2. Отметим, что для данного теста требуется уметь эффективно вычислять аналог символа Лежандра в кольце, а также наибольший общий делитель идеалов, что может оказаться очень нетривиальной задачей.

Далее приведём оценки успеха на одной итерации данных тестов, при условии, что идеал $\mathfrak{n}$ является составным.

Утверждение 3.1. *Вероятность успеха на одной итерации Алгоритма 2 не меньше* $1/2$*, при условии, что идеал* $\mathfrak{n}$ *является составным.*

Доказательство.

Заметим, что множество a, взаимнопростых с с $\mathfrak{n}$, на которых Алгоритм выдаёт ответ 'неизвестно', есть множество $G = \left\{a \in (R/\mathfrak{n})^{\times} | a^{(\mathrm{Nm}(\mathfrak{n})-1)/2} \left[\frac{a}{\mathfrak{n}}\right] \equiv 1 (\mathrm{mod}\, \mathfrak{n})\right\}$. Данное множество образует нетривиальную(исходя из аналога критерия Эйлера) подгруппу конечной группы $(R/\mathfrak{n})^{\times}$, значит, по теореме Лагранжа $|G|/|(R/\mathfrak{n})^{\times}| \leqslant 1/2$, из чего и следует необходимое.

$\otimes$

Далее получим схожий результат для аналога теста Миллера-Рабина.

Введём идеалы, которые являются аналогами целых чисел Кармайкла:

Определение 3.1. Идеал $\mathfrak{n}$ абстрактного числового кольца R будем называть идеалом Кармайкла, если $\mathrm{Nm}(\mathfrak{n})$ нечётно, $\mathfrak{n}$ не является простым, но для любого $a \in R^*$ выполнено $a^{\mathrm{Nm}(\mathfrak{n})-1} \equiv 1 (\mathrm{mod}\, \mathfrak{n})$.

Утверждение 3.2. *Любой идеал Кармайкла* $\mathfrak{n}$ *свободен от квадратов, то есть не существует такого простого идеала* $\mathfrak{p}$*, что* $\mathfrak{n} = \mathfrak{p}^2\mathfrak{m}$.

Доказательство. Предположим, что существует идеал Кармайкла $\mathfrak{n}$, такой что $\mathfrak{n} = \mathfrak{p}^2\mathfrak{m}$ для некоторого простого идеала $\mathfrak{p}$. Тогда $\varphi(\mathfrak{n})$ кратно на $\varphi(\mathfrak{p}^2)$, а значит и на $\mathrm{Nm}(\mathfrak{p})$.

Согласно Теореме Коши в группе $(R/\mathfrak{n})^{\times}$ существует элемент a порядка $\mathrm{Nm}(p)$. С другой стороны $a^{\mathrm{Nm}(\mathfrak{n})-1} \equiv 1 (\mathrm{mod}\, \mathfrak{n})$, а значит и $a^{\mathrm{Nm}(\mathfrak{n})-1} \equiv 1 (\mathrm{mod}\, \mathfrak{p})$. Отсюда следует, что $\mathrm{Nm}(\mathfrak{n}) - 1$ кратно $\mathrm{Nm}(\mathfrak{p})$, откуда получаем противоречие. $\otimes$

Теорема 3.3. *Вероятность успеха на одной итерации Алгоритма 1 при условии, что* $\mathfrak{n}$ *не является простым, не меньше* $1/2$.

Доказательство.

Множество $a \in R/\mathfrak{n}$, на которых алгоритм даёт ответ 'неизвестно', это множество a, таких что $a^u \equiv 1 (\mathrm{mod}\, \mathfrak{n})$ или существует $j \in 0, 1, \ldots, t-1$, что $a^{2^j u} \equiv -1 (\mathrm{mod}\, \mathfrak{n})$(отметим, что все эти $t+1$ условия являются взаимоисключающими). Также отметим, что, если Алгоритм даёт ответ 'неизвестно' на некотором a, то выполнено $a^{\mathrm{Nm}(\mathfrak{n})-1} \equiv 1 (\mathrm{mod}\, \mathfrak{n})$.

Для начала рассмотрим случай, когда $\mathfrak{n}$ не является идеалом Кармайкла. В этом случае множество $G = \{a \in (R/\mathfrak{n})^\times | a^{\mathrm{Nm}(n)-1} \equiv 1 (\mathrm{mod}\, \mathfrak{n})\}$ является нетривиальным и содержит в себе все a, на которых Алгоритм даёт ответ 'неизвестно'. Также это множество образует нетривиальную подгруппу $(R/\mathfrak{n})^\times$, отсюда по теореме Лагранжа получаем, что $|G|/|(R/\mathfrak{n})^\times| \leqslant 1/2$, из чего и следует необходимое.

Далее рассмотрим случай, когда $\mathfrak{n}$ является идеалом Карайкла. Пусть $\mathfrak{n} = \mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_r, r \geqslant 2$ и $\mathfrak{p}_i$ попарно различны и просты. Для простоты введём следующие обзначения: $\mathrm{Nm}(\mathfrak{p}_i) - 1 = 2^{t_i}u_i, (u_i, 2) = 1, s = \max\limits_{i=\overline{1,r}} t_i, P = \prod\limits_{i=1}^{r}(u_i, u)$.

Рассмотрим каждое условие по отдельности. Исходя из Утверждения 2.5 $a^u \equiv 1 (\mathrm{mod}\, \mathfrak{n})$ равносильно системе $a^u \equiv 1 (\mathrm{mod}\, \mathfrak{p}_i), i = \overline{1,r}$. Отметим, что $(R/\mathfrak{p}_i)^\times$ является цикличной исходя из Утверждения 2.4, это означает, что сравнение $a^u \equiv 1 (\mathrm{mod}\, \mathfrak{p}_i)$ эквивалентно сравнению

$$\lambda u \equiv 0 (\mathrm{mod}\, \mathrm{Nm}(\mathfrak{p}_i) - 1),$$

где $a \equiv g^\lambda (\mathrm{mod}\, \mathfrak{p}_i)$ и g – первообразный корень в $(R/\mathfrak{p}_i)^\times$. Отсюда получаем, что такое сравнение имеет $(u, \mathrm{Nm}(\mathfrak{p}_i)-1)$ решений, а сравнение $a^u \equiv 1 (\mathrm{mod}\, \mathfrak{n})$ имеет $\prod\limits_{i=1}^{r}(u, \mathrm{Nm}(\mathfrak{p}_i) - 1) = P$ решений.

Рассуждая аналогичным образом, получаем, что сравнение $a^{2^j u} \equiv -1 (\mathrm{mod}\, \mathfrak{n})$ эквивалентно системе сравнений $a^{2^j u} \equiv -1 (\mathrm{mod}\, \mathfrak{p}_i), i = \overline{1,r}$, каждое из которых в свою очередь равносильно сравнению

$$\lambda 2^j u \equiv \frac{\mathrm{Nm}(\mathfrak{p}_i) - 1}{2} (\mathrm{mod}\, \mathrm{Nm}(\mathfrak{p}_i) - 1).$$

Данное сравнение имеет решение лишь при $j < t_i$, в таком случае оно имеет $(2^j u, \mathrm{Nm}(\mathfrak{p}_i) - 1) = 2^j(u, u_i)$ решений. А значит вся система имеет решение лишь при $j < s$, в этом случае она имеет в точности $2^{jr}P$ решений.

Таким образом, количество $a \in (R/\mathfrak{n})^\times$, на которых алгоритм даёт ответ 'неизвестно' равно:

$$P + \sum_{j=0}^{S-1} 2^{jr}P = P\left(1 + \frac{2^{rs} - 1}{2^r - 1}\right) = P\frac{2^{rs} + 2^r - 2}{2^r - 1}.$$

С другой стороны

$$|(R/\mathfrak{n})^\times| = \varphi(\mathfrak{n}) = \varphi(\mathfrak{p}_1)\varphi(\mathfrak{p}_2)\cdots\varphi(\mathfrak{p}_r) = \prod_{i=1}^{r}(\mathrm{Nm}(\mathfrak{p}_i) - 1) = 2^{\sum\limits_{i=1}^{r} t_i} \prod_{i=1}^{r} u_i \geqslant P2^{sr}$$

Отсюда получаем, что

$$|G|/|(R/\mathfrak{n})^{\times}| \leqslant \frac{2^{rs}+2^{r}-2}{(2^{r}-1)2^{rs}} = \frac{1}{2^{r}-1} + \frac{1}{2^{rs}} - \frac{1}{(2^{r}-1)2^{rs}}.$$

Отметим, что в случае, когда $r = 2$, данное выражение равно $\frac{1}{3} + \frac{2}{3}\frac{1}{4^{s}}$ и не превосходит $1/2$, в случае $r > 2$ данное выражение не превосходит $\frac{1}{7} + \frac{1}{2^{3s}} < \frac{1}{2}$, из чего следует необходимое утверждение.

$\otimes$

Замечание 3.3. Отметим, что в Теореме 3.3 нами была точно вычислена вероятность для случая составного $\mathfrak{n}$ свободного от квадратов.

Замечание 3.4. Отметим, что при повторении k итераций Алгоритмов 1 или 2 в случае, когда $\mathfrak{n}$ является составным, вероятность получить правильный ответ не меньше $1 - \frac{1}{2^{k}}$, то есть при достаточном числе итераций ответ будет получен с очень высокой вероятностью.

ГЛАВА 4.
КОЛЬЦА ЦЕЛЫХ АЛГЕБРАИЧЕСКИХ ЭЛЕМЕНТОВ

В первых двух секциях данной главы введём кольца целых алгебраических элементов конечных расширений поля $\mathbb{Q}$.

4.1 Конечные расширения полей

Определение 4.1. Поле K будем называть расширением поля L, если L является подполем K. Будем говорить, что расширение конечно, если K является конечномерным векторным пространством над полем L. Размерность данного пространства будем обозначать $[K : L]$ и называть степенью расширения.

Определение 4.2. Пусть K – конечное расширение L, базисом поля K будем называть базис в K как в векторном пространстве над L.

Пусть далее K – конечное расширение L.

Далее введём понятие нормы и следа в конечном расширении:

Определение 4.3. Пусть $E = \{e_1, \ldots, e_n\}$ – базис в K, причём α – элемент K. Рассмотрим матрицу $A = (a_{ij}; i,j \in \overline{1,n}) \in L^{n\times n}$, задаваемую условиями

$$\alpha e_i = \sum_{j=1}^{n} a_{ij} e_j. \tag{4.1}$$

Тогда определим след и норму α как $\mathrm{Tr}(\alpha) = \mathrm{Tr}A$ и $\mathrm{Nm}(\alpha) = \det A$.

Отметим, что в работе рассматриваются только расширения поля $\mathbb{Q}$ и для удобства будем полагать, что норма неотрицательна (то есть будем использовать её абсолютное значение). Как мы увидим дальше, эта норма совпадает с нормой введённой в первой главе.

Норма и след обладают свойствами полной мультипликативности и аддитивности соответственно[7]:

Утверждение 4.1. *Норма и след не зависят от выбора базиса K. Причём для любых $x, y \in K$ выполнены соотношения:*

$$\mathrm{Nm}(xy) = \mathrm{Nm}(x)\mathrm{Nm}(y), \quad \mathrm{Tr}(x+y) = \mathrm{Tr}(x) + \mathrm{Tr}(y).$$

Исходя из Теоремы 53[7]:

Утверждение 4.2. *Любое поле K изоморфно полю $L[\alpha]$, то есть полю вида*

$$\{c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1} | c_i \in L, i = \overline{1,n}\}, \tag{4.2}$$

где α - некий элемент поля L с аннулирующим многочленом $g(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}$.

Определение 4.4. Будем говорить, что K – нормальное расширение L, если любой неприводимый над L многочлен $f(x)$, имеющий хотя бы один корень в K представим в виде произведения линейных множителей.

Определение 4.5. Будем говорить, что K – сепарабельное расширение L, если каждый элемент K имеет аннулирующий многочлен без кратных корней.

Определение 4.6. Будем говорить, что K – расширение Галуа поля L, если оно нормально и сепарабельно одновременно.

4.2 Кольца целых алгебраических элементов

Пусть далее K – конечное расширение L.

Определение 4.7. Элемент поля K будем называть алгебраическим, если он является корнем многочлена из $L[x]$. Элемент поля K будем называть целым алгебраическим, если он является корнем приведённого многочлена из $L[x]$.

Определение 4.8. Множество всех целых алгебраических элементов поля K будем обозначать $\mathcal{O}_K$ и называть кольцом целых.

Известен следующий результат[7]:

Утверждение 4.3. *Для любого расширения K множество $\mathcal{O}_K$ порождает область целостности относительно операций сложения и умножения в K.*

Пусть далее K – конечное расширение поля $\mathbb{Q}$.

Определение 4.9. Целым базисом в $\mathcal{O}_K$ будем называть такой базис $E = \{e_1, \ldots, e_n\}$ поля K, что любой элемент $\mathcal{O}_K$ представим в виде линейной комбинации с целыми рациональными коэффициентами.

Утверждение 4.4. *[7]. Целый базис существует в любом конечном расширении* $\mathbb{Q}$.

Во всех алгоритмах элементы кольца будут кодироваться как коэффициенты в разложении по фиксированному целому базису. Инварианты поля K будем считать константами.

Определение 4.10. Пусть $E = \{e_1, \ldots, e_n\}$ – фиксированный целый базис в K и $\alpha = \sum_{i=1}^{n} \alpha_i e_i \in \mathcal{O}_K$. Абсолютным значением или длиной записи α будем называть

$$l(\alpha) = \max_{i=\overline{1,n}} |\alpha_i|. \tag{4.3}$$

Таким образом, логарифм абсолютного значения характеризует длину записи элемента $\mathcal{O}_K$.

В [7] описаны следующие результаты:

Утверждение 4.5. *Для любого* $N \in \mathcal{O}_K$ *выполнено* $\mathrm{Nm}(N) \in \mathbb{Z}$, *более того* $\mathrm{Nm}(N)$ *кратно* N.

Утверждение 4.6. *Для любого необратимого* $N \in \mathcal{O}_K$ *выполнено* $|\mathcal{O}_{K,N}| = \mathrm{Nm}(N)$.

Определение 4.11. Будем говорить, что кольцо $\mathcal{O}_K$ факториально, если любой ненулевой необратимый элемент $\alpha \in \mathcal{O}_K$ может быть записан в виде произведения обратимого элемента ε и простых элементов p_i:

$$\alpha = \varepsilon p_1 \ldots p_r, r \geqslant 1, \tag{4.4}$$

причём данное представление единственно в том смысле, что, если

$$\alpha = \mu q_1 \ldots q_m, m \geqslant 1, \tag{4.5}$$

где μ обратим, а q_i простые, то $r = m$ и существует перестановка σ множества $\{1, \ldots, r\}$, что $p_i = \varepsilon_i q_{\sigma(i)}$, где ε_i обратим.

О п р е д е л е н и е 4.12. Будем говорить, что $\mathcal{O}_K$ является норменно-евклидовым кольцом, если для любых $a, b \in \mathcal{O}_K^*$ существуют $q, r \in \mathcal{O}_K$, что $q = bq + r$ и $\mathrm{Nm}(r) \leqslant \mathrm{Nm}(b)$.

Можно показать, что любое норменно-евклидовое кольцо является факториальным. Часть результатов данной работы будет описана для факториальных колец.

Далее обозначим $K^* = K \setminus \{0\}$ – мультипликативную группу поля, $\mathcal{O}_K^* = \mathcal{O}_K \setminus \{0\}$, $\mathcal{O}_K^\times$ - множество обратимых элементов. Исходя из полной мультипликативности нормы, получаем, что множество обратимых элементов совпадает с множеством элементов с нормой равной 1 и образует группу относительно умножения. Также для удобства введём следующие обозначения: $\mathcal{O}_{K,N} = \mathcal{O}_K/(N)$, $\mathcal{O}_{K,N}^\times = (\mathcal{O}_K/(N))^\times$, $\mathcal{O}_{K,\mathfrak{n}} = \mathcal{O}_K/\mathfrak{n}$, $\mathcal{O}_{K,\mathfrak{n}}^\times = (\mathcal{O}_K/\mathfrak{n})^\times$.

Следующую теорема была доказана Дирихле и описывает структуру группы обратимых элементов:

Утверждение 4.7. *[7] Выполнен изоморфизм $\mathcal{O}_K^\times \simeq G_K \times \mathbb{Z}^h$, где G_K – вращение группы $\mathcal{O}_K^\times$ и $h \in \mathbb{N}_0$.*

Важными свойствами являются следующие:

Утверждение 4.8. *Идеал $\mathfrak{a}$ делится на $\mathfrak{c}$ тогда и только тогда, когда любой элемент $\mathfrak{a}$ принадлежит $\mathfrak{c}$.*

Утверждение 4.9. *Главный идеал $(\mathrm{Nm}(\mathfrak{n}))$ кратен $\mathfrak{n}$.*

Утверждение 4.10. $\mathrm{Nm}(\mathfrak{n})$ *конечно для любого идеала. Причём, если $\mathfrak{n} = (n)$ - главный идеал, то $\mathrm{Nm}(\mathfrak{n}) = \mathrm{Nm}(n)$.*

Утверждение 4.11. *Сравнение*

$$\alpha\xi \equiv \beta (\mathrm{mod}\, \mathfrak{n}), \tag{4.6}$$

выполнено для некоторого ξ тогда и только тогда, когда $(\alpha$,$\mathfrak{a})$ делит $\mathfrak{n}$.

Иногда для точности аналог функции Эйлера будем обозначать за $\varphi_K(\mathfrak{p})$ вместо $\varphi(\mathfrak{p})$.

Таким образом, мы рассмотрели ряд свойств идеалов в произвольных расширениях. В случае факториальных $\mathcal{O}_K$ верно следующее свойство:

Утверждение 4.12. *[7] Пусть K - конечное расширение $\mathbb{Q}$, такое что $\mathcal{O}_K$ факториально. Тогда $\mathcal{O}_K$ является областью главных идеалов.*

Исходя из данного утверждения любой идеал в таких $\mathcal{O}_K$ может быть рассмотрен просто как элемент $\mathcal{O}_K$.

Далее для удобства обозначим через $\mathcal{P}_K$ множество простых идеалов $\mathcal{O}_K$, $P_{1,K}$ – множество простых идеалов чётной нормы, $P_{2,K}$ – множество простых идеалов нечётной нормы. Пусть также $\mathcal{T}_K = \{\varepsilon x | x \in \mathbb{Z}, \varepsilon \in \mathcal{O}_K^\times\}$, $\mathcal{Q}_K = \mathcal{O}_K \setminus \mathcal{T}_K$.

Отметим, что в $\mathcal{O}_K$ верны следующие необходимые и достаточные условия простоты идеалов:

Утверждение 4.13. *Пусть $\mathfrak{p}$ – идеал и $\mathrm{Nm}(\mathfrak{p})$ – простое в $\mathbb{Z}$, тогда $\mathfrak{p}$ простой идеал.*

Доказательство. Предположим, что $\mathfrak{p}$ - не простой, тогда $\mathfrak{p} = \mathfrak{mn}$, где $\mathfrak{m}$,$\mathfrak{n} \neq (1)$. Значит $\mathrm{Nm}(\mathfrak{p}) = \mathrm{Nm}(\mathfrak{n})\mathrm{Nm}(\mathfrak{m})$. Противоречие. $\otimes$

Отметим, что данное утверждение во многих кольцах не является необходимым. В [7] приводится следующее необходимое условие простоты.

Утверждение 4.14. *Пусть $\mathfrak{p}$ – простой идеал, тогда существует $\mathfrak{q}$ – простое в $\mathbb{Z}$, что $\mathrm{Nm}(p) = q^f$, где $f \in \mathbb{N}$.*

Отметим, что данное необходимое условие ни в каком $\mathcal{O}_K$ не является достаточным.

4.3 Способы представления идеалов

В данной секции будут рассмотрены различные способы представления идеалов в кольце $\mathcal{O}_K$.

Следующее простейшее представление будем называть базисным:

Утверждение 4.15. *Любой идеал $\mathfrak{n}$ представим в виде*

$$\mathfrak{n} = (\alpha_1, \ldots, \alpha_r) = \{\xi_1\alpha_1 + \cdots + \xi_r\alpha_r | \xi_i \in \mathcal{O}_K, i = \overline{1,r}\}, \tag{4.7}$$

где $\alpha_i \in \mathcal{O}_K$ – фиксированные элементы, причём $r \leqslant n$.

Определение 4.13. Представление

$$\mathfrak{a} = (e_1, \ldots, e_n)_{\mathbb{Z}} = \{e_1x_1 + \cdots + e_mx_m | x_i \in \mathbb{Z}, i = \overline{1,m}\}, \tag{4.8}$$

где $E = \{e_1, \ldots, e_m\} \subset \mathcal{O}_K$ – базис $\mathfrak{a}$ как $\mathbb{Z}$-модуля, будем называть $\mathbb{Z}$ - представлением идеала $\mathfrak{a}$.

Далее мы не будем требовать, чтобы элементы E были линейно независимы, но, для удобства, будем полагать, что $m = n$.

Далее под $\mathbb{Z}$-представлением будем понимать матрицу $A \in \mathbb{Z}^{n\times n}$, такую что её столбец под номером i - это коэффициенты разложения e_i в фиксированный целый базис $\mathcal{O}_K$.

В источниках [8], [13] может быть найдено следующее утверждение.

Утверждение 4.16. *Любой идеал имеет $\mathbb{Z}$-представление.*

$\mathbb{Z}$-представление требует не меньше памяти для хранения по сравнению с базисным представлением.

Определение 4.14. Представление

$$\mathfrak{a} = (a, \alpha)_2 = \{a\xi_1 + \alpha\xi_2 | \xi_1, \xi_2 \in \mathcal{O}_K\}, \tag{4.9}$$

где $a \in \mathbb{N}_0, \alpha \in \mathcal{O}_K$, будет называть 2-представление идеала $\mathfrak{a}$.

В источниках [8], [13] может быть найдено следующее утверждение.

Утверждение 4.17. *Любой идеал имеет 2-представление.*

Далее под 2-представлением будем понимать вектор $\mathbb{Z}^n$ – коэффициенты разложения α в целый базис и целое неотрицательное число a.

2-представление является частным случаем базисного представления и любое 2-представление задаёт идеал. Отметим, что оно требует меньше памяти для хранения по сравнению с $\mathbb{Z}$-представлением и базисным представлением.

В [13] приведены соответствующие алгоритмы.

Утверждение 4.18. *Существует полиномиальный алгоритм перехода от 2 - представления к $\mathbb{Z}$-представлению и обратно.*

К сожалению, не смотря на полиномиальность алгоритма, он может оказаться достаточно трудоёмким.

Рассмотрим один важный частный случай $\mathbb{Z}$-представления.

Определение 4.15. Будем говорить, что матрица $A \in \mathbb{Z}^{n\times n}$ записана в нормальной эрмитовой форме, если выполнены следующие условия:

1. $m_{i,j} = 0$, если $i > j$.
2. $m_{i,i} > 0$ для любого i.
3. Для любого $i > j$ выполнено $0 \leqslant m_{i,j} \leqslant m_{i,i}$.

Определение 4.16. Представление идеала $\mathfrak{a}$ в нормальной эрмитовой форме будем называть такое его $\mathbb{Z}$-представление

$$\mathfrak{a} = (e_1, \ldots, e_n)_{\mathbb{Z}}, \tag{4.10}$$

что соответствующая матрица является матрицей в эрмитовой нормальной форме.

В источниках [8], [13] может быть найдено следующее утверждение.

Утверждение 4.19. *Любой идеал может быть записан в нормальной эрмитовой форме, причём такое представление единственно.*

В статье [14] был построен необходимый алгоритм:

Утверждение 4.20. *Существует полиномиальный алгоритм получения представления идеала в нормальной эрмитовой форме из его $\mathbb{Z}$-представления.*

Следствие 4.1. Таким образом, за полиномиальное время можно переходить от $\mathbb{Z}$-представления, 2-представления или представления в нормальной эрмитовой форме к любому из них.

Определение 4.17. Пусть дан идеал $\mathfrak{a}$, зафиксирован целый базис E кольца $\mathcal{O}_K$ и $\mathbb{Z}$-представление идеала $\mathfrak{a} = (e_1, \ldots, e_n)_{\mathbb{Z}}$. Тогда введём абсолютное значение идеала $\mathfrak{a}$ как

$$l(\mathfrak{a}) = \max_{i=\overline{1,n}, j=\overline{1,n}} |a_{ij}|, \tag{4.11}$$

где $A = (a_{ij}) \in \mathbb{Z}^{n\times n}$ – матрица соответствующая указанному $\mathbb{Z}$-представлению.

Нетрудно видеть, что логарифм абсолютного значения идеала характеризует количество памяти необходимое для того, чтобы закодировать его $\mathbb{Z}$-представление.

В случае, когда кольцо $\mathcal{O}_K$ факториально, любой идеал является главным, а значит любой идеал может быть задан с помощью порождающего его элемента. Поэтому в таких кольцах идеал, как и любой элемент, будет кодироваться в виде вектора $\mathbb{Z}^n$ коэффициентов разложения в целый базис кольца $\mathcal{O}_K$.

4.4 Операции над элементами

В данном параграфе исследуем некоторые арифметические и модулярные операции над элементами колец целых алгебраических элементов и сложности их выполнения.

Пусть $f(L),\ g(L)$ две различные функции натурального аргумента L. Мы будем писать $f(L) = \tilde{O}(g(L))$, если существует положительная функция $h(L)$, такая что $f(L) \leq h(L)g(L)$ для любых $L \in \mathbb{N}$, и $h(L) = O(\log g(L) \log\log g(L))$. Данное обозначение вводится в связи с известной оценкой сложности перемножения двух натуральных чисел по алгоритму Шанхаге-Штрассена. Любое положительная действительное число C будет называться эффективно вычислимой константной (или просто константой), если оно зависит только от инвариантов поля K (например, степени, дискриминанта, интегрального базиса, системы фундаментальных единиц) и существует алгоритм нахождения данного числа.

Определение 4.18. Для любого $a \in \mathcal{O}_K^*$ обозначим через $\overline{a} \in \mathcal{O}_K^*$ сопряжённый элемент определяемый как $\overline{a} = \mathrm{Nm}(a)/a$.

Далее предполагаем, что элементы заданы с помощью коэффициентов своего разложения в целый базис $\mathcal{O}_K$.

Утверждение 4.21. *Пусть* a,$b \in \mathcal{O}_K^*$ *и* $l(a) \leqslant L, l(b) \leqslant L$, *тогда* $a + b$, ab, b/a *(включая проверку условия* $a|b$*),* $\mathrm{Nm}(a)$, $\overline{a}$ *могут быть вычислены за* $\tilde{O}(\log L)$ *бинарных операций.*

Доказательство.

Рассмотрим произвольные элементы $a = \sum_{i=1}^n \alpha_i e_i$, $b = \sum_{i=1}^n \beta_i e_i \in \mathcal{O}_K$, такие что $l(a) \leqslant L, l(b) \leqslant L$. Утверждение для суммы $a + b$ очевидно. Используя алгоритм Шанхаге-Штрассена быстрого перемножения чисел, нетрудно получить необходимое утверждение для произведения ab. Известно, что

$\mathrm{Nm}(a) = |\det A|$, где $A = (a_{ij}) \in \mathbb{Z}^{n\times n}$ матрица, такая что $ae_i = \sum_{j=1}^{n} a_{ij}e_j$ ($i = 1,\ldots,n$). Определитель $\det A$ может быть найден с помощью операций сложения и умножения за $\tilde{O}(\log L)$ бинарных операций. Пусть $\overline{a} = \sum_{i=1}^{n} x_i e_i$, где x_i неизвестные целые коэффициенты. Пусть

$$\mathrm{Nm}(a) = \sum_{i,j=1}^{n} \alpha_i x_j e_i e_j = \sum_{k=1}^{n} \left(\sum_{i=1}^{n} \sum_{j=1}^{n} \alpha_i x_j \alpha_k^{i,j} \right) e_k, \tag{4.12}$$

где $e_i e_j = \sum_{k=1}^{n} \alpha_k^{i,j} e_k$, тогда выполнено соотношение

$$H(x_1,x_2,\ldots,x_n)^T = (\mathrm{Nm}(a),0,\ldots,0)^T, \tag{4.13}$$

где H матрица элементов $h_{ij} \in \mathbb{Z}$ ($i,j = 1,\ldots,n$), такая что $h_{ij} = O(L)$ ($i,j = 1,\ldots,n$). Тогда существует константа D, такая что $\mathrm{Nm}(a) \leq Dl(a)^n$. Следовательно решение $(x_1,x_2,\ldots,x_n)^T$ может быть найдено за $\tilde{O}(\log L)$ бинарных операций. Пусть $b\overline{a} = \sum_{i=1}^{n} y_i e_i$, $y_i \in \mathbb{Z}$. Тогда $b/a = \frac{b\overline{a}}{\mathrm{Nm}(a)}$, условие $a|b$ эквивалентно условию $\mathrm{Nm}(a)|y_i$ для любых $i = 1,\ldots,n$. Элемент b/a может быть определён за $\tilde{O}(\log L)$ используя произведение в $\mathcal{O}_K$ и деление рациональных чисел.

$\otimes$

Замечание 4.1. В доказательстве утверждения было показано, что существует константа D, такая что $\mathrm{Nm}(a) \leqslant Dl(a)^n$ для любого $a \in \mathcal{O}_K$. Из предыдущего утверждения и правила Крамера следует, что существуют константы R и q, такие что $l(\overline{a}) \leqslant RL^q$ для любого $a \in \mathcal{O}_K$.

Утверждение 4.22. *Существует константа M, такая что для любых $a, m \in \mathcal{O}_K^*$ может быть найдено $z \in \mathcal{O}_K$ удовлетворяющее условию $a \equiv z (\mathrm{mod}\ m)$ and $l(z) \leqslant Ml(m)$. Если $l(a) \leqslant L, l(m) \leqslant L$, тогда такой элемент z может быть определён за $\tilde{O}(\log L)$ бинарных операций.*

Доказательство. Пусть $a = \sum_{i=1}^{n} a_i e_i$, $m = \sum_{i=1}^{n} m_i e_i \in \mathcal{O}_K^*$. Тогда мы получаем

$$\frac{a}{m} = \frac{a\overline{m}}{\mathrm{Nm}(m)} = \frac{1}{\mathrm{Nm}(m)} \sum_{i=1}^{n} b_i e_i = \sum_{i=1}^{n} \left\lfloor \frac{b_i}{\mathrm{Nm}(m)} \right\rfloor e_i + \sum_{i=1}^{n} \frac{b_i'}{\mathrm{Nm}(m)} e_i, \tag{4.14}$$

где $b_i' \in \mathbb{Z}$, $|b_i'| < \mathrm{Nm}(m)$, $i = 1,\ldots,n$. Так как $a\overline{m} \equiv \sum_{i=1}^{n} b_i' e_i (\mathrm{mod}\ \mathrm{Nm}(m))$, мы получаем $\overline{m} \Big| \sum_{i=1}^{n} b_i' e_i$. Тогда $a \equiv z (\mathrm{mod}\ m)$, где $z = \frac{1}{\overline{m}} \sum_{i=1}^{n} b_i' e_i$. Так как

$$z = \frac{1}{\mathrm{Nm}(m)} \sum_{k=1}^{n} e_k \left(\sum_{i,j=1}^{n} b_i' m_j \alpha_k^{i,j} \right), \tag{4.15}$$

получаем

$$l(z) = \max_{k=\overline{1,n}} \left| \frac{1}{\mathrm{Nm}(m)} \sum_{i,j=1}^{n} b'_i m_j \alpha_k^{i,j} \right| < \max_{k=\overline{1,n}} \sum_{i,j=1}^{n} |m_j \alpha_k^{i,j}| \leq$$

$$\leq l(m) \max_{k=\overline{1,n}} \sum_{i,j=1}^{n} |\alpha_k^{i,j}| = Ml(m). \tag{4.16}$$

Предположим, что $l(a) \leqslant L, l(m) \leqslant L$. Тогда $l(\overline{m}) \leq RL^q$, где q и R эффективно вычислимые константы. Так как существует константа D, такая что $\mathrm{Nm}(m) \leq Dl(m)^n$, числа b_i, b'_i могут быть найдены за $\tilde{O}(\log L)$ бинарных операций. Поэтому элемент z может быть определён в K по формуле (4.15) используя не более $\tilde{O}(\log L)$ бинарных операций. $\otimes$

Следствие 4.2. Пусть $k \in \mathbb{N}$, и для a, b, $m \in \mathcal{O}_K^*$ выполнено $l(a) \leqslant L$, $l(b) \leqslant L$, $l(m) \leqslant L$. Элементы z_1, $z_2 \in \mathcal{O}_K$ такие что $a + b \equiv z_1 (\mathrm{mod}\ m)$, $a^k \equiv z_2 (\mathrm{mod}\ m)$, $l(z_1) \leqslant Ml(m)$, $l(z_2) \leqslant Ml(m)$, могут быть определены за $\tilde{O}(\log L)$, $\tilde{O}(\log k \log L)$ бинарных операций соответственно.

4.5 Операции над идеалами

В данной секции будут исследованы алгоритмические аспекты таких операций над идеалами, как сравнение, проверка делимости, вычисление нормы.

Утверждение 4.23. *Пусть идеалы $\mathfrak{a}$ и $\mathfrak{b}$ заданы в виде нормальной эрмитовой формы и $l(\mathfrak{a}), l(\mathfrak{b}) \leqslant L$, то проверка указанных идеалов на равенство может быть выполнена за $O(\log L)$ бинарных операций.*

Доказательство.

Как было указано ранее, любой идеал однозначно задаётся своей нормально эрмитовой формой. Таким образом, достаточно проверить на поэлементное равенство две целочисленные матрицы $n \times n$ с коэффициентами размера $O(L)$. $\otimes$

Утверждение 4.24. *Пусть $\mathfrak{p}$ – простой идеал, заданный в виде 2-представления, а $\mathfrak{n}$ произвольный идеал заданный в виде $\mathbb{Z}$-представления, причём $l(\mathfrak{p}), l(\mathfrak{n}) \leqslant L$. Тогда проверка равенства $\mathfrak{p}$ и $\mathfrak{n}$ может быть выполнена за $\tilde{O}(\log L)$ операций.*

Доказательство.

Пусть $\mathfrak{p} = (\alpha, a)_2$ – 2-представление простого идеала. Нетрудно видеть, что проверка равенства $\mathfrak{p} = \mathfrak{n}$ равносильна проверке того, что $\mathfrak{p}$ делится на $\mathfrak{n}$, что по Утверждению 4.8 равносильно включению $\mathfrak{p}$ в $\mathfrak{n}$. Последнее выполнено тогда и только тогда, когда $\alpha, a \in \mathfrak{n}$ и проверка сводится к проверке разрешимости систем линейных уравнений $n \times n$ с коэффициентами размера $O(L)$, что может быть выполнено за $\tilde{O}(\log L)$ операций

$\otimes$

Утверждение 4.25. *Пусть идеал $\mathfrak{a}$ задан в виде $\mathbb{Z}$-представления и $l(\mathfrak{a}) \leqslant L$, то $\mathrm{Nm}(\mathfrak{a})$ может быть вычислено за $\tilde{O}(\log L)$ бинарных операций.*

Доказательство.

Исходя из утверждения описанного в [13] выполнено равенство $\mathrm{Nm}(\mathfrak{a}) = |\det(A)|$, где A - матрица соответствующая $\mathbb{Z}$-представлению. Нетрудно видеть, что определитель целочисленной матрицы $n \times n$ с коэффициентами размера $O(L)$ может быть вычислен за указанное число операций.

$\otimes$

Утверждение 4.26. *Пусть идеал $\mathfrak{a}$ задан в виде $\mathbb{Z}$-представления и $l(\mathfrak{a}), l(a), l(b) \leqslant L$, то проверка сравнения $a \equiv b (\mathrm{mod}\, \mathfrak{a})$ может быть выполнена за $\tilde{O}(\log L)$ бинарных операций.*

Доказательство.

Пусть изначально $\mathfrak{a}$ задан в виде $\mathbb{Z}$-представления и $l(\mathfrak{a}), l(a), l(b) \leqslant L$. Требуется проверить делимость главного идеала $(a - b)$ на идеал $\mathfrak{a}$. Исходя из Утверждения 4.8 это эквивалентно проверке включения главного идеала $(a - b)$ в идеал $\mathfrak{a}$. А это, в свою очередь, равносильно тому, что $a - b \in \mathfrak{a}$. То есть проверка сравнения сводится к проверке разложимости $a - b$ по базису идеала $\mathfrak{a}$, то есть проверке разрешимости системы линейных уравнений $n \times n$ с коэффициентами размера $O(L)$. Нетрудно видеть, что это может быть сделано за $\tilde{O}(\log L)$ бинарных операций.

$\otimes$

Утверждение 4.27. *Пусть $\mathfrak{n}$ – нетривиальный идеал отличный и $a \in \mathcal{O}_K$. Тогда существует $z \in \mathcal{O}_K$, такое что $z \equiv a (\mathrm{mod}\, \mathfrak{n})$ и $l(z) \leqslant N l(\mathfrak{n})^n$.*

Если $\mathfrak{n}$ задан с помощью $\mathbb{Z}$-представления, причём $l(\mathfrak{n}), l(a) \leqslant L$, то такой элемент z может быть вычислен за $\tilde{O}(\log L)$ бинарных операций.

Доказательство.

Пусть $E = (e_1, \ldots, e_n)$ – целый базис в $\mathcal{O}_K$, $\mathfrak{n} = (\omega_1, \ldots, \omega_n)_{\mathbb{Z}}$ – $\mathbb{Z}$-представление идеала $\mathfrak{n}$.

Пусть далее $a = \sum_{i=1}^{n} \alpha_i e_i$ и $\theta = \text{НОК}(\text{Nm}(\omega_1), \ldots, \text{Nm}(\omega_n))$.

Нетрудно видеть, что $\theta \in \mathfrak{n}$, в следствии чего $\theta \equiv 0 (\text{mod}\, \mathfrak{n})$. Отсюда следует, что $a \equiv a - \beta\theta (\text{mod}\, \mathfrak{n})$ для любого $\beta \in \mathcal{O}_K$.

Положим $\beta = \sum_{i=1}^{n} \beta_i e_i$, где $\alpha_i = \theta\beta_i + r_i$, $r_i < \theta, i = \overline{1,n}$, а также $z = a - \beta\theta$.

Тогда

$$l(z) = \max_{i=\overline{1,n}} |r_i| \leqslant |\theta| \leqslant \prod_{i=1}^{n} \text{Nm}(\omega_i) \leqslant D^n \prod_{i=1}^{n} l(\omega_i) \leqslant D^n l(\mathfrak{n})^n = N l(\mathfrak{n})^n. \quad (4.17)$$

Нетрудно видеть, что рассмотренные операции могут быть выполнены за $\tilde{O}(\log L)$ бинарных операций.

$\otimes$

Следствие 4.3. Пусть $k \in \mathbb{N}$ и $a,\ b,\ \in \mathcal{O}_K^*$, $\mathfrak{n}$ – нетривиальный идеал заданный с помощью $\mathbb{Z}$-представления. Пусть выполнено $l(a) \leqslant L$, $l(b) \leqslant L$, $l(\mathfrak{n}) \leqslant L$. Элементы $z_1,\ z_2 \in \mathcal{O}_K$ такие что $a + b \equiv z_1 (\text{mod}\ \mathfrak{n})$, $a^k \equiv z_2 (\text{mod}\ \mathfrak{n})$, $l(z_1) \leqslant N l(\mathfrak{n})^n$, $l(z_2) \leqslant N l(\mathfrak{n})^n$, могут быть определены за $\tilde{O}(\log L)$, $\tilde{O}(\log k \log L)$ бинарных операций соответственно.

Замечание 4.2. Отметим, что все указанные операции могут быть выполнены за полиномиальное время в случае, когда идеалы заданы с помощью одного из представлений: $\mathbb{Z}$-представление, 2-представление, нормальная эрмитовая форма; в силу того, что из одного представления может быть получено другое за полиномиальное время.

4.6 Вероятностное тестирование на простоту

В параграфах ранее нами были исследованы все необходимые операции для реализации Алгоритма 1. В данной секции мы оценим его сложность, а также уточним оценки вероятности на случай факториального $\mathcal{O}_K$.

Утверждение 4.28. *Алгоритм 1 имеет сложность равную* $\tilde{O}(\log^2 l(\mathfrak{n}))$ *бинарных операций.*

Доказательство.

Очевидным образом следует из оценок сложностей операций над элементами и идеалами в $\mathcal{O}_K$, которые были описаны ранее.

$\otimes$

Рассмотрим случай факториального $\mathcal{O}_K$ и оценим вероятность успеха. Далее оценим вероятность ответа 'n не является простым' предполагая, что $\mathfrak{n}$ не является простым идеалом в $\mathcal{O}_K$, $\mathrm{Nm}(\mathfrak{n})$ нечётна, при случайном выборе a.

Пусть $\mathcal{S}_\mathfrak{n}$ – множество всех $a \in \mathcal{O}_{K,\mathfrak{n}}^\times$, таких что Алгоритм 1 даёт ответ 'неизвестно', то есть $\mathcal{S}_\mathfrak{n}$ состоит из всех $a \in \mathcal{O}_{K,\mathfrak{n}}^\times$, таких что одно из следующих условий выполняется: 1) $a^u \equiv 1 (\mathrm{mod}\, \mathfrak{n})$; 2) $\exists k \in \{0, \ldots, t-1\}$, такое что $a^{2^k u} \equiv -1 (\mathrm{mod}\, \mathfrak{n})$, где $\mathrm{Nm}(\mathfrak{n}) - 1 = 2^t u$, $(u,2) = 1$.

Пусть $\mathcal{A}_\mathfrak{n}$ – множество всех $a \in \mathcal{O}_{K,\mathfrak{n}}^\times$, таких что выполняется хотя бы одно из следующих условий: 1) $a^{\mathrm{Nm}(\mathfrak{n})-1} \not\equiv 1 (\mathrm{mod}\, \mathfrak{n})$; 2) существует простой делитель p идеала $\mathfrak{n}$, такой что a является первообразным корнем в группе $\mathcal{O}_{K,p}^\times$ и $a^z \not\equiv -1 (\mathrm{mod}\, \mathfrak{n})$ для любого $z \in \mathbb{Z}$.

Обозначим множество $\mathcal{G}_{\mathfrak{n},\mathfrak{p}} = \{1 + k\mathfrak{n}/\mathfrak{p} | k \in \mathcal{O}_{K,\mathfrak{p}}\}$ для любого простого делителя $\mathfrak{p}$ идеала $\mathfrak{n}$, такого что $\mathfrak{p}^2 | \mathfrak{n}$.

Утверждение 4.29. *Для любого* $a \in \mathcal{A}_\mathfrak{n}$ *выполнено* $a\mathcal{S}_\mathfrak{n} \cap \mathcal{S}_\mathfrak{n} = \varnothing$.

Доказательство.

Пусть $s \in \mathcal{S}_\mathfrak{n}$ и $a \in \mathcal{A}_\mathfrak{n}$. Требуется доказать, что $as \notin \mathcal{S}_\mathfrak{n}$.

Рассмотрим следующие случаи:

Случай 1. $a^{\mathrm{Nm}(\mathfrak{n})-1} \not\equiv 1 (\mathrm{mod}\, \mathfrak{n})$. Так как $s \in \mathcal{S}_\mathfrak{n}$, то $s^{\mathrm{Nm}(\mathfrak{n})-1} \equiv 1 (\mathrm{mod}\, \mathfrak{n})$. Следовательно, $(as)^{\mathrm{Nm}(\mathfrak{n})-1} \not\equiv 1 (\mathrm{mod}\, \mathfrak{n})$. Поэтому $as \notin \mathcal{S}_N$.

Случай 2. Существует простой делитель p элемента $\mathfrak{n}$, такой что a является первообразным корнем в $\mathcal{O}_{K,p}^\times$ и

$$a^z \not\equiv -1 (\mathrm{mod}\, \mathfrak{n}) \; \forall z \in \mathbb{Z}. \tag{4.18}$$

Предположим, что $as \in \mathcal{S}_\mathfrak{n}$. Рассмотрим следующие четыре подслучая:

Случай 2a. $s^u \equiv 1 (\mathrm{mod}\, \mathfrak{n})$ и $(as)^u \equiv 1 (\mathrm{mod}\, \mathfrak{n})$. Получаем, что $a^u \equiv 1 (\mathrm{mod}\, \mathfrak{n})$. Так как $a^u \equiv 1 (\mathrm{mod}\, p)$ и a - первообразный корень в группе $\mathcal{O}_{K,p}^\times$, то $(\mathrm{Nm}(p) - 1) | u$. Последнее невозможно, так как u и $\mathrm{Nm}(p)$ нечётны.

Случай 2b. $s^u \equiv 1 (\mathrm{mod}\, \mathfrak{n})$ и $(as)^{2^l u} \equiv -1 (\mathrm{mod}\, \mathfrak{n})$, где $l \in \{0, \ldots, t-1\}$. Таким образом, $a^{2^l u} \equiv -1 (\mathrm{mod}\, \mathfrak{n})$. Это противоречит соотношению (4.18).

Случай 2c. $s^{2^k u} \equiv -1(\mathrm{mod}\,\mathfrak{n})$ для некоторого $k \in \{0,\ldots,t-1\}$ и $(as)^u \equiv 1(\mathrm{mod}\,\mathfrak{n})$. Следовательно $a^{-2^k u} \equiv -1(\mathrm{mod}\,\mathfrak{n})$, что противоречит соотношению (4.18).

Случай 2d. $s^{2^k u} \equiv -1(\mathrm{mod}\,\mathfrak{n})$ и $(as)^{2^l u} \equiv -1(\mathrm{mod}\,\mathfrak{n})$ для некоторых k, $l \in \{0,\ldots,t-1\}$. Рассмотрим следующие три подслучая:

Случай 2d1. $k = l$. Получаем, что $a^{2^k u} \equiv 1(\mathrm{mod}\,\mathfrak{n})$. Так как $a^{2^k u} \equiv 1(\mathrm{mod}\,p)$ и a - первообразный корень по модулю p, то $(\mathrm{Nm}(p)-1)|2^k u$. Согласно Утверждению 2.8 мы получаем, что $s^{2^k u} \equiv 1(\mathrm{mod}\,p)$, что противоречит с $s^{2^k u} \equiv -1(\mathrm{mod}\,\mathfrak{n})$.

Случай 2d2. $k < l$. Мы получаем, что $a^{2^l u} \equiv -1(\mathrm{mod}\,\mathfrak{n})$, что противоречит соотношению (4.18).

Случай 2d3. $k > l$. Мы получаем, что $a^{-2^k u} \equiv -1(\mathrm{mod}\,\mathfrak{n})$, что противоречит соотношению (4.18).

Таким образом, $as \notin \mathcal{S}_\mathfrak{n}$. Следовательно $a\mathcal{S}_\mathfrak{n} \cap \mathcal{S}_\mathfrak{n} = \varnothing$.

$\otimes$

Утверждение 4.30. *Пусть* $a \in \mathcal{A}_\mathfrak{n}$, $b \in \mathcal{O}_{K,\mathfrak{n}}^\times$, $a \neq b$ *и* $\left(ab^{-1}\right) \in \mathcal{A}_\mathfrak{n}$. *Тогда* $a\mathcal{S}_\mathfrak{n} \cap b\mathcal{S}_\mathfrak{n} = \varnothing$.

Доказательство.

Предположим, что существуют s_1, $s_2 \in \mathcal{S}_\mathfrak{n}$, такие что $as_1 \equiv bs_2(\mathrm{mod}\,\mathfrak{n})$. Тогда $s_2 \equiv ab^{-1}s_1(\mathrm{mod}\,\mathfrak{n})$, что противоречит Утверждению 4.29. Следовательно, $a\mathcal{S}_\mathfrak{n} \cap b\mathcal{S}_\mathfrak{n} = \varnothing$.

$\otimes$

Утверждение 4.31. $(\mathcal{G}_{\mathfrak{n},\mathfrak{p}},\cdot)$ *является подгруппой* $\mathcal{O}_{K,\mathfrak{n}}^\times$.

Доказательство.

Нетрудно видеть, что данная группа является образом эндоморфизма τ группы $\mathcal{O}_{K,\mathfrak{n}}^\times$, такого что $\tau(k) = 1 + k\mathfrak{n}/\mathfrak{p}$.

$\otimes$

Утверждение 4.32. *Пусть* $\mathfrak{n} \in \mathcal{O}_K$ *– идеал, такой что* $\mathfrak{n} = \mathfrak{p}\mathfrak{q}$, *где* $\mathfrak{p}$, $\mathfrak{q}$ *– различные простые идеалы,нечётной нормы, причём* $\mathrm{Nm}(\mathbb{N}) - 1 = 2^t u$, $\mathrm{Nm}(\mathfrak{p}) - 1 = \mathrm{Nm}(\mathfrak{q}) - 1 = 2^{t_1} u_1$, t, u, t_1, u_1 *- целые,* $(u,2) = (u_1,2) = 1$. *Тогда* $|\mathcal{S}_\mathfrak{n}| = (4^{t_1}+2)(u,u_1)^2/3$.

Доказательство.

Заметим, что $|\mathcal{S}_{\mathfrak{n}}|$ равно числу элементов $s \in \mathcal{O}^{\times}_{K,\mathfrak{n}}$ для которых одно из сравнений $s^u \equiv 1(\mathrm{mod}\,\mathfrak{n})$, $s^{2^k u} \equiv -1(\mathrm{mod}\,\mathfrak{n})$, $k \in \{0,\ldots,t-1\}$ выполнено. Преобразовав, первое сравнение можно записать в виде следующей эквивалентной системы:

$$\begin{cases} u \log_{\alpha} s \equiv 0(\mathrm{mod}\,\varphi_K(\mathfrak{p})), \\ u \log_{\beta} s \equiv 0(\mathrm{mod}\,\varphi_K(\mathfrak{q})), \end{cases} \tag{4.19}$$

где α и β – первообразные корни в группах $\mathcal{O}^{\times}_{K,\mathfrak{p}}$ и $\mathcal{O}^{\times}_{K,\mathfrak{q}}$ соответственно. Исходя из Утверждения 2.5 получаем, что эта система имеет ровно $(u,\varphi_K(\mathfrak{p}))(u,\varphi_K(\mathfrak{q})) = (u,u_1)^2$ решений.

Для любого числа $k \in \{0,\ldots,t-1\}$ сравнение $s^{2^k u} \equiv -1(\mathrm{mod}\,\mathfrak{n})$ равносильно системе:

$$\begin{cases} 2^k u \log_{\alpha} s \equiv \dfrac{\varphi_K(\mathfrak{p})}{2}(\mathrm{mod}\,\varphi_K(\mathfrak{p})), \\ 2^k u \log_{\beta} s \equiv \dfrac{\varphi_K(\mathfrak{q})}{2}(\mathrm{mod}\,\varphi_K(\mathfrak{q})). \end{cases} \tag{4.20}$$

Заметим, что данная система неразрешима при $k \geqslant t_1$, иначе она имеет ровно

$$(2^k u,\varphi_K(\mathfrak{p}))(2^k u,\varphi_K(\mathfrak{q})) = 4^k (u,u_1)^2 \tag{4.21}$$

решений. Таким образом,

$$|\mathcal{S}_{\mathfrak{n}}| = (u,u_1)^2 + \sum_{i=0}^{t_1-1} 4^i (u,u_1)^2 = (4^{t_1}+2)(u,u_1)^2/3. \tag{4.22}$$

$\otimes$

Теорема 4.1. *Пусть* $\mathfrak{n}$ *– нетривиальный идеал не являющийся простым в* $\mathcal{O}_K$, $\mathrm{Nm}(\mathfrak{n})$ *нечётна. Тогда выполнены следующие утверждения:*

1. *Если существует простой идеал* $\mathfrak{p}$, *такой что* $\mathfrak{p}^2 | N$, *тогда* $|S_{\mathfrak{n}}| \leqslant |\mathcal{O}^{\times}_{K,\mathfrak{n}}|/\mathrm{Nm}(\mathfrak{p})$.
2. *Если* $\mathfrak{n}$ *имеет три различных делителя, то* $|S_{\mathfrak{n}}| \leqslant |\mathcal{O}_{K,\mathfrak{n}}|/4$.
3. *Если* $\mathfrak{n} = \mathfrak{p}\mathfrak{q}$, *причём* $\mathrm{Nm}(\mathfrak{p}) \neq \mathrm{Nm}(\mathfrak{q})$, *то* $|S_{\mathfrak{n}}| \leqslant |\mathcal{O}_{K,\mathfrak{n}}|/4$.
4. *Если* $\mathfrak{n} = \mathfrak{p}\mathfrak{q}$, *причём* $\mathfrak{p}$ *и* $\mathfrak{q}$ *– различные идеалы и* $\mathrm{Nm}(\mathfrak{p}) = \mathrm{Nm}(\mathfrak{q})$, *тогда* $|S_{\mathfrak{n}}| = \frac{2+4^m}{3\cdot 4^m}|\mathcal{O}^{\times}_{K,\mathfrak{n}}|$, *где* m *– максимальная степень двойки делящая* $\mathrm{Nm}(\mathfrak{p}) - 1$.

Доказательство.

Отметим, что исходя из факториальности $\mathcal{O}_K$ все идеалы являются главными и их можно отождествлять с элементами порождающими их.

Поочерёдно рассмотрим все четыре случая:

Случай 1. Пусть существует простой идеал $\mathfrak{p} \in \mathcal{O}_K$, такой что $\mathfrak{p}^2|N$. Покажем, что для любого $g \in \mathcal{G}_{\mathfrak{n},\mathfrak{p}}$, $g \neq 1$, выполнено $g \in \mathcal{A}_\mathfrak{n}$. Рассмотрим произвольное $g \in \mathcal{G}_{\mathfrak{n},\mathfrak{p}}$, $g \neq 1$. Тогда для любого $k \in \mathcal{O}_{K,\mathfrak{p}}$ выполнено $g^{\mathrm{Nm}(\mathfrak{n})-1} \equiv (1+k\mathfrak{n}/\mathfrak{p})^{\mathrm{Nm}(\mathfrak{n})-1} \equiv 1 + k(\mathrm{Nm}(\mathfrak{n})-1)\mathfrak{n}/\mathfrak{p} (\mathrm{mod}\, \mathfrak{n})$. Заметим, что $g^{\mathrm{Nm}(\mathfrak{n})-1} \not\equiv 1 (\mathrm{mod}\, \mathfrak{n})$. Значит, $g \in \mathcal{A}_\mathfrak{n}$. Из Утверждений 4.30 и 4.31 получаем, что $g_1\mathcal{S}_\mathfrak{n} \cap g_2\mathcal{S}_\mathfrak{n} = \varnothing$ для различных g_1, $g_2 \in \mathcal{G}_{\mathfrak{n},p}$. Следовательно, $\bigcup_{g\in\mathcal{G}_{\mathfrak{n},p}}(g\mathcal{S}_\mathfrak{n}) \subseteq \mathcal{O}^\times_{K,\mathfrak{n}}$. Окончательно получаем, $|\mathcal{O}^\times_{K,\mathfrak{n}}| \geqslant \sum_{g\in\mathcal{G}_{\mathfrak{n},p}} |g\mathcal{S}_\mathfrak{n}| = |\mathcal{G}_{\mathfrak{n},\mathfrak{p}}||S_\mathfrak{n}| = \mathrm{Nm}(\mathfrak{p})|\mathcal{S}_\mathfrak{n}| \geqslant 3|\mathcal{S}_\mathfrak{n}|$.

Случай 2. Существует по крайней мере три простых идеала $\mathfrak{p}_i$, $i \in \{1,2,3\}$ в $\mathcal{O}_K$, таких что $\mathfrak{p}_i|\mathfrak{n}$ для любых $i = 1,2,3$ и $(\mathfrak{p}_i,\mathfrak{p}_j) = 1$ для любых i, $j \in \{1,2,3\}$, $i \neq j$. Согласно Утверждению 2.5, для любых $i \in \{1,2,3\}$ существуют $c_i \in \mathcal{O}^\times_{K,\mathfrak{n}}$, такие что $c_i \equiv a_i (\mathrm{mod}\, \mathfrak{p}_i)$ и $c_i \equiv 1 (\mathrm{mod}\, \mathfrak{p}_k)$, $k \in \{1,2,3\}$, $k \neq i$, где a_i – первообразный корень по модулю $\mathfrak{p}_i$. Нетрудно видеть, что c_i, c_i^{-1}, c_ic_j, $c_ic_j^{-1} \in \mathcal{A}_\mathfrak{n}$ для любых i, $j \in \{1,2,3\}$, $i \neq j$ (все эти элементы удовлетворяют условию (2) определения $\mathcal{A}_\mathfrak{n}$). Используя Утверждение 4.30, получаем, что $|\mathcal{O}^\times_{K,\mathfrak{n}}| \geqslant |\mathcal{S}_\mathfrak{n}| + |c_1\mathcal{S}_\mathfrak{n}| + |c_2\mathcal{S}_\mathfrak{n}| + |c_1c_2\mathcal{S}_\mathfrak{n}| = 4|\mathcal{S}_\mathfrak{n}|$.

Случай 3. Пусть $\mathfrak{n} = \mathfrak{p}_1\mathfrak{p}_2$, где $\mathfrak{p}_1$, $\mathfrak{p}_2$ простые идеалы $\mathcal{O}_K$, не нарушая общности пусть $\mathrm{Nm}(\mathfrak{p}_1) < \mathrm{Nm}(\mathfrak{p}_2)$. Согласно Утверждению 2.5, для любого $i \in \{1,2\}$ существуют $c_i \in \mathcal{O}^\times_{K,\mathfrak{n}}$, такие что $c_i \equiv a_i (\mathrm{mod}\, \mathfrak{p}_i)$ и $c_i \equiv 1 (\mathrm{mod}\, \mathfrak{p}_k)$, $k \in \{1,2\}$, $k \neq i$, где a_i – первообразные корни по модулю $\mathfrak{p}_i$. Аналогично случаю 3 получаем, что c_1, $c_2 \in \mathcal{A}_\mathfrak{n}$. Покажем, что $d = c_1c_2 \in \mathcal{A}_\mathfrak{n}$. Предположим, что $d^{\mathrm{Nm}(\mathfrak{n})-1} \equiv 1 (\mathrm{mod}\, \mathfrak{n})$. Следовательно, $d^{\mathrm{Nm}(\mathfrak{n})-1} \equiv 1 (\mathrm{mod}\, \mathfrak{p}_2)$. Так как d является первообразным корнем по модулю $\mathfrak{p}_2$, то $(\mathrm{Nm}(\mathfrak{p}_2)-1)|(\mathrm{Nm}(\mathfrak{n})-1) = \mathrm{Nm}(\mathfrak{p}_1)(\mathrm{Nm}(\mathfrak{p}_2)-1) + \mathrm{Nm}(\mathfrak{p}_1) - 1$. Получаем противоречие, так как $\mathrm{Nm}(\mathfrak{p}_1) < \mathrm{Nm}(\mathfrak{p}_2)$ и $\mathrm{Nm}(\mathfrak{p}_2) \geq 3$. Таким образом, $c_1c_2 \in \mathcal{A}_\mathfrak{n}$. Аналогичным образом можно доказать, что $c_1c_2^{-1} \in \mathcal{A}_\mathfrak{n}$. Как и в случае 3, получаем неравенство $|\mathcal{O}^\times_{K,\mathfrak{n}}| \geqslant 4|\mathcal{S}_\mathfrak{n}|$.

Случай 4. Пусть $\mathfrak{n} = \mathfrak{p}\mathfrak{q}$, где $\mathfrak{p}$, $\mathfrak{q}$ простые идеалы в $\mathcal{O}_K$ такие, что $(\mathfrak{p},\mathfrak{q}) = 1$ и $\mathrm{Nm}(\mathfrak{p}) = \mathrm{Nm}(\mathfrak{q})$. Пусть $\mathrm{Nm}(\mathfrak{n})-1 = 2^tu$, $\mathrm{Nm}(\mathfrak{p})-1 = \mathrm{Nm}(\mathfrak{q})-1 = 2^{t_1}u_1$, t, u, t_1, u_1 целые числа такие, что, $(u,2) = (u_1,2) = 1$. Тогда $\varphi_K(\mathfrak{n}) = \varphi_K(\mathfrak{p})\varphi_K(\mathfrak{q}) =$

$2^{2t_1}u_1^2$. Используя Утверждение 4.32, получаем, что

$$\frac{|\mathcal{S}_{\mathfrak{n}}|}{|\mathcal{O}_{K,\mathfrak{n}}^{\times}|} = \frac{(2+4^{t_1})(u,u_1)^2}{3u_1^2 4^{t_1}} \leqslant \frac{2+4^{t_1}}{3\cdot 4^{t_1}} \leqslant \frac{1}{2}. \tag{4.23}$$

$\otimes$

Замечание 4.3. Отметим, что в первых трех случаях теоремы верна оценка $|\mathcal{S}_{\mathfrak{n}}| \leqslant 1/3|\mathcal{O}_{K,\mathfrak{n}}^{\times}|$.

Если рассматривать идеалы, свободные от делителей нормы 2 и 3(то есть, некоторого конечного множества делителей), то в первых трёх случаях теоремы верна оценка $|\mathcal{S}_{\mathfrak{n}}| \leqslant 1/4|\mathcal{O}_{K,\mathfrak{n}}^{\times}|$.

Минимальное соотношение $|S_{\mathfrak{n}}|$ и $|\mathcal{O}_{K,\mathfrak{n}}^{\times}|$ достигается в случае $\mathfrak{n} = \mathfrak{pq}$, где $\mathfrak{p}$,$\mathfrak{q}$ различные идеалы, $\mathrm{Nm}(\mathfrak{p}) = \mathrm{Nm}(\mathfrak{q})$ и $\mathrm{Nm}(p) - 1 = 2u, (u,2) = 1$. В этом случае, $|S_{\mathfrak{n}}| = 1/2|\mathcal{O}_{K,\mathfrak{n}}^{\times}|$. Таким образом, в общем случае $|S_{\mathfrak{n}}|/|\mathcal{O}_{K,\mathfrak{n}}^{\times}| \leqslant 1/2$.

В некоторых кольцах можно несколько улучшить данную оценку, например, при в $\mathbb{Z}[i]$, если $\mathrm{Nm}(\mathfrak{n})$ чётна, то $\mathrm{Nm}(\mathfrak{n})$ кратна 4, а значит $|S_{\mathfrak{n}}|/|\mathcal{O}_{K,\mathfrak{n}}^{\times}| \leqslant 3/8$.

Тем не менее, в некоторых кольцах доказанная оценка достигается. Рассмотрим кольцо $\mathbb{Z}[\sqrt{-2}]$. Положительное нечётное число может быть представлено в виде $x^2 + 2y^2$,$x,y \in \mathbb{N}$,$(x,y) = 1$ в случае, если оно свободно от простых делителей вида $8n+5, 8n+7$[22]. Рассмотрим последовательность чисел $N_l, l \in \mathbb{N}$ - простых чисел вида $8k+3$. Так как $\left(\frac{\Delta_K}{8n+3}\right) = \left(\frac{-8}{8n+3}\right) = 1$, получаем, что N_l – составное в $\mathbb{Z}[\sqrt{-2}]$([16]), а значит $N_l = z_l \cdot \overline{z_l}$, где z_l – простые в $\mathcal{O}_K$ и $(z_l,\overline{z_l}) = 1$. Пусть $\mathfrak{n}_l = (z_l)$ – главный простой идеал. Тогда $|S_{\mathfrak{n}_l}|/|\mathcal{O}_{K,\mathfrak{n}_l}^{\times}| = 1/2$

Замечание 4.4. Результат схожий с Теоремой 4.1 для теста Миллера-Рабина в кольце целых чисел был доказан Рабиным.Пусть $\mathcal{O}_K$ факториально. Если элемент $N \notin \mathcal{O}_K^{\times}$ не является простым в $\mathcal{O}_K$ и имеет нечётную норму, тогда, согласно Теореме 4.1, Алгоритм 1 позволяет доказать, что N не является простым с вероятностью $\mathbb{P} \geq 1 - 2^{-M}$, где M - это число итераций Алгоритма 1.

Рассмотрим случай факториального $\mathcal{O}_K$. Заметим, что для любого $a \in \mathcal{O}_{K,\mathfrak{n}}^{\times}$, свидетельствующего о простоте $\mathfrak{n}$, верно $a^{\mathrm{Nm}(\mathfrak{n})-1} \equiv 1 (\mathrm{mod}\, \mathfrak{n})$, то есть вероятность успеха не хуже, чем в тесте Ферма, а значит оценка $\mathbb{P} \geqslant 1/2$ выполнена для всех идеалов, не являющихся аналогами идеалов Кармайкла.

4.7 Детерминированное тестирование на простоту

Далее докажем усиленный аналог критерия Миллера в предположении ERH.

Для начала сформулируем необходимые утверждения связанные с Расширенной Гипотезой Римана.

Определение 4.19. Характером Дирихле абелевой группы G будем называть гомоморфизм $\chi : G \to \mathbb{C}^*$.

Рассмотрим характер группы $\mathcal{O}_{K,\mathfrak{n}}^{\times}$. Его можно продолжить на всю группу $\mathcal{O}_K^*$ по правилу: $\psi(x) = 0$, если $(x,\mathfrak{n}) \neq 1$; $\psi(x) = \xi(x \bmod \mathfrak{n})$, если $(x,\mathfrak{n}) = 1$. Нетрудно видеть, что ψ - характер $\mathcal{O}_K^*$.

Характер будем называть нетривиальным, если его образ не является тривиальной группой.

Определение 4.20. L-функция Гекке ассоциированная с характером $\chi : \mathcal{O}_K \to \mathbb{C}^*$ определяется как

$$L(s,\chi) = \sum_{a \in \mathcal{O}_K^*} \frac{\chi(a)}{(\mathrm{Nm}(a))^s},\ s \in \mathbb{C}, \tag{4.24}$$

где сумма справа берётся по всем ненулевым идеалам $\mathfrak{a}$.

Следующая версия расширенной гипотезы Римана (ERH) предполагается верной для доказательства аналога теоремы Анкени.

Гипотеза 1. [3] Все L-функции Гекке не имеют нулей в полуплоскости $\mathrm{Re}(s) > 1/2$ (ERH).

Далее считаем, что кольцо $\mathcal{O}_K$ факториально.

Следующим образом выглядит аналог Теоремы Анкени в числовых полях[3].

Утверждение 4.33. *Предположим, что ERH выполнена. χ – нетривиальный характер Дирихле группы $\mathcal{O}_{K,N}^{\times}$. Тогда существует простой элемент $p \in \mathcal{O}_K$, $(p,N) = 1$, такое что $\mathrm{Nm}(p) \leqslant 12\log^2(\Delta_K^2 \mathrm{Nm}(N))$ и $\chi(N) \neq 1$.*

Из неё можно получить следующее следствие.

Утверждение 4.34. *Предположим, что ERH выполнена. Пусть G является конечной абелевой группой и $\chi : \mathcal{O}_{K,N}^{\times} \to G$ нетривиальный гомоморфизм. Тогда существует простое $p \in \mathcal{O}_K$, $(p,N) = 1$, такое что $\mathrm{Nm}(p) \leqslant 12\log^2(\Delta_K^2\mathrm{Nm}(N))$ и $\chi(p) \neq 1_G$.*

Доказательство. Так как образ $\mathrm{Im}\,\chi$ отображения χ является нетривиальной подгруппой группы G, то можно определить нетривиальный гомоморфизм $\xi : \mathrm{Im}\,\chi \to \mathbb{C}^*$. Заметим, что $\xi \circ \chi : \mathcal{O}_{K,N}^{\times} \to \mathbb{C}^*$ является нетривиальным характером Дирихле. Понятно, что $\xi \circ \chi$ может быть расширено на все идеалы $\mathcal{O}_K$. Так как $\xi \circ \chi$ может быть рассмотрен в смысле Определения 4.19, мы можем сделать вывод, что из Утверждения 4.33 следует существование элемента $p \in \mathcal{O}_K$, $(p,N) = 1$, такого что

$$\mathrm{Nm}(p) \leqslant 12\log^2(\Delta_K^2\mathrm{Nm}(N)) \tag{4.25}$$

и $(\xi \circ \chi)(p) \neq 1$. ⊗

В данном параграфе будем считать, что выполнена ERH и что $\mathcal{O}_K$ факториально.

Утверждение 4.35. *Пусть $\mathfrak{p}$ является нетривиальным простым идеалом нечётной нормы. Тогда сравнение*

$$x^{\mathrm{Nm}(\mathfrak{p})-1} \equiv 1 (\mathrm{mod}\,\mathfrak{p}^2) \tag{4.26}$$

имеет не более $\mathrm{Nm}(\mathfrak{p}) - 1$ решений относительно $x \in \mathcal{O}_{K,\mathfrak{p}^2}^{\times}$.

Доказательство.

Так как $\mathcal{O}_K$ факториально, то $\mathfrak{p}$ - главный идеал, пусть $\mathfrak{p} = (p)$. Рассмотрим сравнение $x^{\mathrm{Nm}(p)-1} \equiv 1(\mathrm{mod}\,p)$. Из Утверждения 2.8 следует, оно выполнено для любого элемента $x \in \mathcal{O}_{K,p}^{\times}$, другими словами оно имеет ровно $\mathrm{Nm}(p) - 1$ решений относительно x.

Очевидно, что каждое решение сравнения $x^{\mathrm{Nm}(p)-1} \equiv 1(\mathrm{mod}\,p^2)$ может быть записано в виде $a + pt, a \in \mathcal{O}_{K,p}^{\times}, t \in \mathcal{O}_{K,p}$, где a - это решение $x^{\mathrm{Nm}(p)-1} \equiv 1(\mathrm{mod}\,p)$.

Применяя формулу бинома Ньютона к многочлену $P(t) = (a+pt)^{\mathrm{Nm}(p)-1} - 1$ получаем, что

$$\frac{a^{\mathrm{Nm}(p)-1} - 1}{p} + t(\mathrm{Nm}(p) - 1)a^{\mathrm{Nm}(p)-2} \equiv 0(\mathrm{mod}\,p). \tag{4.27}$$

Заметим, что данное сравнение является линейным относительно t, а значит имеет единственное решение при фиксированном a, так как $\big((\mathrm{Nm}(p)-1)a^{\mathrm{Nm}(p)-2}, p\big) = 1$.

Таким образом, сравнение $x^{\mathrm{Nm}(p)-1} \equiv 1(\mathrm{mod}\, p^2)$ имеет не более $\mathrm{Nm}(p)-1$ решений относительно $x \in \mathcal{O}^{\times}_{K,p^2}$. $\otimes$

Теорема 4.2. *Предположим, что ERH выполняется. Пусть* $\mathfrak{n}$ *– нетривиальный идеал нечётной нормы. Тогда следующие утверждения эквиваленты:*

1)$\mathfrak{n}$ *является простым идеалом.*

2)$\forall a, (a,\mathfrak{n}) = 1, \mathrm{Nm}(a) \leqslant 12\log^2(\Delta_K \mathrm{Nm}(\mathfrak{n})), a^u \not\equiv 1(\mathrm{mod}\,\mathfrak{n}) : \exists k \in \{0,\dots,t-1\}$*, такое что* $a^{2^k u} \equiv -1(\mathrm{mod}\,\mathfrak{n})$*,*

где $\mathrm{Nm}(\mathfrak{n}) - 1 = 2^t u, (u,2) = 1$.

Доказательство.

Так как $\mathcal{O}_K$ факториально, то $\mathfrak{n}$ – главный идеал, пусть $\mathfrak{n} = (N)$. Необходимость следует из Теоремы 3.2.

Докажем достаточность. Предположим, что $N \in \mathcal{O}_K \backslash \mathcal{O}^{\times}_K$ это составной элемент нечётной нормы, для которого утверждение (2) выполнено.

Предположим, что N не является свободным от квадратов, то есть существует делитель $p \in \mathcal{P}_{2,K}$ элемента N, такой что N делится на p^2. Рассмотрим отображение $\chi : \mathcal{O}^{\times}_{K,p^2} \to \mathcal{O}^{\times}_{K,p^2}$, такое что для любого $a \in \mathcal{O}^{\times}_{K,N}$ выполнено $\chi(a) = a^{\mathrm{Nm}(p)-1}$. Нетрудно видеть, что χ является эндомофризмом группы $\mathcal{O}_{K,p^2}$. Согласно Утверждению 4.35 χ является нетривиальным. Применяя Утверждение 4.34 получаем существование $\alpha \in \mathcal{O}_{K,N}$, такого что $\mathrm{Nm}(\alpha) \leqslant 12\log^2(\Delta_K \mathrm{Nm}(N))$ и $\alpha^{\mathrm{Nm}(p)-1} \not\equiv 1(\mathrm{mod}\, p^2)$.

Предположим, что $\alpha^{\mathrm{Nm}(N)-1} \equiv 1(\mathrm{mod}\, N)$. Отсюда получаем сравнение $\alpha^{\mathrm{Nm}(N)-1} \equiv 1(\mathrm{mod}\, p^2)$. Значит выполнено

$$\mathrm{ord}_{\mathcal{O}_{K,p^2}}(\alpha) | \mathrm{Nm}(N) - 1, \tag{4.28}$$

$$\mathrm{ord}_{\mathcal{O}_{K,p^2}}(\alpha) | \varphi_K(p^2) = \mathrm{Nm}(p)(\mathrm{Nm}(p)-1). \tag{4.29}$$

Из этого следует соотношение $\mathrm{ord}_{\mathcal{O}_{K,p^2}}(\alpha) | \mathrm{Nm}(p) - 1$, которое противоречит сравнению $\alpha^{\mathrm{Nm}(p)-1} \not\equiv 1(\mathrm{mod}\, N)$.

Таким образом, $\alpha^{\mathrm{Nm}(N)-1} \not\equiv 1(\mathrm{mod}\, N)$ верно и оно противоречит предположению.

Следовательно, N является свободным от квадратов. Пусть $p, q \in \mathcal{P}_{2,K}$ - различные простые делители N. Обозначим через $v_2(n)$ максимальную сте-

пень двойки делящую n. Без потери общности будем считать, что $v_2(\mathrm{Nm}(p)-1) \geqslant v_2(\mathrm{Nm}(q)-1)$. Введём следующий элемент $d \in \mathcal{O}_K$:

$$d = \begin{cases} pq, \text{ если } v_2(\mathrm{Nm}(p)-1) = v_2(\mathrm{Nm}(q)-1), \\ p, \text{ если } v_2(\mathrm{Nm}(p)-1) > v_2(\mathrm{Nm}(q)-1). \end{cases} \tag{4.30}$$

Рассмотрим отображение $\xi : \mathcal{O}_{K,N}^{\times} \to \mathcal{O}_{K,N}^{\times}$, такое что для любого $a \in \mathcal{O}_{K,N}^{\times}$ выполнено $\xi(a) = \left[\frac{a}{d}\right]$. Заметим, что ξ является нетривиальным эндоморфизмом группы $\mathcal{O}_{K,N}^{\times}$. Применяя Утверждение 4.34 получаем существование $\alpha \in \mathcal{O}_{K,N}$, такого что $\mathrm{Nm}(\alpha) \leqslant 12\log^2(\Delta_K \mathrm{Nm}(N))$ и $\left[\frac{\alpha}{d}\right] \equiv -1 (\mathrm{mod}\, N)$. Пусть $\beta = \alpha^u$. Исходя из нечётности u получаем $\left[\frac{\beta}{d}\right] = -1$, значит, $\beta \not\equiv 1(\mathrm{mod}\, d)$. Пусть j минимальное число, такое что $\alpha^{2^j u} \equiv -1(\mathrm{mod}\, N)$. Тогда $\mathrm{ord}_{\mathcal{O}_{K,p}^{\times}}(\beta) = \mathrm{ord}_{\mathcal{O}_{K,q}^{\times}}(\beta) = 2^{j+1}$.

Далее рассмотрим следующие два случая:

Случай 1: $v_2(\mathrm{Nm}(p)-1) > v_2(\mathrm{Nm}(q)-1)$.

В этом случае $\mathrm{ord}_{\mathcal{O}_{K,q}^{\times}}(\beta) = 2^{j+1} | \varphi_K(q) = \mathrm{Nm}(q)-1$, значит

$$\mathrm{ord}_{\mathcal{O}_{K,p}^{\times}}(\beta) = 2^{j+1} | (\mathrm{Nm}(p)-1)/2. \tag{4.31}$$

Получаем, что одной стороны $\left[\frac{\beta}{d}\right] = \left[\frac{\beta}{p}\right] = -1$, с другой же $b^{(\mathrm{Nm}(p)-1)/2} \equiv 1(\mathrm{mod}\, p)$, получаем противоречие с Теоремой 3.1.

Случай 2: $v_2(\mathrm{Nm}(p)-1) = v_2(\mathrm{Nm}(q)-1)$.

В данном случае $\left[\frac{\beta}{d}\right] = \left[\frac{\beta}{q}\right]\left[\frac{\beta}{p}\right] = -1$. Без потери общности, будем считать, что $\left[\frac{\beta}{p}\right] = -1$ и $\left[\frac{\beta}{q}\right] = 1$. Согласно Теореме 3.1 получаем, что $\beta^{(\mathrm{Nm}(q)-1)/2} \equiv 1(\mathrm{mod}\, q)$ и $\mathrm{ord}_{\mathcal{O}_{K,p}^{\times}}(\beta) = \mathrm{ord}_{\mathcal{O}_{K,q}^{\times}}(\beta) | (\mathrm{Nm}(q)-1)/2$. Так как $v_2(\mathrm{Nm}(p)-1) = v_2(\mathrm{Nm}(q)-1)$, то мы имеем $\mathrm{ord}_{\mathcal{O}_{K,p}^{\times}}(\beta) | (\mathrm{Nm}(p)-1)/2$, а значит $\beta^{\frac{\mathrm{Nm}(p)-1}{2}} \equiv 1(\mathrm{mod}\, p)$, что противоречит равенству $\left[\frac{\beta}{p}\right] = -1$.

Таким образом, в обоих случаях было получено противоречие и N является простым элементом. $\otimes$

Докажем усиленный аналог критерия Эйлера:

Теорема 4.3. *Предположим, что ERH верна. Пусть $\mathfrak{n}$ – нетривиальный идеал нечётной нормы. Тогда $\mathfrak{n}$ является простым в $\mathcal{O}_K$ тогда и только тогда, когда для любого $a \in \mathcal{O}_{K,\mathfrak{n}}^{\times}$, $\mathrm{Nm}(a) \leqslant 12\log^2(\Delta_K \mathrm{Nm}(\mathfrak{n}))$, выполнено сравнение*

$$a^{(\mathrm{Nm}(\mathfrak{n})-1)/2} \equiv \left[\frac{a}{\mathfrak{n}}\right] (\mathrm{mod}\, \mathfrak{n}). \tag{4.32}$$

Доказательство.

Так как $\mathcal{O}_K$ факториально, то $\mathfrak{n}$ - главный идеал, пусть $\mathfrak{n} = (N)$.

Необходимость следует из Теоремы 3.1.

Докажем достаточность. Предположим, что $N \in \mathcal{O}_K \backslash \mathcal{O}_K^\times$ не является простым элементом нечётной нормы и для любого $a \in \mathcal{O}_{K,N}^\times$, такого что $\mathrm{Nm}(a) \leqslant 12\log^2(\Delta_K \mathrm{Nm}(N))$, выполнено $a^{(\mathrm{Nm}(N)-1)/2} \equiv \left[\frac{a}{N}\right] (\mathrm{mod}\, N)$. Введём отображение $\chi : \mathcal{O}_{K,N}^\times \to \mathcal{O}_{K,N}^\times$, такое что для любого $a \in \mathcal{O}_{K,N}^\times$ выполняется $\chi(a) = a^{(\mathrm{Nm}(N)-1)/2}\left[\frac{a}{N}\right]$. Отметим, что χ является эндоморфизмом группы $\mathcal{O}_{K,N}^\times$. Из Теоремы 3.1 следует, что χ нетривиален. Применяя Утверждение 4.34 получаем, что существует $\alpha \in \mathcal{O}_{K,N}$, такое что $\mathrm{Nm}(\alpha) \leqslant 12\log^2(\Delta_K \mathrm{Nm}(N))$ и $\alpha^{(\mathrm{Nm}(N)-1)/2}\left[\frac{\alpha}{N}\right] \not\equiv 1 (\mathrm{mod}\, N)$. Получаем противоречие с предположением.

Следовательно, N является простым элементом кольца $\mathcal{O}_K$. $\otimes$

Далее рассмотрим детерминированный аналог теста Миллера-Рабина на основе ERH. Предполагаем, что $\mathcal{O}_K$ факториально, а значит все нетривиальные идеалы можно отождествлять с элементами кольца $\mathcal{O}_K$.

Пусть $\varepsilon_1, \ldots, \varepsilon_h$ фундаментальные единицы K.

Определение 4.21. Пусть $N \in \mathcal{O}_K \backslash \mathcal{O}_K^\times$ элемент нечётной нормы. Пусть $a \in \mathcal{O}_K, (a,N) = 1$ и $a^u \not\equiv 1 (\mathrm{mod}\ N)$. Будем говорить, что a свидетель простоты N, если для любого $b \in \{\varepsilon_1^{k_1} \ldots \varepsilon_h^{k_h} a, |k_i| \leqslant \Phi\lceil \log_2(Ml(N))\rceil\}$ существует $k \in \{0, \ldots, t-1\}$, такое что $b^{2^k u} \equiv -1 (\mathrm{mod}\ N)$, где $\mathrm{Nm}(N) - 1 = 2^t u, (u,2) = 1$.

Если $h = 0$, то a будем называть свидетелем простоты, если $\exists k \in \{0, \ldots, t-1\}$ такое что $a^{2^k u} \equiv -1 (\mathrm{mod}\ N)$, где $\mathrm{Nm}(N) - 1 = 2^t u, (u,2) = 1$.

Теорема 4.4. *Предположим ERH выполнена. Пусть $N \in \mathcal{O}_K \backslash \mathcal{O}_K^\times$ элемент нечётной нормы. Тогда следующие утверждения эквивалентны.*

1. *N простое число.*
2. *$\forall a, (a,N) = 1, l(a) \leqslant A\log^{2/n} l(N) + B, a^u \not\equiv 1 (\mathrm{mod}\, N)$: a - свидетель простоты N.*

где $\mathrm{Nm}(N) - 1 = 2^t u, (u,2) = 1$, A и B константы зависящие только от K и E.

Доказательство.

Необходимость следует из ранее доказанных результатов.

Предположим, что (2) выполнено, но N не простое. Тогда существует b, такое что $(b,N) = 1$, $b^u \not\equiv 1(\mathrm{mod}\, N)$, $\mathrm{Nm}(b) \leqslant 12\log^2(\Delta_K \mathrm{Nm}(N))$ и $b^{2^k u} \not\equiv -1(\mathrm{mod}\ N)$ для любого и $k \in \{0,\ldots,t-1\}$.Тогда найдётся $a = \varepsilon_1^{k_1}\ldots\varepsilon_h^{k_h} b$, где $|k_i| \leqslant \Phi\lceil\log_2(Ml(N))\rceil$, такое что a является Δ-сбалансированным. В частности, $\mathrm{Nm}(a) = \mathrm{Nm}(b)$.

Заметим, что

$$l(a) \leqslant \Gamma\Delta\sqrt[n]{\mathrm{Nm}(a)} \leqslant \Gamma\Delta\sqrt[n]{12\log^2(\Delta_K \mathrm{Nm}(N))} \leqslant A\log^{2/n} l(N) + B. \quad (4.33)$$

Не нарушая общности, a такое что $l(a) \leqslant Ml(N)$. Но a не является свидетелем простоты, что противоречит (2).

$\otimes$

Замечание 4.5. Предположим, что мы знаем фундаментальные единицы K и константы A и B(они могут быть легко вычислены, если мы знаем константы Γ,Δ,Φ). Таким образом, проверка простоты $N \in \mathcal{O}_K$ может быть выполнена за полиномиальное время, а именно $\widetilde{O}(\log^{4+h} l(N))$, в предположении ERH.

Таким образом, было получено доказательство того, что задача тестирования на простоту принадлежит классу $\mathcal{P}$ в классе факториальных колец в предположении ERH.

Замечание 4.6. Отметим, что данные результаты могут быть использованы для генерации простых идеалов в кольцах целых алгебраических элементов числовых полей.

Рассмотрим 2-представление идеалов: $\mathfrak{p} = (a,\alpha)_2, a \in \mathbb{N}, \alpha \in \mathcal{O}_K$, причём $\alpha = \sum\limits_{i=1}^{n} \alpha_i e_i$. Выберем $l_i, r_i, l_i < r_i, i = \overline{0,n}$, пусть $\rho = \max\{\max\limits_{i=\overline{0,n}} |r_i|, \max\limits_{i=\overline{0,n}} |l_i|\}$. Рассмотрим множество идеалов, таких что $l_0 \leqslant a \leqslant r_0, l_i \leqslant \alpha_i \leqslant r_i, i = \overline{1,n}$.

К каждому идеалу из данного множества можно применить вероятностный аналог теста Миллера-Рабина, тем самым отсеяв значительную часть составных идеалов. Пусть мы применяем k итераций данного теста к каждому идеалу. Тогда затратив время $\tilde{O}\left(k\log^2\rho\prod\limits_{i=0}^{n}|r_i - l_i|\right)$ мы отсеем часть составных идеалов из рассматриваемого множества. Остальные могут быть проверены на простоту с помощью каких-либо детерминированных тестов, например полученного выше.

ГЛАВА 5.
КООРДИНАТНЫЕ КОЛЬЦА

5.1 Координатные кольца

Определение 5.1. Кольцо $C_f = \mathbb{F}[x,y]/(f)$, где $f \in F[x,y]$ будем называть координатным кольцом кривой f.

Далее будем рассматривать лишь несингулярные кривые, то есть такие кривые, что одна из формальных производных в любой точке $(x,y) \in \mathbb{F}^2$ не равна 0.

Как уже было сказано в Замечании 2.2 координатные кольца несингулярных кривых над конечным полем являются примерами абстрактных числовых колец.

Замечание 5.1. Приведём несколько классических примеров координатных колец.

Рассмотрим прямую $f(x,y) = y - kx - b$. Нетрудно видеть, что координатное кольцо C_f изоморфно кольку многочленов от одной переменной $\mathbb{F}[t]$.

Аналогичный результат может быть получен для координатного кольца параболы $f(x,y) = y - x^2$.

В это же время, координатные кольца гиперболы $f(x,y) = xy - 1$ и окружности $g(x,y) = x^2 + y^2 - 1$ имеют менее тривиальный вид.

5.2 Кольцо многочленов от одной переменной

Как видно из примеров выше, часто координатные кольца несингулярных кривых оказываются изоморфны кольцам многочленов от одной переменной, в частности, $\mathbb{F}[x]$ является абстрактным числовым кольцом для конечного $\mathbb{F}$.

В данной главе мы исследуем применимость Алгоритма 1 в кольце многочленов одной переменной. Отметим, что $\mathbb{F}[x]$ является евклидовым, а значит областью главных идеалов, к тому же, оно является факториальным, а значит любой идеал однозначно задаётся порождающим многочленом и мы можем,

не нарушая общности, исследовать простоту элементов кольца, вместо идеалов.

В данном параграфе мы получим алгоритмы для выполнения необходимых операций и оценим их сложность.

Будет предполагать, что элементы поля $\mathbb{F}_q \simeq \mathbb{Z}_p[x]/(f)$ представлены многочленами с коэффициентами - многочленами степени не выше α с коэффициентами из $\mathbb{Z}_p$. Под операциями в $\mathbb{F}_q[x]$ или $\mathbb{Z}$ будем понимать сложение, вычитание, умножение и деление с остатком в соответствующем кольце. Под операциями в произвольном кольце R будем понимать сложение и умножение.

Для начала рассмотрим операции сложения и вычитания многочленов над конечным полем.

Утверждение 5.1. *Операция сложения/вычитания многочленов $f, g \in \mathbb{F}_q, \deg f, \deg g \leqslant n$ могут быть выполнены за $O(n)$ операций в поле $\mathbb{F}_q$ и $O(\alpha n)$ операций в $\mathbb{Z}$, причём данная оценка является асимптотически точной.*

Доказательство. Нетрудно видеть, что достичь такой сложности с помощью алгоритма сложения/вычитания многочленов столбиком. Точность оценки следует их необходимой сложности считывания входных данных алгоритма. $\otimes$

Далее сведём задачу о делении многочленов с остатком к задаче перемножения многочленов.

Отметим, что кольцо $K[x]$, где K – поле, является Евклидовым, то есть для любой пары многочленов $f, g \in K[x]$ найдётся единственная пара многочленов $q, r \in K[x]$, что выполнено равенство $f = qg + r$, причём $\deg r < \deg g$. В данной части, покажем, что задача о нахождении q, r по паре $f, g, \deg f, \deg g \geqslant 1$ сводится к задаче перемножения многочленов и асимптотические сложности данных задач совпадают.

Определение 5.2. Пусть $f = \sum\limits_{i=0}^{n} c_i x^i, \deg f = n$. Тогда $Rev(f)$ определим как $Rev(f) = \sum\limits_{i=0}^{n} c_{n-i} x^i$.

Утверждение 5.2. *Верно следующее:*

1. *Свободный член $Rev(f)$ всегда ненулевой.*
2. *$\deg f \geqslant \deg Rev(f)$, причём равенство выполнено тогда и только тогда, когда свободный член f отличен от нуля.*

3. $Rev(Rev(f)) = f$ *тогда и только тогда, когда свободный член* f *отличен от нуля.*
4. $Rev(f) = x^{\deg f} f\left(\frac{1}{x}\right)$.
5. $Rev(fg) = Rev(f)Rev(g)$.
6. $Rev(f+g) = Rev(f) + x^{\deg f - \deg g} Rev(g)$, *если* $\deg f \geqslant \deg g$.

Доказательство. Первые четыре свойства следуют непосредственно из определения. Пятое свойство верно так как

$$Rev(fg) = x^{\deg f + \deg g} f\left(\frac{1}{x}\right) g\left(\frac{1}{x}\right) = Rev(f)Rev(g).$$

Шестое свойство также можно проверить исходя из определения.

$\otimes$

Лемма 5.1. *Пусть* $f, g, q, r \in \mathbb{F}_q[x]$, *причём* $f = gq + r$ *и* $\deg r < \deg g < \deg f$. *Тогда выполнено*

$$Rev(q) = Rev(g)^{-1} Rev(f) (\mathrm{mod}\, x^{\deg f - \deg g}).$$

Доказательство. Исходя из Утверждения 5.2 имеем

$$Rev(f) = Rev(q)Rev(g) + x^{\deg f - \deg r} Rev(r).$$

Исходя из того, что $\deg r < \deg g$ получаем сравнение:

$$Rev(f) \equiv Rev(q)Rev(g) (\mathrm{mod}\, x^{\deg f - \deg g}).$$

Отметим, что $Rev(g)$ имеет ненулевой свободный член исходя из Утверждения 5.2, а значит $(Rev(g), x^l) = 1$ для любого $l \geqslant 0$, а значит существует обратный элемент по модулю x^l. Отсюда получаем, что

$$Rev(q) \equiv Rev(f)Rev(g)^{-1} (\mathrm{mod}\, x^{\deg f - \deg g}).$$

$\otimes$

Лемма 5.2. *Пусть* $fh \equiv 1 (\mathrm{mod}\, x^l)$, *причём*

$$h = h_0 + h_1 x^l,$$

$$fh_0 = 1 + ax^l.$$

Тогда для $g = f + x^l b$, *где* $b \equiv -f(a + fb) (\mathrm{mod}\, x^{2l})$ *выполнено* $gh \equiv 1 (\mathrm{mod}\, x^{2l})$.

Доказательство.

Требуется найти такое b, что выполнено

$$1 \equiv (a + x^l b)(h_0 + x^l b) \equiv ah_0 + x^l(bh_0 + ah_1) \equiv 1 + x^l(c + bh_0 + ah_1)(\mathrm{mod}\, x^{2l}).$$

Данное равенство равносильно тому, что

$$b \equiv -h_0^{-1}(a + fb) \equiv -f(a + fb)(\mathrm{mod}\, x^l).$$

$\otimes$

Утверждение 5.3. *Операция деления с остатком двух многочленов f, g в кольце $K[x]$ может быть выполнена за асимптотически такое же число операций как и их умножение.*

Доказательство.

Отметим, что легко разобрать случаи, когда степень одного из многочленов нулевая или $\deg f \leqslant \deg g$. В противном случае Лемма 5.1 сводит за конечное число операций в $K[x]$ задачу нахождения остатка к нахождению $Rev(g)^{-1}$ по модулю $x^{\deg f - \deg g}$, это следует из факта, что $\deg q = \deg f - \deg g$. Последняя задача может быть эффективно решена с помощью Леммы 5.2. А именно, верно следующее неравенство

$$T(l) \leqslant C_1 M(l) + C_2 l + T(l/2),$$

где $T(l)$ – число операций в $K[x]$ для нахождения обратного к многочлену по модулю x^l, $M(l)$ – число операций в $K[x]$ для перемножения двух многочленов степеней не выше x^l, C_1, C_2 – некоторые положительные константы. Можно предположить, что $M(l)$ является строго возрастающей функцией, причём $l \leqslant M(l) \leqslant l^2$, что позволяет получить из рекуррентного неравенства, что $T(l) = O(M(l))$, из чего и следует утверждение.

$\otimes$

Далее рассмотрим операцию перемножения двух многочленов над конечным полем.

Существует ряд оценок умножения многочленов над кольцом. В частности, в [31] приводится следующий результат.

Утверждение 5.4. *Перемножение двух многочленов степени не более n над кольцом R может быть выполнено за $O(n \log n \log\log n)$ операций в R, причём константы в O не зависят от кольца R.*

Далее для удобства обозначить за $M(n)$, такую величину что перемножение двух многочленов над $\mathbb{F}$ степеней не превосходящих n равно $O(M(n))$ операций в $\mathbb{F}[x]$, а за $O(M(\alpha, n))$, такую величину, что перемножение двух многочленов над $\mathbb{F}_q[x]$ степеней не превосходящих n равно $O(M(n))$ операций в $\mathbb{Z}$.

Утверждение 5.5. *Выполнены следующие асимптотические равенства:*

$$M(n) = O(n \log\log\log n),$$

$$M(n, \alpha) = O(M(n)M(\alpha)) = O(n\alpha \log n \log\alpha \log\log n \log\log\alpha).$$

Доказательство.

Первая часть утверждения следует из Предложения 5.4. Дабы доказать вторую, требуется показать, что операции в $\mathbb{F}_q$ могут быть выполнены за $O(M(\alpha))$ операций в $\mathbb{Z}$. Действительно, сложение $a, b \in \mathbb{F}_q$ равносильно сложению двух многочленов над $\mathbb{Z}_p$ степеней не выше α и взятие остатка по модулю некоторого многочлена f степени α. Из утверждений выше это может быть выполнено за $O(M(\alpha))$ операций. Аналогичные результаты для вычитания, умножения и нахождения обратного могут быть получены схожим образом.

$\otimes$

Следствие 5.1. С помощью бинарного алгоритма возведения в степень вычисление $g^k \pmod f$, где $k \in \mathbb{N}, f, g \in \mathbb{F}_q[x], \deg g, \deg g \leqslant n$, может быть выполнено за $O(M(n)\log k)$ операций в $\mathbb{F}_q$ и $O(M(n)M(\alpha)\log k)$ операций в $\mathbb{Z}$.

Далее непосредственно рассмотрим аналог теста Миллера-Рабина в кольце многочленов:

Далее будем предполагать, что идеал $\mathfrak{f}$ подаваемый на вход алгоритму представляется с помощью многочлена $f \in \mathbb{F}[x]$, такого что $\mathfrak{f} = (f)$.

Алгоритм 3. Вход: Многочлен $f \in \mathbb{F}[x]$, требуется определить является ли идеал $\mathfrak{f} = (f)$ простым.

1. Вычислить $\mathrm{Nm}(\mathfrak{f}) = q^{\deg f}$, а также такие u, t, что $\mathrm{Nm}(\mathfrak{f}) - 1 = 2^t u, (u, 2) = 1$.
2. Выбрать случайное $a \in \mathbb{F}[x]/(f)$.

3. Вычислить $r_0 \equiv a^u (\mathrm{mod}\, f)$. Если $r_0 \equiv \pm 1 (\mathrm{mod}\, f)$ алгоритм останавливается с ответом 'неизвестно', в противном случае продолжает работу.
4. Последовательно для каждого $j \in \{1, \ldots, t-1\}$ вычислить $r_j \equiv r_{j-1}^2 (\mathrm{mod}\, f)$.
5. Если некоторое $r_j \equiv -1 (\mathrm{mod}\, f)$, то алгоритм останавливается с ответом 'неизвестно', если такого j не нашлось, то ответ 'ƒ не является простым'.

Утверждение 5.6. *Алгоритм 3 для $f \in \mathbb{F}_q[x], \deg f \leqslant n$, может быть выполнен за*

$$O(M(n) n \alpha \log p)$$

операций в $\mathbb{F}_q$ и $\mathbb{Z}$, и за

$$O(M(n) M(\alpha) n \alpha \log p),$$

операций в $\mathbb{Z}$.

Доказательство. Шаг 1 требует $O(\alpha n \log p)$ операций в $\mathbb{Z}$. Шаг 2 требует $O(1)$ операций. Шаг 3 требует $O(M(n)M(\alpha)n\alpha \log p)$ операций в $\mathbb{Z}$. Шаги 4-5 также требуют $O(M(n)M(\alpha)n\alpha \log p)$ операций в $\mathbb{Z}$. Аналогичным образом получается результат при подсчёта операций в $\mathbb{F}_q$ и $\mathbb{Z}$. $\otimes$

5.3 Способы представления идеалов

В данной главе мы рассмотрим координатное кольцо C_f произвольной несингулярной кривой и способы задания идеалов в указанном абстрактном числовом кольце.

Для этого требуется ввести понятия базиса Грёбнера[32].

Рассмотрим кольцо $R = \mathbb{F}[x_1, \ldots, x_n]$ многочленов от n переменных над полем $\mathbb{F}$. Оно является Нётеровым и любой идеал в нём может быть записать в виде конечного порождающего множества: $\mathfrak{I} \subset R, \mathfrak{I} = (f_1, f_2, \ldots, f_n)$.

Определение 5.3. Пусть у нас есть лекфикографический порядок на переменных: $x_i \prec x_j$, тогда и только тогда, когда $i < j$.

Тогда можно ввести порядок на мономах из кольца R.

$$\lambda x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n} \prec \mu x_1^{\beta_1} x_2^{\beta_2} \ldots x_n^{\beta_n}$$

тогда и только тогда, когда $\sum\limits_{i=1}^{n} \alpha_i > \sum\limits_{i=1}^{n} \beta_i$ или $\sum\limits_{i=1}^{n} \alpha_i = \sum\limits_{i=1}^{n} \beta_i$ и существует $j \in \{1, 2, \ldots, n\}$, что

$$\alpha_k = \beta_k, k \leqslant j,$$

$$\alpha_j > \beta_j.$$

Замечание 5.2. Нетрудно видеть, что это отношение полного порядка на множестве мономов с фиксированным коэффициентом.

Замечание 5.3. Для поля $\mathbb{F}[x, y]$ будем считать, что $y \prec x$.

Определение 5.4. Для многочлена $p \in R$ старшим членом будет называть моном p_C, который является наибольшим среди мономов p по вышеописанному порядку.

Определение 5.5. Базисом Грёбнера для идеала $\mathfrak{I} \subset R$ будем называть такое порождающее множество $\{f_1, f_2, \ldots, f_n\}$, что $h \in R$ принадлежит $\mathfrak{I}$ тогда и только тогда, когда h_C делится на некоторое f_{jC}. Также будем считать, что f_i является приведённым.

Определение 5.6. Базис Грёбнера $I = (f_1, f_2, \ldots, f_n)$ будем называть редуцированным, если ни один моном многочлена f_i не делится на старший моном многочлена f_j для всех $i, j \in \{1, 2, \ldots, n\}$ и $i \neq j$.

Утверждение 5.7. *Для любого идеала $\mathfrak{I} \subset R$ редуцированный базис Грёбнера определён однозначно с точностью до домножения элементов базиса на элементы поля $\mathbb{F}$.*

Утверждение 5.8. *Существует полиномиальный алгоритм, который по базису Грёбнера для идеала находит его редуцированный базис Грёбнера.*

Далее опишем представление идеалов координатного кольца $C_f = \mathbb{F}[x, y]/(f)$ для несингулярной кривой f. Пусть $\mathfrak{I}$ – идеал C_f, тогда

$$C_f/\mathfrak{I} = \mathbb{F}[x, y]/((f) \cup \mathfrak{I}),$$

где $(f) \cup \mathfrak{I}$ – идеал кольца $\mathbb{F}[x,y]$. Все модулярные операции, то есть операции по модулю $\mathfrak{I}$ можно рассматривать как операции в $C_f/\mathfrak{I}$, то есть в $\mathbb{F}[x, y]/((f) \cup \mathfrak{I})$. Это позволяет нам перейти от идеала кольца C_f со сложным строением к идеалу более простого кольца $\mathbb{F}[x, y]$. Таким образом, далее

под представлением идеала $\mathfrak{I}$ будем понимать редуцированный базис Грёбера идеала $(f) \cup \mathfrak{I}$ кольца $\mathbb{F}[x, y]$, в частности, будет предполагать, что на вход алгоритмам идеалы подаются именно с помощью такого способа записи. Под размером записи идеала $\mathfrak{I}$ кольца C_f будем подразумевать размер записи его представления(то есть просто конечного набора многочленов), данную величину будем обозначать за $l(\mathfrak{I})$.

По описанным выше причинам далее мы часто будем работать с фактор-кольцом $\mathbb{F}[x, y]/\mathfrak{I}$ для некоторого идеала $\mathfrak{I}$ кольца $\mathbb{F}[x, y]$ вместо фактор-кольца $C_f/\mathfrak{J}$ для некоторого идеала $\mathfrak{J}$ кольца C_f.

Далее для простоты и точности условимся использовать следующую терминологию. Будем говорить, что элемент $g \in R/\mathfrak{J}$, где K – кольцо, $\mathfrak{J}$ – идеал R, имеет представителя/представлен f, если $g = f + \mathfrak{J}$, f будем называть представителем g.

Будем говорить, что элементы $f, g \in R$ эквивалентны в $R/\mathfrak{J}$, если $f - g \in \mathfrak{J}$. Часто не будет указываться относительно какого фактор-кольца элементы эквивалентны. Нетрудно видеть, что это действительно отношение эквивалентности.

Будем говорит, что $R/\mathfrak{J}$ имеет описание/описывается $A \subset R$, если элементы A попарно неэквивалентны в $R/\mathfrak{J}$ и для любого элемента $R/\mathfrak{J}$ найдётся представитель в A.

5.4 Необходимые операции

В данном параграфе исследуем выполнение операций(за исключением операции вычисления нормы) необходимых для реализации Алгоритма 1 в координатном кольце.

Пусть далее $\mathbb{F}$ – конечное поле, $\mathbb{F}[x, y]$ – кольцо многочленов от двух переменных над полем $\mathbb{F}$, $C_f = F[x,y]/(f)$ – координатное кольцо алгебраической несингулярной кривой $f \in \mathbb{F}[x,y]$.

Лемма 5.3. *Фактор-кольцо $\mathbb{F}[x,y]/\mathfrak{I}$, где $\mathfrak{I}$ – идеал $\mathbb{F}[x,y]$, является векторным пространством над полем $\mathbb{F}$.*

Доказательство. Заметим, что операции сложения и умножения на скаляр из поля определены корректно: $(a + I) + (b + I) = (a + b) + I$ и

$\lambda(a + I) = \lambda a + I$. Все остальные аксиомы векторного пространства следуют из аксиом кольца и поля.

$\otimes$

Замечание 5.4. Если фактор-кольцо $\mathbb{F}[x,y]/\mathfrak{I}$ конечно, то оно является конечномерным векторным пространством.

Лемма 5.4. *Если фактор-кольцо $\mathbb{F}[x, y]/\mathfrak{I}$ конечно, то $\mathfrak{I} \cap \mathbb{F}[x] \neq \emptyset$ и $\mathfrak{I} \cap \mathbb{F}[y] \neq \emptyset$.*

Доказательство. Предположим, что $\mathfrak{I} \cap \mathbb{F}[x] = \emptyset$. Тогда элементы $\{x^n + I | n \in \mathbb{N}\}$ являются попарно различными в $\mathbb{F}[x,y]/\mathfrak{I}$, а также образуют бесконечную линейно независимую систему векторов в $\mathbb{F}[x,y]/\mathfrak{I}$, что противоречит его конечномерности.

$\otimes$

Лемма 5.5. *Если фактор-кольцо $\mathbb{F}[x, y]/\mathfrak{I}$ конечно, то в базисе Грёбнера для $\mathfrak{I}$ найдутся два многочлена f и g, такие что $f_C = x^n$ и $g_C = y^m$. Если базис Грёбнера является редуцированным, то для любого элемента $f' \neq f$ базиса Грёбнера верно $\deg_x f' < n$ и для любого элемента $g' \neq g$ базиса Грёбнера верно $\deg_y g' < m$.*

Доказательство. Исходя из предыдущей леммы существует $p(x) \in \mathbb{F}[x] \cap \mathfrak{I}$. Исходя из определения базиса Грёбнера p_C должен делиться на старший моном какого-то из многочленов базиса Грёбнера. Так как p_C имеет вид λx^k, такой старший моном должен содержать только степени x, а значит найдётся необходимый элемент f базиса Грёбнера. Аналогично строится элемент g.

Пусть теперь базис Грёбнера является редуцированным. По определению, никакой моном элемента базиса Грёбнера не делится на $f_C = x^n$, значит для любого $f \neq f'$ выполнено неравенство $\deg_x f' < n$. Аналогичным образом доказывается неравенство для y.

$\otimes$

Следствие 5.2. 1. Рассмотрим фактор-кольцо $C_f/\mathfrak{I}$, где $\mathfrak{I}$ – идеал координатного кольца C_f. Данное факторкольцо может быть рассмотрено как кольцо $\mathbb{F}[x,y]/(\mathfrak{I} \cup (f))$. Из результатов выше следует, что редуцированный базис Грёбнера для $\mathfrak{I} \cup (f)$ будет содержать элементы $f, g \in \mathbb{F}[x,y]$, такие что $f_C = x^n, g_C = y^m$ и для любого монома(за исключением f_C) элемента базиса Грёбнера степень x меньше n, и для

любого монома(за исключением g_C) элемента базиса Грёбнера степень y меньше m.

2. Пусть далее $\mathfrak{J} = \mathfrak{I} \cup (f)$, $R = \mathbb{F}[x,y]/(\mathfrak{I} \cup (f)) = \mathbb{F}[x,y]/\mathfrak{J}$. Проверка равенства $a = b \mod \mathfrak{J}$ в R равносильна проверке $a - b = 0 \mod \mathfrak{J}$ и может быть выполнены с помощью алгоритма редукции описанного в [32].
3. Пусть a является элементом $\mathbb{F}[x,y]$, требуется найти $b \in \mathbb{F}[x,y]$, такое что $a = b \mod \mathfrak{J}$ и $\deg_x b, \deg_y b$ были ограничены некоторыми параметрами редуцированного базиса Грёбнера для $\mathfrak{J}$.

   Пусть $\lambda x^i y^j$ – моном a, такой что $i \geqslant n$. Тогда рассмотрим $\hat{a} = a - \lambda x^{n-i} y^j f(x)$. Нетрудно видеть, что $a = \hat{a} \mod \mathfrak{J}$. Повторяя такую процедуру для всех вышеописанных мономов получим $c \in \mathbb{F}[x,y]$, такое что $a = c \mod \mathfrak{J}$ и $\deg_x c \leqslant n-1$.

   Далее проделаем такую же процедуру для степеней y и элемента g и получим $d \in \mathbb{F}[x,y]$, такой что $a = d \mod \mathfrak{J}$, причём $\deg_x d \leqslant 2n-2$ и $\deg_y d \leqslant m-1$.

   Нетрудно видеть, что данная процедура имеет сложность порядка $O(l(\mathfrak{I}) + \deg_x b \cdot \deg_y b)$.
4. Из рассуждений выше следует оценки на порядок кольца $\mathbb{F}[x,y]/\mathfrak{J}$:

$$|\mathbb{F}[x,y]/\mathfrak{J}| \leqslant |\mathbb{F}|^{2\min(m,n)+\max(m,n)-3}.$$

Таким образом, нетрудно видеть, что все необходимые для Алгоритма 1 операции, за исключением вычисления нормы идеала, могут быть выполнены за полиномиальное время.

5.5 Вычисление нормы

В данном разделе нами будут исследованы вопросы нахождения нормы идеала по его представлению. Исходя из определения представления идеала, нас интересует вычисление $|\mathbb{F}[x,y]/\mathfrak{I}|$ по известному редуцированному базису Грёбнера для идеала $\mathfrak{I}$.

Продемонстрируем описанную технику на ряде примеров:

1. Пусть $\mathfrak{I} = (y^3 + y)$. Тогда $\mathfrak{J} = (y^3 + y, x^2 + y^2 + 1)$, с помощью Sage проверяем, что это представление также является редуцированным базисом

Грёбнера для $\mathfrak{J}$.

Отметим, что для любого элемента $\mathbb{Z}_2[x,y]/\mathfrak{J}$ существует представитель $f \in \mathbb{Z}_2[x,y]$, такой что $\deg_x f \leqslant 1$. Пусть $x^i y^j, i \leqslant 1$ – некоторый моном f, что $j \geqslant 3$. Тогда многочлен f эквивалентен в $\mathbb{Z}_2[x,y]/\mathfrak{I}$ многочлену $f - x^i y^{j-3}(y^3+y) = f - x^i y^j - x^i y^{j-2}$. Повторяя аналогичную процедуру получаем, что f эквивалентен некоторому многочлену $\hat{f}$, такому что $\deg_x f \leqslant 1, \deg_y f \leqslant 2$. То есть каждый элемент $\mathbb{Z}_2[x,y]/\mathfrak{I}$ имеет представителя в следующем множестве

$$\{a_1 + a_2 y + a_3 x + a_4 y^2 + a_5 xy + a_6 y^2 x | a_i \in \mathbb{Z}_2\},$$

Предположим, что какие-то два элемента вышеописанного множества совпадают. Из этого следует, что в множестве есть ненулевой многочлен, который является элементом идеала $\mathfrak{J}$, отсюда получаем противоречие исходя из определения базиса Грёбнера. Таким образом, $|\mathbb{Z}_2[x,y]/\mathfrak{I}| = 64$.

2. Пусть $\mathfrak{I} = (xy)$. Тогда $\mathfrak{J} = (x^2+y^2+1, xy)$. Вычислим редуцированный базис Грёбнера для $\mathfrak{J}$ с помощью Sage:

$$\mathfrak{J} = (y^3+y, x^2+y^2+1, xy).$$

Заметим, что каждый элемент $\mathbb{Z}_2[x,y]/\mathfrak{J}$ имеет представителя в множестве

$$\{a_1 + a_2 y + a_3 x + a_4 y^2 + a_5 xy + a_6 y^2 x | a_i \in \mathbb{Z}_2\},$$

что следует из предыдущего пункта, где был рассмотрен идеал порождённый подбазисом $\mathfrak{J}$ – (y^3+y, x^2+y^2+1).

Далее, если ввести в рассмотрение xy, получаем, что значения коэффициентов при xy и y^2x не играют роли. Таким образом, $\mathbb{Z}_2[x,y]/\mathfrak{J}$ может быть записано с помощью следующих представителей

$$\{a_1 + a_2 y + a_3 x + a_4 y^2 | a_i \in \mathbb{Z}_2\}.$$

Аналогично предыдушему пункту получаем, что это и есть описание $\mathbb{Z}_2[x,y]/\mathfrak{J}$ и $|\mathbb{Z}_2[x,y]/\mathfrak{I}| = 16$.

3. Пусть $\mathfrak{I} = (x^2+y)$. Тогда $\mathfrak{J} = (x^2+y, x^2+y^2+1)$. Вычислим редуцированный базис Грёбнера с помощью Sage:

$$\mathfrak{J} = (x^2+y, y^2+y+1).$$

Пользуясь рассуждения аналогичными первому пункту мы можем получить, что для любого $f \in \mathbb{Z}_2[x,y]/\mathfrak{I}$ есть представитель $\hat{f} \in \mathbb{Z}_2[x,y]$, что $\deg_x f \leqslant 1, \deg_y f \leqslant 1$, то есть

$$\{a_1 + a_2 y + a_3 x + a_4 xy | a_i \in \mathbb{Z}_2\},$$

нетрудно видеть, что все они различны в $\mathbb{Z}_2[x,y]/\mathfrak{I}$ исходя из определения базиса Грёбнера. Таким образом, $|\mathbb{Z}_2[x,y]/\mathfrak{I}| = 16$.

4. Пусть $\mathfrak{I} = (y^3 + y^2 + x + 1)$. Тогда $\mathfrak{J} = (y^3 + y^2 + x + 1, x^2 + y^2 + 1)$. С помощью Sage проверяем, что это действительно редуцированный базис Грёбнера для $\mathfrak{J}$.

   Заметим, что для любого элемента $\mathbb{Z}_2[x,y]/\mathfrak{I}$ существует представитель $f \in \mathbb{Z}_2[x,y]$, что $\deg_x f \leqslant 1$. Пусть $x^i y^j, i \leqslant 1$ – моном f, такой что $j \geqslant 3$. Тогда многочлен f эквивалентен многочлену $f - x^i y^{j-3}(y^3 + y^2 + x + 1)$. Повторяя такую процедуру для каждого монома с $j \geqslant 3$ получаем многочлен g эквивалентный f, такой что $\deg_x f \leqslant 2$ и $\deg_y f \leqslant 2$. Далее заметим, что

$$x^2 = 1 + y^2 \mod \mathfrak{J},$$

$$x^2 y = y(1 + y^2) = y^3 + y = y^2 + y + x + 1 \mod \mathfrak{J},$$

$$x^2 y^2 = y^2(1 + y^2) = y^4 + y^2 = y^3 + y^2 + xy + y = xy + y + x + 1 \mod \mathfrak{J}.$$

   Значит каждый элемент $\mathbb{Z}_2[x,y]/\mathfrak{I}$ имеет представителя $f \in \mathbb{Z}_2[x,y]$ с $\deg_y f = 2, \deg_x f = 1$, то есть все представители лежат в множестве

$$\{a_1 + a_2 y + a_3 x + a_4 y^2 + a_5 xy + a_6 y^2 x | a_i \in \mathbb{Z}_2\},$$

   Далее исходя из определения базиса Грёбнера получаем, что все элементы данного множества попарно не эквивалентны и $|\mathbb{Z}_2[x,y]/\mathfrak{I}| = 64$.

5. Пусть $\mathfrak{I} = (x + y + xy)$. Тогда $\mathfrak{J} = (x + y + xy, x^2 + y^2 + 1)$. С помощью Sage находим редуцированный базис Грёбнера:

$$\mathfrak{J} = (y^3 + y^2 + x + 1, x^2 + y^2 + 1, x + y + xy)$$

   Пользуясь результатами прошлого пункта замечаем, что каждый элемент $\mathbb{Z}_2[x,y]/\mathfrak{I}$ имеет представителя $f \in \mathbb{Z}_2[x,y]$, такого что $\deg_x f \leqslant 1, \deg_y f \leqslant 2$. Пользуясь тем, что теперь у нас в базисе есть элемент $x + y + xy$ получаем, что каждый элемент $\mathbb{Z}_2[x,y]/\mathfrak{I}$ имеет представителя f, такого что $\deg_x f \leqslant 1, \deg_y f \leqslant 2$ и коэффициенты при xy и xy^2

равны 0, так как

$$xy = x + y \mod \mathfrak{J},$$

$$xy^2 = xy + y^2 = x + y + y^2 \mod \mathfrak{J}.$$

То есть все представители элементов $\mathbb{Z}_2[x,y]/\mathfrak{I}$ лежат в множестве

$$\{a_1 + a_2y + a_3x + a_4y^2 | a_i \in \mathbb{Z}_2\},$$

причём из определения базиса Грёбнера следует, что это и есть описание $\mathbb{Z}_2[x,y]/\mathfrak{I}$ и $|\mathbb{Z}_2[x,y]/\mathfrak{I}| = 16$.

Порой эту идею можно обобщить на более широкий круг идеалов.

Некоторые результаты можно обобщить на более широкий круг идеалов. Например, в координатном кольце окружности для главных идеалов вида $(p(x))$ или $(p(y))$ норма может быть вычислена следующим образом:

Утверждение 5.9. *Пусть идеал $\mathfrak{I} \subset K$ обладаем тем свойством, что $\mathfrak{J}$ имеет редуцированный базис Грёбнера вида $(p(x), x^2 + y^2 + 1)$, где $p \in \mathbb{Z}_2[x]$. Тогда $|K/\mathfrak{I}| = |\mathbb{Z}_2[x,y]/\mathfrak{J}| = 2^{2\deg p}$.*

Доказательство.

Заметим, что любой элемент $K/\mathfrak{I}$ имеет представителя $f \in \mathbb{Z}_2[x,y]$, такого что $\deg_y f \leqslant 1$. Пусть $x^i y^j, j \leqslant 1$ моном многочлена f, такой что $i \geqslant \deg p$. Тогда f эквивалентен моному $f - x^{i-\deg p} y^j p(x)$. Повторяя данную процедуру для всех мономов f с $i \geqslant \deg p$ получаем, что любой элемент $K/\mathfrak{I}$ эквивалентен $g \in \mathbb{Z}_2[x,y]$ с $\deg_x g \leqslant \deg p - 1, \deg_y g \leqslant 1$. Далее из определения базиса Грёбнера следует, что это и есть всё описание $K/\mathfrak{I}$, в частности $|K/\mathfrak{I}| = 2^{2\deg p}$.

$\otimes$

Замечание 5.5. Таким образом, для вышеописанных идеалов в кольце окружности можно применять аналог теста Миллера-Рабина, причём, как нетрудно видеть, сложность будет порядка $O(\log^3 l(\mathfrak{I}))$ бинарных операций.

Далее сформулируем гипотезу, которая подтверждается результатами полученными выше.

Гипотеза 2. Пусть $\mathfrak{J}$ – идеал $\mathbb{F}[x,y]$, редуцированный базис Грёбнера для которого имеет вид (f,g), где $f_C = x^n$ и $g_C = y^m$. Тогда

$$|\mathbb{F}[x,y]/\mathfrak{J}| = |\mathbb{F}|^{nm}.$$

Замечание 5.6. Данная гипотеза подтверждается вышеизложенными примерами.

Также, исходя из определение редуцированного базиса Грёбнера можно заметить, что элементы $\{f + \mathfrak{J} | f \in \mathbb{F}[x,y], \deg_x f < n, \deg_y f < m\}$ являются попарно различными в $\mathbb{F}[x,y]/\mathfrak{J}$, а значит верна оценка снизу:

$$|\mathbb{F}|^{nm} \leqslant |\mathbb{F}[x,y]/\mathfrak{J}|.$$

Также последнее следствие указывается, что должно быть что-то похожее.

Замечание 5.7. Пусть далее $\mathbb{F} = \mathbb{Z}_2$. Рассмотрим случаи как в Гипотезе выше.

1. $\mathfrak{J} = (x^2 + y^2 + 1, y^3 + x)$. Аналогично вышеизложенному для любого многочлена $f \in \mathbb{Z}_2[x,y]$ найдётся многочлен $g \in \mathbb{Z}_2[x,y]$, что $f = g \mod \mathfrak{J}$ и $\deg_x g \leqslant 2, \deg_y g \leqslant 2$. Далее заметим, что

$$x^2y^2 = (y^2+1)y^2 = y^4 + y^2 = y^2 + xy \mod \mathfrak{J},$$

$$x^2y = y(y^2+1) = y^3 + y = x + y \mod \mathfrak{J},$$

$$x^2 = y^2 + 1 \mod \mathfrak{J}.$$

   Таким образом описанием $\mathbb{Z}_2[x,y]/\mathfrak{J}$ является

$$\{a_1 + a_2y + a_3x + a_4y^2 + a_5xy + a_6xy^2 | a_i \in \mathbb{Z}_2\},$$

   и гипотеза выполнена.

2. Аналогично в случае $\mathfrak{J} = (x^2 + xy + y^2, y^3 + x)$:

$$x^2y^2 = (xy+y^2)y^2 = xy^3 + y^4 = x^2 + xy = xy + y^2 + xy = y^2 \mod \mathfrak{J},$$

$$x^2y = (xy+y^2)y = x + xy^2 \mod \mathfrak{J},$$

$$x^2 = xy + y^2 \mod \mathfrak{J},$$

   гипотеза снова выполнена.

3. Аналогично в случае $\mathfrak{J} = (x^2 + xy + y^2, y^3 + xy)$:

$$x^2y^2 = (xy+y^2)y^2 = xy^3+y^4 = x^2y+xy^2 = xy^2+y^3+xy^2 = y^3 = xy \mod \mathfrak{J},$$

$$x^2y = (xy+y^2)y = xy^2 + y^3 = xy^2 + xy \mod \mathfrak{J},$$

$$x^2 = xy + y^2 \mod \mathfrak{J},$$

   гипотеза снова выполнена.

ЗАКЛЮЧЕНИЕ

Таким образом, в работе были исследованы критерии простоты идеалов абстрактных числовых колец, алгоритмы тестирования идеалов на простоту, а также возможность реализации данных алгоритмов в кольцах целых алгебраических элементов конечных расширений поля $\mathbb{Q}$ и координатных кольцах несингулярных кривых.

1. Были получены аналоги критериев Миллера и Эйлера в абстрактных числовых кольцах, а также исследован вероятностный аналог теста Миллера-Рабина для произвольных абстрактных числовых колец.
2. Были разработаны вероятностные и детерминированные аналоги теста Миллера-Рабина для колец целых алгебраических элементов конечных расширений $\mathbb{Q}$, исследованы их свойства.
3. Было проведено исследование вероятностного аналога теста Миллера-Рабина в классе координатных колец несингулярных кривых.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. *Miller G.* Riemann's Hypothesis and Tests for Primality / G. Miller. // Journal of Computer and System Sciences. — 1976. — V. 13. — 3. — P. 300–317.
2. *Rabin M.O.* Probabilistic Algorithm for Testing Primality / M.O.Rabin. // Journal of number theory. — 1980. — V. 12. — P. 128–138.
3. *Bach E.* Explicit bounds for primality testing and related problems / E. Bach. // Mathematics of Computation. — 1990. — P. 355–380.
4. *Solovay R.* A fast Monte-Carlo test for primality / R. Solovay , S. Folker // SIAM Journal on Computing. – 1977. – P.84—85
5. *Adleman M. L.* On distinguishing prime numbers from composite numbers / Leonard M. Adleman, Carl Pomerance and Robert S. Rumely. // Annals of Mathematics — 1983. — P. 7—25.
6. *Agrawal M.* Primes in P. / M. Agrawal, N. Kayal, N. Saxena // Annals Of Mathematics - 2004. — Vol. 160, Iss. 2. — P. 781–793.
7. *Гекке Э.* Лекции по теории алгебраических чисел / Э. Гекке // Государственное издательство техническо-теоретической литературы – Москва 1940.
8. *Cohen H.* A Course in Computational Algebraic Number Theory / H. Cohen // Springer, 1996.
9. *Kranakis E.* Primality and Cryptography / E. Kranakis. // Teubner. — 1986.
10. *Lenstra H.W.* Computing Jacoby Symbols in Algebraic Number Fiels / H.W.Lenstra // Neieuw Archief voor Wiskunde. — 1995 — p.421–426.
11. *Wikstrom D.* On the l-Ary GCD-Algotihm in Ring of Integers / D.Wikstrom // Springer-Verlag Berlin Heidelberg. — 2005 — p.1189–1201.
12. *Cohen H.* Advanced Topics in Computational Number Theory / H. Cohen // Springer, 1999.
13. *Post E.M.* Computational Algebraic Number Theory / Michael E. Post // Birkhauser Verlag, 1993.
14. *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.
15. *Bernstein D.J.* Detecting perfect powers in essentially linear time / D. J. Bernstein // Mathematics of Computation, – 1998 – V.67 – P.1253 – 1283.
16. *Dekker T.J.* Primes in quadratic fields / T.J.Dekker // CWI Quartetly – 1994 – V.7 – P.367–394.

17. *Howe E.W.* Higher order Carmichael Numbers / Everette W.Howe // Math.Comp. – 2000 – V.69 – P.1711–1719.
18. *Steel G.A.* Carmichael numbers in number rings / G.Ander Steel // Journal Of Number Theory – 2008 – V.128 – P.910–917.
19. *Vaskouski M.* Primes in quadratic unique factorization domains / M. Vaskouski, N. Kondratyonok., N. Prochorov // Journal of Number Theory – November 2016 – V.168 – P. 101-116.
20. *Dandan Huang* An algorithm for computing the factor ring of an ideal in Dedekind domain with finite rank / Huang Dandan, Deng Yingpu // Science China Mathematics – 2017 – V. 61 – P.783–796.
21. *Василенко О.Н.* Теоретико-числовые алгоритмы в криптографии / О.Н. Василенко // МЦНМО, 2003.
22. *Бухштаб А.А.* Теория чисел / А.А. Бухштаб // Москва, Просвещение, 1966.
23. *Bohr. H.* Neue Anwendungen der Theorie der Diophantischen Approximationen auf die Riemannsche Zetafunktion / H. Bohr, R. Courant // Journal fur die reine und angewandte Mathematik –1914 – V.144 – P.249–274.
24. *Birkhoff G. D.* Demonstration d'un theoreme elementaire sur les functions entieres / G. D. Birkhoff // C. R. Acad. Sci. Paris, – 1929 – v.189 – P.473–475.
25. *Dobbs N.* Line, spiral, dense / N.Dobbs // L'Enseignement Mathematique – 2016 – v. 62 – P. 91–107.
26. *de Melo W.* One-Dimensional Dynamic / W. de Melo, S. van Strien // Springer, Berlin, 1993.
27. *Evans L.S.* Measure Theory and Fine Properties of Functions / L.S. Evans, Gariepy R.F. // CRC Press, Boca Raton, 1991.
28. *Fletcher A.* On quasiregular linearizers / A. Fletcher, D. Macclure. // Comput. Methods Funct. – 2015 – V.15 – P.263–276.
29. *Винберг Э.Б.* Курс алгебры / Э.Б. Винберг // МЦНМО, 2013.
30. *Atiyah M.F.* Introduction to commutative algebra / M.F. Atiyah, I.G. Macdonald, // Addison-Wesley Publishing Company, 1969.
31. *Cantor G. David* On fast multiplication of polynomials over arbitrary algebras / David G. Cantor, Erich Kaltofen // Acta Informatica. – 1991 – V.28 – P.693-701.
32. *Аржанцев И.В.* Базисы Грёбнера и системы алгебраичеких уравнений. МНЦМО, Москва, 2003.

Список публикаций автора работы

1–А. Прохоров Н.П. Вероятностный и детерминированный аналоги алгоритма Миллера-Рабина для идеалов колец целых алгебраических элементов конечных расширений поля $\mathbb{Q}$ / Н.П. Прохоров // Весц. Нац. акад. навук Беларусі. Сер. фіз.-мат. навук. – 2020. – Т. 56, №2. – С.144-156.

2–А. Vaskouski M. Dense analytic curves generated by iterations of complex periodic functions / Vaskouski M., Prochorov N., Sheshko N. // Comput. Methods Funct. Theory. — 2019. — V.19. – P. 285 – 298. – https://doi.org/10.1007/s40315-019-00262-3.

3–А. Васьковский М.М. Аналог теста Соловея-Штрассена в квадратичных Евклидовых кольцах / Васьковский М.М., Кондратёнок Н.В., Прохоров Н.П. // Доклады Национальной Академии Наук Беларуси. – 2017. – Т.61. – С.28-32.

4–А. Vaskouski M. Primes in quadratic unique factorization domains / Vaskouski M., Kondratyonok N., Prochorov N. // Journal of Number Theory. – November 2016 – V. 168 – P. 101-116.

5–А. Васьковский М.М. Аналог критерия простоты Миллера в факториальном кольце целых алгебраических элементов расширения Галуа поля Q степени не выше 3 / Васьковский М.М., Прохоров Н.П. // «Всероссийская конференция «Алгебра и теория алгоритмов», посвященная 100-летию факультета математики и компьютерных наук Ивановского государственного университета» — г. Иваново, 21-24 марта 2018 г.

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

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

8–А. Прохоров Н.П. Графы самопересечений замкнутых ломаных / Прохоров Н.П. Дуль Е.Н. // Журнал Белорусского государственного университета. Математика. Информатика, 2021(принята к печати).