Санкт-Петербургский государственный университет

Чемокос Олег Алексеевич

Выпускная квалификационная работа

Уравнение Пелля в квадратичных кольцах

Уровень образования: бакалавриат

Направление 01.03.02 «Прикладная математика и информатика»

Основная образовательная программа СВ.5004.2017 «Прикладная математика и информатика»

Профиль «Вычислительная стохастика и статистические модели»

Научный руководитель:
Кафедра высшей алгебры
и теории чисел
к. ф.-м. н., доцент И. М. Зильберборд

Рецензент:
Национальный исследовательский
университет «Высшая школа экономики» в
Санкт-Петербурге. Санкт-Петербургская
школа физико-математических и
компьютерных наук, департамент
информатики
к.ф.-.м.н., доцент М. А. Антипов

Санкт-Петербург

2021

Saint Petersburg State University

Applied Mathematics and Computer Science

Computational Stochastics and Statistical Models

CHEMOKOS Oleg Alekseevich

Graduation Project

PELL'S EQUATIONS IN QUADRATIC RINGS

Scientific Supervisor:

Associate Professor, Department of Algebra and Number Theory I. M. Zilberbord

Reviewer:

Higher School of Economics — National Research University in Saint-Petersburg, St.Petersburg School of Physics, Mathematics and Computer Science, Department of Informatics, Ph.D., associate professor M. A. Antipov

Saint Petersburg

2021

Оглавление

Введение

Часто так случается, что новые задачи возникают из уже существующих путем изменения некоторых условий. Настоящая работа не является исключением: по сути, это вариация классической задачи об описании решений уравнения Пелля в целых числах. Возможны, конечно, и другие вариации. Например, об уравнении Пелля в кольце многочленов написано в [1]. Эти вариации имеют связь с задачами из других областей математики. Работа [2], например, посвящена связи между некорректными краевыми задачами в ограниченной полуалгебраической области для дифференциальных уравнений с частными производными, задачей Понселе и алгебраическим уравнением Пелля—Абеля.

В данной работе рассматривается уравнение Пелля в квадратичных расширениях кольца целых чисел, то есть в кольцах вида $\mathbb{Z}[\sqrt{n}]$, где $n \in \mathbb{Z}$. В главе 2 представлены известые результаты, касающиеся классического уравнения Пелля. В главе 2 описана постановка задачи настоящей работы, а также возможные формы записи уравнения и разумные ограничения на параметры. В главе 3 с точностью до изоморфизма описывается алгебраическая структура группы решений уравнения Пелля в квадратичных кольцах. Доказано, что при введенных ограничениях на параметры группа изоморфна $\mathrm{C}_2 \times \mathbb{Z}^+ \times \mathbb{Z}^+$. В главе 4 рассматривается эффективное построение этих решений и строится алгоритм для поиска образующих. В ходе работы алгоритма сначала находятся решения двух классических уравнений Пелля с помощью цепных дробей. В качестве одной из образующих берется решение, соответствующее одному из найденных. Затем для каждого делителя параметра уравнения некоторые выражения проверяются на целочисленность и в зависимости от успешности проверки в качестве второго обрузующего берется либо решение, соответствующие пройденной проверке, либо решение, соответствующее оставшемуся из найденных классических.

Глава 1

Классическое уравнение Пелля

1.1. Решения образуют группу

Уравнением Пелля в классической постановке задачи называется уравнение

$$a^2 - mb^2 = 1, \tag{1.1}$$

где a и b — целые переменные, а m — целый параметр, не являющийся квадратом. Требуется описать все множество решений и разработать алгоритм, позволяющий эффективно эти решения находить. Под решением здесь понимается такая пара целых чисел (a, b), что при подстановке соответствующих ее компонент в уравнение оно при фиксированном m обращается в равенство.

Решение задачи в классической постановке известно и подробно описано в [3] и [4]. Здесь приведем некоторые результаты, которые нам понадобятся в дальнейшем, но сначала дадим одно из ключевых определений, используемых в данной работе:

Определение 1. Пусть R_1 — некоторое расширение кольца R_2. Тогда норма любого элемента R_1 как расширения R_2 есть прозведение всех автоморфизмов R_1, сохраняющих любой элемент из R_2: $\mathrm{N}t = \sigma_1(t)\sigma_2(t)\ldots\sigma_r(t)$, $t \in R_1$.

Поскольку $a^2 - mb^2 = (a - \sqrt{m}b)(a + \sqrt{m}b)$, то уравнение можно переписать в виде $\mathrm{N}t = 1$, где $t \in \mathbb{Z}[\sqrt{m}]$, а N — норма в $\mathbb{Z}[\sqrt{m}]$ как расширении $\mathbb{Z}$.

Понятно, что между парами (a, b) и элементами множества $\mathbb{Z}[\sqrt{m}]$ существует взаимно-однозначное соответствие. При этом, введя на множестве пар (a, b) умножение, соответствующее умножению в $\mathbb{Z}[\sqrt{m}]$, мы получим изоморфизм: $(a_1, b_1)(a_2, b_2) = (a_1a_2 + mb_1b_2, a_1b_2 + a_2b_1)$.

Утверждение 1. *Пары (a, b), являющиеся решением уравнения (1.1), образуют абелеву группу относительно введенной операции.*

Доказательство. См. в [4]. $\square$

1.2. Группа решений конечно порождена

Утверждение 2. *Если* (a, b) *— решение уравнения (1.1), то* $(-a, b)$, $(a, -b)$, $(-a, -b)$ *— тоже решения.*

Исходя из утверждения, мы можем рассматривать лишь такие решения (a, b), где a и b положительны. Также можно заметить, что если (x_0, y_0), (x_1, y_1) — положительные решения и $x_0 \leqslant x_1$, то $y_0 \leqslant y_1$, поскольку $x^2 = 1 + my^2$. Таким образом, можно говорить об отношении порядка на множестве решений и о минимальности положительного решения.

Теорема 1. *Группа решений уравнения (1.1) порождена двумя элементами: минимальным положительным и решением* $(-1, 0)$. *При этом подгруппа, порожденная положительными решениями, циклическая.*

Доказательство. См. в [3]. $\square$

1.3. Теорема Дирихле

Сформулируем еще один известный факт, который очень важен при решении уравнения Пелля любого вида, а перед этим дадим определение ранга абелевой группы, которое можно найти, например, в [5]:

Определение 2. Рангом абелевой группы G называется мощность базиса максимальной свободной подгруппы F.

Теорема 2 (о единицах, Дирихле)**.** *Пусть* $\mathbb{K}$ *— числовое поле (то есть конечное расширение* $\mathbb{Q}$*), а* $\mathcal{O}_K$ *— его кольцо целых чисел. Тогда ранг группы обратимых элементов* $\mathcal{O}_K$ *равен* $d = r + s - 1$*, где* r *— число различных вложений* $\mathbb{K}$ *в поле вещественных чисел* $\mathbb{R}$*, а* s *— число пар комплексно-сопряжённых различных вложений в* $\mathbb{C}$*, не являющихся чисто вещественными (то есть не явлющихся вложениями в* $\mathbb{R}$*).*

Глава 2

Постановка задачи и возможные представления уравнения

Задачей настоящей работы является исследование свойств решений приведенного выше уравнения (1.1), где $a, b \in \mathbb{Z}[\sqrt{n}]$, а $m \in \mathbb{N}$, $n \in \mathbb{Z}$. Также есть случаи, в которых уравнение получается в некотором смысле вырожденным: их решения полностью определяются классическим уравнением. Чтобы исключить такие случаи, введем дополнительные ограничения: m и n не являются точными квадратами и $n > 0$, $m \neq ng^2$, $n \neq mg^2$, где g — некоторое целое. Соответствующие утверждения будут сформулированы и доказаны в этой главе.

Поскольку $a, b \in \mathbb{Z}[\sqrt{n}]$, то они однозначно представимы в виде $a = x + y\sqrt{n}$, $b = u + v\sqrt{n}$, где $x, y, u, v \in \mathbb{Z}$. При подстановке этих выражений в уравнение оно принимает вид

$$(x + y\sqrt{n})^2 - m(u + v\sqrt{n})^2 = 1.$$

Исходя из этого, под решениями мы будем также понимать такие упорядоченные четверки целых чисел (x, y, u, v), при подстановке соответствующих компонент которых в уравнение, оно при фиксированном m обращается в равенство.

Обсудим теперь возможные представления уравнения Пелля. Пусть m и n такие, как описано выше. Уравнение Пелля в кольце целых чисел:

$$a^2 - mb^2 = 1, \text{ где } a, b \in \mathbb{Z}. \tag{2.1}$$

Уравнение Пелля в кольце $\mathbb{Z}[\sqrt{n}]$ — то же, что и (2.1), но теперь $a, b \in \mathbb{Z}[\sqrt{n}]$. Равносильное ему уравнение Пелля в кольце $\mathbb{Z}[\sqrt{n}][\sqrt{m}]$, если $a = x + y\sqrt{n}$, $b = u + v\sqrt{n}$:

$$(x + y\sqrt{n})^2 - m(u + v\sqrt{n})^2 = 1, \text{ где } x, y, u, v \in \mathbb{Z}. \tag{2.2}$$

И, наконец, система уравнений, равносильная (2.2):

$$\begin{cases} xy = muv \\ x^2 + ny^2 - mu^2 - mnv^2 = 1 \end{cases}, \text{ где } x, y, u, v \in \mathbb{Z}. \tag{2.3}$$

Сформулируем и докажем первое утверждение об ограничениях:

Утверждение 3. *Если n — точный квадрат, то есть $n = g^2$, где g — некоторое целое, то все решения уравнения (2.2) имеют вид $x = a - yg$, $u = b - vg$, где a и b целые и удовлетворяют классическому уравнению Пелля (2.1), а y и v — произвольные целые.*

Доказательство. Действительно, пусть $n = g^2$, тогда уравнение (2.2) принимает вид $(x + yg)^2 - m(u + vg)^2 = 1$, и если положить $a = x + yg$ и $b = u + vg$, то получится классическое уравнение Пелля $a^2 - mb^2 = 1$. Что касается линейных диофантовых уравнений $a = x + yg$ и $b = u + vg$, то их решения тривиальны: y и v произвольные целые, а $x = a - yg$ и $u = b - vg$ по ним однозначно находятся. □

2.1. Сведение к системе уравнений

Пусть все числа в первом уравнении системы (2.3) неотрицательны, тогда можно положить $m = x_m y_m$, где $x_m = \text{НОД}(x, m)$, а $y_m = m/x_m$. Далее, разделив правую и левую части уравнения на m, в получившемся уравнении $x^* y^* = uv$, где $x^* = x/x_m$, $y^* = y/y_m$ — целые, аналогичным образом положим $u = x_u y_u$, то есть $x_u = \text{НОД}(x^*, u)$, а $y_u = u/x_u$. Разделив теперь на u, получим уравнение $x^{**} y^{**} = v$, где $x^{**} = x/(x_m x_u)$, $y^{**} = y/(y_m y_u)$ — целые. Теперь можем положить просто $x_v = x^{**}$, $y_v = y^{**}$, откуда $v = x_v y_v$. Таким образом, получили разложение $m = x_m y_m$, $u = x_u y_u$, $v = x_v y_v$, причем $x = x_m x_u x_v$, $y = y_m y_u y_v$.

Перейти от неотрицательных чисел к целым нетрудно, так как ясно, что любую комбинацию знаков чисел x, y, u, v, удовлетворяющую первому уравнению (2.3), можно получить, положив отрицательными нужные компоненты в разложении, но, конечно, такой выбор не обязательно однозначен. Например, в случае отрицательных x, y, u, v можно положить отрицательными как компоненты x_u и y_v, так и компоненты x_v и y_u. Теперь можем представить второе уравнение системы (2.3) в виде

$$x_m^2 x_u^2 x_v^2 - x_m y_m x_u^2 y_u^2 + n y_m^2 y_u^2 y_v^2 - n x_m y_m x_v^2 y_v^2 = 1.$$

Выполнив ряд преобразований, получим

$$x_m x_u^2 (x_m x_v^2 - y_m y_u^2) + n y_m y_v^2 (y_m y_u^2 - x_m x_v^2) = 1,$$

$$(x_m x_v^2 - y_m y_u^2)(x_m x_u^2 - n y_m y_v^2) = 1.$$

Последнее уравнение равносильно выполнению одной из двух систем:

$$\begin{cases} x_m x_v^2 - y_m y_u^2 = 1 \\ x_m x_u^2 - n y_m y_v^2 = 1 \end{cases}, \quad \begin{cases} x_m x_v^2 - y_m y_u^2 = -1 \\ x_m x_u^2 - n y_m y_v^2 = -1 \end{cases}. \tag{2.4}$$

Докажем теперь еще одно утверждение об ограничениях:

Утверждение 4. *Если $n < 0$, то решения уравнения Пелля (2.2) совпадают с решениями классического уравнения Пелля (2.1).*

Доказательство. Исключим здесь также и тривиальный случай $n = 0$. В этом случае компоненты x и u уравнения (2.2) являются решениями классического уравнения (2.1), а y и v произвольны.

Далее заметим, что если $n < 0$, то вторые уравнения обеих систем (2.4) имеют только тривиальные решения при $x_m = 1$ и $y_m = m$, поэтому $y_v = 0$, а значит, компоненты y и v исходного решения нулевые, то есть все решения (2.2) являются решениями классического уравнения Пелля. Обратное включение очевидно. □

Теперь ясно, что для решения исходного уравнения Пелля (2.2), достаточно найти решения систем (2.4) при всяком наборе параметров x_m, y_m, что $x_m y_m = m$. А поскольку все уравнения в системах имеют вид $kx^2 - ty^2 = 1$, то достаточно уметь находить все решения таких уравнений.

Заметим, что уравнение $kx^2 - ty^2 = 1$ эквивалентно уравнению $\mathrm{N}\mu = k$, где $\mu \in M = \left\{kx + y\sqrt{kt} \mid x, y \in \mathbb{Z}\right\}$, а N — норма $\mathbb{Z}[\sqrt{kt}]$ как расширения $\mathbb{Z}$. Будем такое уравнение называть неоднородным. Уравнение же $\mathrm{N}\eta = 1$, где $\eta \in \mathbb{Z}[\sqrt{kt}]$, можно считать соответствующим однородным для уравнения $\mathrm{N}\mu = k$, поскольку, согласно общей теории представлений чисел бинарными квадратичными формами, подробно описанной в [5], всякое решение неоднородного уравнения представляется в виде некоторого фиксированного частного решения этого уравнения, умноженного на какое-то решение однородного. Иными словами, учитывая, что ранг группы решений однородного равен единице, все решения уравнения $\mathrm{N}\mu = k$ с точностью до знака можно представить в виде $\mu = \mu_0 \eta^r$, где $\mathrm{N}\mu_0 = k$, η — свободный образующий группы решений однородного, а r — некоторое целое число.

Заметим также, что, на самом деле, нас интересуют лишь целые компоненты x и y в представлении числа μ, поэтому решение неоднородного можно записывать в виде

$\theta = \mu/\sqrt{k}$, причем тогда $\mathrm{N}\theta = 1$, где N — норма кольца $\mathbb{Z}[\sqrt{k}][\sqrt{t}]$ как расширения $\mathbb{Z}[\sqrt{k}]$. При этом очевидно, что тогда для любого θ справедливо такое же представление, что и для μ, а именно: $\theta = \theta_0\eta^r$ с точностью до знака. Далее для удобства вычислений будем пользоваться именно таким видом решений.

2.2. Существование решений

Пусть теперь имеется такое θ, как описано выше. Напишем его в явном виде: $\theta = x\sqrt{k} + y\sqrt{t}$, где x и y целые и удовлетворяют уравнению $kx^2 - ty^2 = 1$, где $k, t \in \mathbb{N}$. Далее поскольку $\mathrm{N}\theta = 1$, где N — норма кольца $\mathbb{Z}[\sqrt{k}][\sqrt{t}]$ как расширения $\mathbb{Z}[\sqrt{k}]$, то и $\mathrm{N}\theta^2 = 1$. С другой стороны, $\mathrm{N}\theta^2 = \mathrm{N}(kx^2 + ty^2 + 2xy\sqrt{kt}) = (kx^2 + ty^2)^2 - 4x^2y^2kt$. Таким образом, получается, что $\theta^2 \in \mathbb{Z}[\sqrt{kt}]$ — решение однородного уравнения. Положим, что пара (x_0, y_0) — компоненты этого решения. Не умаляя общности, будем считать, что это решение положительное. Тогда имеем систему

$$\begin{cases} kx^2 + ty^2 = x_0 \\ 2xy = y_0 \end{cases}.$$

Разрешая ее относительно x и y и рассматривая только положительные x и y, приходим к системе

$$\begin{cases} x = \sqrt{\frac{(x_0 \pm 1)}{2k}} \\ y = \frac{y_0}{2x} \end{cases}.$$

Сформулируем теперь несколько ключевых утверждений в виде леммы:

Лемма 1. *В предположениях и обозначениях, сделанных выше:*

1) Решения уравнения $kx^2 - ty^2 = 1$ существуют, тогда и только тогда, когда числа $x = \sqrt{(x_0 + 1)/2k}$ и $y = y_0/2x$ целые, где (x_0, y_0) — минимальное положительное решение однородного уравнения.

2) Аналогичные условия верны для уравнения $kx^2 - ty^2 = -1$: должны быть целыми числа $x = \sqrt{(x_0 - 1)/2k}$ и $y = y_0/2x$.

3) Решения уравнений $kx^2 - ty^2 = \pm 1$ при $k \neq 1$ не могут существовать одновременно.

Доказательство. Докажем последний пункт в предположении, что доказаны первые. Ясно, что для фиксированной пары (x_0, y_0) только одно из чисел $\sqrt{(x_0 \pm 1)/2k}$ может быть целым. Это и означает, что решения может иметь лишь одно из уравнений $kx^2 - ty^2 = \pm 1$, поскольку остальные допущения о положительности, которые делались раньше, не влияют на принадлежность к одному из уравнений.

Первые два пункта будем доказывать одновременно. Из рассуждений, приведенных выше, сразу следует, что целочисленность выражений $x = \sqrt{(x_0 \pm 1)/2k}$ и $y = y_0/2x$ необходима, где (x_0, y_0) — какое-то решение однородного уравнения. С другой стороны, если для некоторого решения однородного уравнения с компонентами (x_0, y_0) такие x и y целые, то либо $kx^2 - ty^2 = 1$, либо $kx^2 - ty^2 = -1$, так как из уравнения $\mathrm{N}\theta^2 = 1$ следует, что либо $\mathrm{N}\theta = 1$, либо $\mathrm{N}\theta = -1$. Непосредственной проверкой можно убедиться что знак перед единицей в выражении $\sqrt{(x_0 \pm 1)/2k}$ соответствует такому же знаку перед единицей в уравнении $kx^2 - ty^2 = \pm 1$. Таким образом, мы почти получили утверждение первых двух пунктов, за исключением произвольности (x_0, y_0).

Покажем теперь, что условие на целочисленность выражений можно проверять не для каждого решения однородного уравнения, а только для его свободного образующего. Действительно, для некоторого решения θ_0 существует такое q, что $\theta_0^2 = \eta^q$, где η — свободный образующий однородного уравнения. Заметим, что если q четно, тогда θ_0 или $-\theta_0$, а значит, θ_0 является решением однородного уравнения, что соответствует случаю $k = 1$ с положительной правой частью, поэтому будем считать q нечетным. Положим $2r = 1 - q$. Тогда должно существовать решение $\theta = \theta_0\eta^r = \sqrt{\eta}$, что и требовалось. Также с учетом вышесказанного из этого следует, что при $k \neq 1$ решения могут существовать лишь у одного из уравнений $kx^2 - ty^2 = \pm 1$.

□

Сформулируем теперь и докажем последние два утверждения об ограничениях:

Утверждение 5. *Если m — точный квадрат, то уравнение Пелля (2.2) равносильно выполнению одного из двух уравнений: классического уравнения Пелля $x^2 - nmv^2 = 1$ и уравнения $ny^2 - mu^2 = 1$.*

Доказательство. Заметим сперва, что первые уравнения обеих систем (2.4) не имеют решений при НОД$(x_m, y_m) \neq 1$. Это означает, что x_m и y_m — тоже являются точными квадратами, но тогда $x_m x_v^2 - y_m y_u^2 = 1$ имеет лишь решения $x_v = \pm 1$, $y_u = 0$ при $x_m = 1$, $y_m = m$, а уравнение $x_m x_v^2 - y_m y_u^2 = -1$ имеет лишь решения $x_v = 0$, $y_u = \pm 1$ при $x_m = m$, $y_m = 1$. Таким образом, в обоих случаях остаются только вторые уравнения, причем уравнение из первой системы примет вид $x^2 - nmv^2 = 1$, а уравнение из второй системы — вид $mu^2 - ny^2 = -1$. $\square$

Замечание 1. Пусть (x_0, v_0) — свободный образующий уравнения $x^2 - nmv^2 = 1$ с положительными компонентами. Тогда если числа $y_0 = \sqrt{\frac{x_0+1}{2n}}$ и $u_0 = \frac{v_0}{2y}$ целые, то все решения с точностью до знака находятся как целые компоненты степеней $y_0\sqrt{n}+u_0\sqrt{m}$, причем четным степеням соответствуют решения вида $(x, 0, 0, v)$, а нечетным — вида $(0, y, u, 0)$.

Утверждение 6. *Если $m = ng^2$ или $n = mg^2$, то группа решений уравнения Пелля в кольце $\mathbb{Z}[\sqrt{n}]$ (2.2) совпадает с группой решений классического уравнения (2.1), где g — некоторое целое.*

Доказательство. Если $m = ng^2$ или $n = mg^2$, то левая часть уравнений $x_u^2 - mnu_v^2 = \pm 1$ является разностью квадратов, откуда сразу следует, что у вторых уравнений систем (2.4) $x_m x_u^2 - ny_m y_v^2 = \pm 1$ существуют решения лишь при наборе параметров $x_m = 1$, $y_m = m$, причем они тривиальны, то есть $y_v = 0$, что означает, что компоненты y и v в исходном решении нулевые. $\square$

Глава 3

Алгебраическая структура

3.1. Группа решений

Введем на множестве упорядоченных четверок целых чисел умножение по следующему правилу: $(x_1, y_1, u_1, v_1)(x_2, y_2, u_2, v_2) = (x_1x_2 + ny_1y_2 + mu_1u_2 + mnv_1v_2, x_1y_2 + y_1x_2 + mu_1v_2 + mu_2v_1, x_1u_2 + ny_1v_2 + x_2u_1 + ny_2v_1, x_1v_2 + y_1u_2 + x_2v_1 + y_2u_1)$. Это умножение, по сути, естественным образом возникает из умножения в $\mathbb{Z}[\sqrt{m}][\sqrt{n}]$ и позволяет построить изоморфизм между группой решений и некоторой подгруппой группы обратимых элементов кольца $\mathbb{Z}[\sqrt{m}][\sqrt{n}]$, так как элементы единичной нормы обратимы. Поскольку уравнение (2.2) равносильно $\mathrm{N}t = 1$, где $t \in \mathbb{Z}[\sqrt{m}][\sqrt{n}]$, а N — норма в $\mathbb{Z}[\sqrt{m}][\sqrt{n}]$ как расширении над $\mathbb{Z}[\sqrt{n}]$, то получаем утверждение, аналогичное утверждению (1):

Утверждение 7. *Четверки (x, y, u, v), являющиеся решением уравнения (2.2), образуют абелеву группу относительно введенной операции.*

Доказательство. Замкнутость относительно введенной операции получается ровно так же, как и в утверждении (1). Коммутативность точно так же наследуется из $\mathbb{R}$. Нейтральным элементом является $(1, 0, 0, 0)$, а обратным к (x, y, u, v) является элемент $(x, y, -u, -v)$ (проверяется непосредственно). □

3.2. Виды решений

Из первого уравнения в (2.3) сразу следует, что количество отрицательных компонент в решении с ненулевыми компонентами всегда четно. Более того:

Утверждение 8. *Если (x, y, u, v) — решение, то элементы $(-x, -y, u, v)$, $(-x, y, -u, v)$, $(-x, -y, u, -v)$, $(x, -y, -u, v)$, $(x, -y, u, -v)$, $(x, y, -u, -v)$, $(-x, -y, -u, -v)$ — тоже решения.*

Поэтому достаточно изучать только решения с неотрицательными компонентами. Далее в этой главе, говоря о решениях некоторого вида, будем подразумевать, что все буквенные символы положительны.

Заметим также, что, кроме $(1,0,0,0)$, решений с нечетным количеством нулей быть не может. Это, опять же, сразу следует из уравнений системы (2.3). Также не может существовать решений вида $(0,y,0,v)$, так как в таком случае второе уравнение системы (2.3) превращается в $n(y^2-mv^2)=1$, не имеющее решений при $|n|>1$. И, наконец, решений вида $(x,y,0,0)$ и $(0,0,u,v)$ тоже не существует, что следует из первого уравнения системы (2.3). Таким образом, приходим к выводу о возможных видах решений:

Утверждение 9. *Все неотрицательные решения уравнения (2.2) имеют один из следующих видов:* $(1,0,0,0)$, $(x,0,u,0)$, $(0,y,u,0)$, $(x,0,0,v)$, (x,y,u,v).

3.3. Структура группы решений при выполнении ограничений

Пусть все ограничения, введенные в главе 1, выполнены. Рассмотрим норму N кольца $\mathbb{Z}[\sqrt{n}][\sqrt{m}]$ как расширения кольца $\mathbb{Z}$. Тогда уравнение $\mathrm{N}t=1$, где $t\in\mathbb{Z}[\sqrt{n}][\sqrt{m}]$, можно записать как $\sigma_1(t)\sigma_2(t)\sigma_3(t)\sigma_4(t)=1$, где $\sigma_i(t)$ — все различные автоморфизмы t кольца $\mathbb{Z}[\sqrt{n}][\sqrt{m}]$ над $\mathbb{Z}$. Поскольку t единственным образом представляется в виде $t=x+y\sqrt{n}+u\sqrt{m}+v\sqrt{mn}$ с некоторыми целыми x,y,u,v, то последнее уравнение примет вид

$$(x+y\sqrt{n}+u\sqrt{m}+v\sqrt{mn})(x+y\sqrt{n}-u\sqrt{m}-v\sqrt{mn})\cdot$$

$$\cdot(x-y\sqrt{n}+u\sqrt{m}-v\sqrt{mn})(x-y\sqrt{n}-u\sqrt{m}+v\sqrt{mn})=1.$$

Далее, положив здесь $\sigma_1(t)\sigma_2(t)=\sigma_3(t)\sigma_4(t)=1$, получим уравнение Пелля в виде (2.2). Таким образом, группа решений уравнения Пелля образует подгруппу в группе единиц кольца $\mathbb{Z}[\sqrt{n}][\sqrt{m}]$, а значит, можем заключить:

Лемма 2. *При выполнении ограничений группа решений уравнения Пелля (2.2) конечно порождена, причем ее ранг не превосходит 3.*

Доказательство. Выше уже было замечено, что группа решений уравнения Пелля образует подгруппу в группе единиц кольца $\mathbb{Z}[\sqrt{n}][\sqrt{m}]$. По теореме Дирихле о единицах ранг этой группы равен 3 ($r=4, s=0$), откуда немендленно следует нужное утверждение, поскольку известно, что ранг подгруппы не превосходит ранга группы. $\square$

Докажем теперь более обстоятельный результат, позволяющий целиком описать алгебраическую структуру решений:

Теорема 3. *При выполнении ограничений ранг r группы решений уравнения (2.2) равен 2. Периодическая же часть группы состоит из решений* $(\pm 1, 0, 0, 0)$*. Иными словами, группа решений уравнения (2.2) изоморфна группе* $\mathrm{C}_2 \times \mathbb{Z}^+ \times \mathbb{Z}^+$.

Доказательство. Докажем сперва неравенство $r \geqslant 2$*:*
Заметим, что решения вида $(x, 0, u, 0)$ и $(x, 0, 0, v)$ существуют всегда, так как они соответствуют уравнениям $x^2 - mu^2 = 1$ и $x^2 - mnv^2 = 1$. Относительно введенного умножения множества элементов этих видов замкнуты, то есть один вид из другого получить не удастся. Предположим теперь, что достаточно одной образующей t. Тогда для любого решения вида $(x, 0, u, 0)$ существует такое целое число s, что $t^s = (x, 0, u, 0)$. Аналогично для $(x, 0, 0, v)$ существует такое целое r, что $t^r = (x, 0, 0, v)$. Это означает, что t^{sr} должно одновременно быть и вида $(x, 0, u, 0)$, и вида $(x, 0, 0, v)$, но тогда $t^{2sr} = (1, 0, 0, 0)$, то есть t имеет конечный порядок, чего быть не может.

Докажем теперь неравенство $r \leqslant 2$*:*

Рассмотрим снова уравнение $\mathrm{N}t = \sigma_1(t)\sigma_2(t)\sigma_3(t)\sigma_4(t) = 1$. Положим теперь в нем $\sigma_1(t)\sigma_3(t) = \sigma_2(t)\sigma_4(t) = 1$. В этом случае получится уравнение, получающееся из уравнения Пелля (2.2), если заменить друг на друга параметры m и n. Уже известно, что у такого уравнения есть решения вида $(x, 0, y, 0)$, причем элемент такого вида при обратной замене параметров m и n перейдет в элемент вида $(x, y, 0, 0)$, что не является решением уравнения Пелля (2.2).

Профакторизуем группу обратимых элементов кольца $\mathbb{Z}[\sqrt{n}][\sqrt{m}]$ по подгруппе решений. Заметим, что множество элементов вида $(x, y, 0, 0)$ замкнуто относительно заданного умножения, а значит, любая подгруппа вида $< (x, y, 0, 0) >$, где $(x, y, 0, 0)$ обратим, инвариантна относительно факторизации, то есть в ней не найдется элементов, произведение которых будет элементом подгруппы решений. При этом из теории о решении уравнения Пелля в целых числах известно, что существуют элементы вида $(x, y, 0, 0)$, порядок которых неограничен. Таким образом, из вышесказанного следует, что построенная факторгруппа свободна, поскольку она конечно порождена и не имеет элементов конечного порядка, кроме единицы, а значит, ранг подгруппы решений строго меньше ранга группы обратимых элементов кольца, то есть не превосходит 2, что и требовалось.

Утверждение про периодическую часть группы очевидно, так как представленные элементы — все корни из единицы во всем поле $\mathbb{R}$. $\square$

Глава 4

Конструктивное построение решений

4.1. Выбор образующих

Заметим, что проверка условия о целочисленности выражений из леммы 1 соответствует, на самом деле, поиску разложения $\sqrt{\eta}$ в виде $\sqrt{k}x + \sqrt{t}y$. Покажем, что такое разложение в контексте задачи единственно:

Утверждение 10. *Существует не более одного набора параметров x_m и y_m, где x_m свободен от квадратов, при котором у одной из систем (2.4) уравнения не являются классическими уравнениями Пелля (2.1), и их решения существуют.*

Доказательство. Предположим, что нам удалось представить $\sqrt{\eta}$ в виде $\sqrt{k_1}x_1 + \sqrt{t_1}y_1$ и в виде $\sqrt{k_2}x_2 + \sqrt{t_2}y_2$, причем k_i и t_i взаимно просты и k_i свободны от квадратов. Тогда из $\sqrt{k_1}x_1 + \sqrt{t_1}y_1 = \sqrt{k_2}x_2 + \sqrt{t_2}y_2$ получается, что степени расширения $\mathbb{Z}[\sqrt{k_i}][\sqrt{t_i}]$ над $\mathbb{Z}$ не меньше 2, причем они равны и совпадают со степенью расширения $\mathbb{Z}[\sqrt{k_1}][\sqrt{t_1}][\sqrt{k_2}][\sqrt{t_2}]$ над $\mathbb{Z}$. Таким образом, иррациональности левой и правой части совпадают, а значит, равны слагаемые. Тогда ясно, что либо $k_1 = k_2$, $t_1 = t_2$, $x_1 = x_2$, $y_1 = y_2$, либо $k_1 = t_2$, $t_1 = k_2$, $x_1 = y_2$, $y_1 = x_2$, причем из вида уравнений $x_m x_u^2 - n y_m y_v^2 = \pm 1$ систем (2.4) сразу следует невозможность второго варианта. □

В предыдущем утверждении для единственности существенно, что x_m свободен от квадратов, хотя это, конечно, не всегда так. Покажем, что для решения исходного уравнения это не имеет значения:

Утверждение 11. *Пусть $x_m^{(1)} = g^2 x_m^{(2)}$, $g^2 y_m^{(1)} = y_m^{(2)}$. Положим также, что при этих наборах параметров существуют решения уравнения (2.2). Тогда множества решений (2.2), соответствующие этим наборам, совпадают.*

Доказательство. Поскольку решения существуют, то $x_m^{(1)}$ и $y_m^{(1)}$ взаимно просты. Тогда для первого уравнения имеем $\sqrt{x_m^{(1)}}x_v^{(1)} + \sqrt{y_m^{(1)}}y_u^{(1)} = \sqrt{x_m^{(2)}}x_v^{(2)} + \sqrt{y_m^{(2)}}y_u^{(2)} = \sqrt{\eta_1}$, откуда в силу взаимной простоты $x_m^{(1)}$ и $y_m^{(1)}$ и уравнений в условии получаем следующие соотношения: $x_v^{(2)} = g x_v^{(1)}$, $y_u^{(1)} = g y_u^{(1)}$. Аналогично из второго уравнения получим соотношения $x_u^{(2)} = g x_u^{(1)}$, $y_v^{(1)} = g y_v^{(1)}$. Тогда выходит, что $x_m^{(1)} x_u^{(1)} x_v^{(1)} = x_m^{(2)} x_u^{(2)} x_v^{(2)}$, $y_m^{(1)} y_u^{(1)} y_v^{(1)} = y_m^{(2)} y_u^{(2)} y_v^{(2)}$, $x_u^{(1)} y_u^{(1)} = x_u^{(2)} y_u^{(2)}$, $x_v^{(1)} y_v^{(1)} = x_v^{(2)} y_v^{(2)}$, что и требовалось. □

Будем считать, что параметр x_m свободен от квадратов. Введем на множестве решений систем (2.4) покомпонентное умножение: то есть если θ_{11} и θ_{12} — некоторые решения первого уравнения одной из систем, а θ_{21} и θ_{22} — соответствующие им решения второго уравнения, то произведением будем считать пару $\theta_{11}\theta_{12}$ — решение первого уравнения и $\theta_{21}\theta_{22}$ — решение второго уравнения. Тогда можно сформулировать утверждение:

Утверждение 12. *Множество решений систем (2.4) относительно введенной операции образует абелеву группу.*

Доказательство. Замкнутость очевидна, поскольку умножение покомпонентное, а решения неоднородных уравнений единственны в смысле утверждения 10. Единица — пара $\theta_1 = \theta_2 = 1$. Обратные элементы в силу покомпонентности достаточно предъявить отдельно для решения каждого из уравнений вида $kx^2 - ty^2 = 1$. Ясно, что если $\theta = \sqrt{k}x + \sqrt{t}y$ — решение, то $\theta^{-1} = \sqrt{k}x - \sqrt{t}y$ — тоже решение, причем $\theta\theta^{-1} = 1$. $\square$

Тогда становится ясно, как выбирать образующие только что построенной группы, если мы ищем решения систем (2.4):

Утверждение 13. *Пусть η_1 и η_2 — свободные образующие уравнений $x_v^2 - my_u^2 = 1$ и $x_u^2 - nmy_v^2 = 1$ соответственно. Если при каких-то x_m и y_m, таких что $x_m y_m = m$, существуют разложения $\sqrt{\eta_1}$ в виде $\sqrt{x_m}x_v + \sqrt{y_m}y_u$ и $\sqrt{\eta_2}$ в виде $\sqrt{x_m}x_u + \sqrt{ny_m}y_v$, то $\sqrt{\eta_1}$ и $\sqrt{\eta_2}$ можно взять в качестве свободных образующих группы решений систем (2.4). В противном же случае в качестве свободных образующих можно взять сами η_1 и η_2.*

Доказательство. Второй случай тривиален, поскольку в условии явно указано, что никаких решений, кроме как у системы с однородными уравнениями, не существует. Первый случай сразу следует из предыдущего утвреждения, поскольку в силу утверждения 10 только у одной системы с неоднородными уравнениями существуют решения, причем все они описываются нечетными степенями $\sqrt{\eta_1}$ и $\sqrt{\eta_2}$. Решения же системы с однородными уравнениями описываются четными степенями $\sqrt{\eta_1}$ и $\sqrt{\eta_2}$. $\square$

Остается понять, как получить свободные образующие исходного уравнения. Сформулируем перед этим утверждение о связи решений систем (2.4) и решений уравнения (2.2):

Утверждение 14. *Сопоставление некоторому решению одной из систем (2.4) решения уравнения (2.2), построенное в главе 1, является эпиморфизмом групп.*

Доказательство. Сюръективность сразу следует из построения. Докажем морфизм. Назовем это сопоставление ψ. Рассмотрим сначала случай с одинаковыми x_m и y_m. Пусть $\theta_{11} = \sqrt{x}_m x_v^{(1)} + \sqrt{y}_m y_u^{(1)}$ и $\theta_{12} = \sqrt{x}_m x_v^{(2)} + \sqrt{y}_m y_u^{(2)}$ — некоторые решения первого уравнения системы, а $\theta_{21} = \sqrt{x}_m x_u^{(1)} + \sqrt{n}\sqrt{y}_m y_v^{(1)}$ и $\theta_{22} = \sqrt{x}_m x_u^{(2)} + \sqrt{n}\sqrt{y}_m y_v^{(2)}$ — некоторые решения второго. Пусть при этом (x_1, y_1, u_1, v_1) и (x_2, y_2, u_2, v_2) — соответствующие им решения исходного. Тогда

$$\theta_{11}\theta_{12} = x_m x_v^{(1)} x_v^{(2)} + y_m y_u^{(1)} y_u^{(2)} + \sqrt{m}(x_v^{(1)} y_u^{(2)} + x_v^{(2)} y_u^{(1)}) = x_v^* + \sqrt{m} y_u^* = \eta_{1*},$$

причем $x_m^* = 1$, $y_m^* = m$. Аналогично

$$\theta_{21}\theta_{22} = x_m x_u^{(1)} x_u^{(2)} + n y_m y_v^{(1)} y_v^{(2)} + \sqrt{mn}(x_u^{(1)} y_v^{(2)} + x_u^{(2)} y_v^{(1)}) = x_u^* + \sqrt{mn} y_v^* = \eta_{2*}.$$

Таким образом, получается $(x^*, y^*, u^*, v^*) = (x_m^* x_u^* x_v^*, y_m^* y_u^* y_v^*, x_u^* y_u^*, x_v^* y_v^*)$ — некоторое решение исходного уравнения, причем

$$x^* = x_1 x_2 + n y_1 y_2 + m u_1 u_2 + mn v_1 v_2, \quad y^* = x_1 y_2 + x_2 y_1 + m u_1 v_2 + m u_2 v_1,$$

$$u^* = x_1 u_2 + x_2 u_1 + n y_1 v_2 + n y_2 v_1, \quad v^* = x_1 v_2 + x_2 v_1 + y_1 u_2 + y_2 u_1.$$

Таким образом,

$$\psi(\theta_{11}\theta_{12}, \theta_{21}\theta_{22}) = (x^*, y^*, u^*, v^*) = (x_1, y_1, u_1, v_1)(x_2, y_2, u_2, v_2) = \psi(\theta_{11}, \theta_{21})\psi(\theta_{12}, \theta_{22})$$

Случай, когда x_m и y_m разные, почти ничем не отличается. Такое возможно, только если решение неоднородного уравнения умножается на решение однородного. Этот случай можно проверить непосредственно, как это сделано выше для случая одинаковых x_m и y_m, либо же разделив уравнения $\theta_{i1}\theta_{i2} = \eta_{i*}$, например, на θ_{i2}. Действительно, так как $\theta_{12}^{-1} = \sqrt{x}_m x_v^{(2)} - \sqrt{y}_m y_u^{(2)}$, а $\theta_{22}^{-1} = \sqrt{x}_m x_u^{(2)} - \sqrt{n}\sqrt{y}_m y_v^{(2)}$, то пара θ_{12}^{-1} и θ_{22}^{-1} соответствует решению $(x_2, y_2, -u_2, -v_2)$. Обозначим $\theta_{1*} = \theta_{12}^{-1}$ и $\theta_{2*} = \theta_{22}^{-1}$. В силу произвольности всех компонент имеем

$$\psi(\eta_{1*}\theta_{1*}, \eta_{2*}\theta_{2*}) = (x_1, y_1, u_1, v_1) = (x^*, y^*, u^*, v^*)(x_2, y_2, -u_2, -v_2) = \psi(\eta_{1*}, \eta_{2*})\psi(\theta_{1*}, \theta_{2*})$$

$\square$

Остается заключить, какие исходные решения можно брать в качестве свободных образующих:

Теорема 4. *Если существуют разложения $\sqrt{\eta_1}$ в виде $\sqrt{x_m}x_v + \sqrt{y_m}y_u$ и $\sqrt{\eta_2}$ в виде $\sqrt{x_m}x_u + \sqrt{ny_m}y_v$, в качестве свободных образующих исходного уравнения можно взять решение, соответствующее $\sqrt{\eta_1}$ и $\sqrt{\eta_2}$, и, например, решение, соответствующее η_1 и 1_2. В противном же случае можно взять решение, соответствующее η_1 и 1_2, и решение, соответствующее 1_1 и η_2, где 1_i — тривиальное решение i-го однородного уравнения.*

Доказательство. Обозначим образующие исходного уравнения γ_1 и γ_2, где γ_1 — решение, соответствующее η_1 и 1_2. Тогда в первом случае $\gamma_3 = \gamma_1^{-1}\gamma_2^2$ — решение, соответствующее 1_1 и η_2, и все решения, соответствующие однородной системе, есть $\gamma_1^k\gamma_3^s$, а все решения, соответствующие неоднородной, есть $\gamma_2\gamma_1^k\gamma_3^s$. Во втором случае есть только однородная система, и все ее решения соответствуют $\gamma_1^k\gamma_2^s$. □

Замечание 2. Решение, соответствующее η_1 и 1_2, имеет вид $(x, 0, u, 0)$, то есть является решением классического уравнения Пелля.

4.2. Алгоритмическая схема поиска решений

Теперь можем вывести простую алгоритмическую схему для построения решений:

- Находим образующие уравнений $x_v^2 - my_u^2 = 1$ и $x_u^2 - mny_v^2 = 1$. Запишим их как $(x_v^{(0)}, y_u^{(0)})$ и $(x_u^{(0)}, y_v^{(0)})$.

- Для каждого делителя x_m числа m проверяем, являются ли целыми числа $x_v = \sqrt{(x_v^{(0)} \pm 1)/2x_m}$, $x_u = \sqrt{(x_u^{(0)} \pm 1)/2x_m}$. Если они целые при одном и том же знаке перед единицей, то проверяем, целые ли числа $y_u = y_u^{(0)}/2x_v$, $y_v = y_v^{(0)}/2x_u$. Если все проверки прошли, то останавливаемся.

- В качестве одного из свободных образующих берем $(x_v^{(0)}, 0, y_u^{(0)} 0)$. Если при каком-то делителе x_m все проверки прошли, то в качестве второго свободного образующего берем $(x_m x_u x_v, y_m y_u y_v, x_u y_u, x_v y_v)$. В противном случае берем $(x_u^{(0)}, 0, 0, y_v^{(0)})$.

Замечание 3. Алгоритмическая сложность такого алгоритма будет $2T + O(2^{N+2})$, где T — сложность поиска в классическом случае, а N — число простых делителей числа m.

4.3. Примеры

Рассмотрим несколько примеров, отражающих ситуацию:

Задача 1

Описать все решения уравнения $x^2 - 2y^2 = 1$ в кольце $\mathbb{Z}[\sqrt{3}]$.

Решение

- Первым делом находим образующие уравнений $x_v^2 - 2y_u^2 = 1$ и $x_u^2 - 6y_v^2 = 1$: $(x_v^{(0)}, y_u^{(0)}) = (3, 2)$, $(x_u^{(0)}, y_v^{(0)}) = (5, 2)$.

- Числа $x_v = \sqrt{(x_v^{(0)} \pm 1)/2x_m}$, $x_u = \sqrt{(x_u^{(0)} \pm 1)/2x_m}$ ни при каких x_m не являются целыми при одном и том же знаке перед единицей.

- В качестве свободных образующих берем $(3, 0, 2, 0)$ и $(5, 0, 0, 2)$.

Задача 2

Описать все решения уравнения $x^2 - 29y^2 = 1$ в кольце $\mathbb{Z}[\sqrt{2}]$.

Решение

- Находим образующие $x_v^2 - 29y_u^2 = 1$ и $x_u^2 - 58y_v^2 = 1$:
  - Найдем подходящую дробь $\sqrt{29}$, числитель и знаменатель которой удовлетворяют уравнению $x_v^2 - 29y_u^2 = 1$: $\sqrt{29} \approx [5; 2, 1, 1, 2, 10, 2, 1, 1, 2] = \frac{9801}{1820}$.
  - Аналогично со вторым уравнением: $\sqrt{58} \approx [7; 1, 1, 1, 1, 1, 1, 14, 1, 1, 1, 1, 1, 1] = \frac{19603}{2574}$.
  - Итого имеем: $(x_v^{(0)}, y_u^{(0)}) = (9801, 1820)$, $(x_u^{(0)}, y_v^{(0)}) = (19603, 2574)$.
- При $x_m = 1$ получаем
  $(x_v, y_u) = (\sqrt{(9801-1)/2},\ 1820/(2\cdot 70)) = (70, 13)$,
  $(x_u, y_v) = (\sqrt{(19603-1)/2},\ 2574/(2\cdot 99)) = (99, 13)$.
- В качестве образующих берем $(x_v^{(0)}, 0, y_u^{(0)} 0) = (9801, 0, 1820, 0)$ и $(x_m x_u x_v, y_m y_u y_v, x_u y_u, x_v y_v) = (99{\cdot}70, 29{\cdot}13{\cdot}13, 99{\cdot}13, 70{\cdot}13) = (6930, 4901, 1287, 910)$.

Задача 3

Описать все решения уравнения $x^2 - 73y^2 = 1$ в кольце $\mathbb{Z}[\sqrt{5}]$.

Решение

- Находим образующие $x_v^2 - 73y_u^2 = 1$ и $x_u^2 - 365y_v^2 = 1$:
  - Найдем подходящую дробь $\sqrt{73}$, числитель и знаменатель которой удовлетворяют уравнению $x_v^2 - 73y_u^2 = 1$: $\sqrt{73} \approx [8; 1, 1, 5, 5, 1, 1, 16, 1, 1, 5, 5, 1, 1] = \frac{2281249}{267000}$.
  - Аналогично со вторым уравнением: $\sqrt{365} \approx [19; 9, 1, 1, 9, 38, 9, 1, 1, 9] = \frac{23915529}{1251796}$.
  - Итого имеем: $(x_v^{(0)}, y_u^{(0)}) = (2281249, 267000)$, $(x_u^{(0)}, y_v^{(0)}) = (23915529, 1251796)$.
- При $x_m = 1$ получаем
  $(x_v, y_u) = (\sqrt{(2281249-1)/2},\ 267000/(2\cdot 1068)) = (1068, 125)$,
  $(x_u, y_v) = (\sqrt{(23915529-1)/2},\ 1251796/(2\cdot 3458)) = (3458, 181)$.
- В качестве образующих берем $(x_v^{(0)}, 0, y_u^{(0)} 0) = (2281249, 0, 267000, 0)$ и $(x_m x_u x_v, y_m y_u y_v, x_u y_u, x_v y_v) = (3458 \cdot 1068, 73 \cdot 125 \cdot 181, 3458 \cdot 125, 1068 \cdot 181) = (3693144, 1651625, 432250, 193308)$.

Задача 4

Описать все решения уравнения $x^2 - 2y^2 = 1$ в кольце $\mathbb{Z}[\sqrt{-3}]$.

Решение

Уравнения $x^2 - mny^2 = \pm 1$ при $n < 0$ имеют только тривиальное решение, поэтому

- $(x_v^{(0)}, y_u^{(0)}) = (3, 2)$, $(x_u, y_v) = (1, 0)$.
- В качестве образующего берем $(x_v^{(0)}, 0, y_u^{(0)} 0) = (3, 0, 2, 0)$.
- Таким образом, как и предполагалось, решения в кольце $\mathbb{Z}[\sqrt{-3}]$ совпадают с решениями в кольце $\mathbb{Z}$.

Задача 5

Описать все решения уравнения $x^2 - 2y^2 = 1$ в кольце $\mathbb{Z}[\sqrt{9}]$.

Решение

- Решения классического уравнения $a^2 - 2b^2 = 1$ в кольце $\mathbb{Z}$ с точностью до знака описываются степенями $(a_0, b_0) = (3, 2)$.
- Тогда все решения уравнения в условии имеют вид $(a - 9y, y, b - 9v, v)$, где пара (a, b) — некоторая степень (a_0, b_0), а y и v — произвольные целые.

Задача 6

Описать все решения уравнения $x^2 - 4y^2 = 1$ в кольце $\mathbb{Z}[\sqrt{5}]$.

Решение

- Решения уравнения $x^2 - 20v^2 = 1$ в кольце $\mathbb{Z}$ с точностью до знака описываются степенями $(x_0, v_0) = (9, 2)$.
- Числа $y = \sqrt{\frac{9+1}{2 \cdot 5}} = 1$ и $u = \frac{2}{2} = 1$ — целые.
- Таким образом, все решения уравнения в условии с точностью до знака описываются степенями $(x_0, y_0, u_0, v_0) = (0, 1, 1, 0)$.

Задача 7

Описать все решения уравнения $x^2 - 2y^2 = 1$ в кольце $\mathbb{Z}[\sqrt{18}]$.

Решение

Уравнения $x^2 - 36y^2 = \pm 1$ имеют только тривиальное решение, поэтому далее все, как в задаче 4:

- $(x_v^{(0)}, y_u^{(0)}) = (3, 2)$, $(x_u, y_v) = (1, 0)$.
- В качестве образующего берем $(x_v^{(0)}, 0, y_u^{(0)} 0) = (3, 0, 2, 0)$.
- Решения уравнения в условии совпадают с решениями в кольце $\mathbb{Z}$, как и предполагалось.

Заключение

В ходе проведенной работы группа решений уравнения Пелля в кольце $\mathbb{Z}[\sqrt{n}]$ была описана с точностью до изоморфизма при выполнении условий, описанных в главе 1. Приведем сводку всех результатов, в том числе если какое-то условие не выполняется:

- Если $n < 0$, то группа решений уравнения (2.2) совпадает с группой решений уравнения (2.1).
- Если $n = g^2$ при некотором целом g, то все решения уравнения (2.2) принимают вид $(a - yg, y, b - vg, v)$, где числа a и b целые и удовлетворяют классическому уравнению Пелля (2.1), а y и v — произвольные целые числа.
- Если $m = g^2$ при некотором целом g, то все решения описываются уравнениями $x^2 - nmv^2 = 1$ и $ny^2 - mu^2 = 1$.
- Если $m = ng^2$ или $n = mg^2$, то группа решений уравнения (2.2) совпадает с группой решений уравнения (2.1).
- Если все условия выполняются, то группа решений уравнения (2.2) изоморфна $\mathrm{C}_2 \times \mathbb{Z}^+ \times \mathbb{Z}^+$.

Также была построена алгоритмическая схема для нахождения свободных образующих в случае выполнения всех условий: первым образующим берется решение классического уравнения Пелля, а другой выбирается в зависимости от выполнения условий целочисленности из леммы 1.

Список литературы

1. Пастор А. В. Обобщённые полиномы Чебышёва и уравнение Пелля-Абеля // Фундаментальная и прикладная математика. — 2001. — стр. 1123—1145.
2. Бурский В. П. Граничные задачи для уравнения колебания струны, задача Понселе и уравнение Пелля-Абеля: связи и соотношения // СМФН. — 2006. — стр. 1483—1487.
3. Бугаенко В. О. Уравнения Пелля. — Москва : Московский центр непрерывного математического образования, 2010.
4. Гельфонд А. О. Решения уравнений в целых числах. — Москва : Наука, 1978.
5. Боревич З. И., Шафаревич И. Р. Теория чисел. — Москва : Наука, 1985.