Санкт-Петербургский государственный университет
Прикладная математика и информатика

Отчет по научно-исследовательской работе

Уравнение Пелля в квадратичных кольцах

Выполнил:
Чемокос Олег Алексеевич
группа 17.Б04-мм

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

Санкт-Петербург
2020

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. Сведения об этом можно найти в [2].

Настоящая работа является продолжением курсовой работы на 3 курсе. Ранее было получено, что решения образуют группу, а также были найдены всевозможные их виды (см. 3.1, 3.2). В этом семестре были сформулировны теоремы о структуре решений в вещественном и комплексом случаях, а также разобран частный случай с равными параметрами (см. 3.3 — 3.5).

Глава 1

Постановка задачи

Уравнением Пелля в класической постановке задачи называется уравнение

$$a^2 - mb^2 = 1,$$

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

Решение задачи в классической постановке известно и подробно описано в [3] и [4]. Некоторые результаты будут необходимы в дальнейшем, а потому еще будут приведены ниже.

Задачей настоящей работы является исследование свойств решений приведенного выше уравнения (1.1), где $a, b \in \mathbb{Z}[\sqrt{n}]$, а $m, n \in \mathbb{Z}$ — свободны от квадратов.

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 понимать такие упорядоченные четверки целых чисел (x, y, u, v), при подстановке соответствующих компонент которых в уравнение, оно при фиксированном m обращается в тождество.

1.1. Возможные представления уравнения Пелля

Уравнение Пелля в кольце целых чисел:

$$a^2 - mb^2 = 1, \text{ где } a, b \in \mathbb{Z}. \tag{1.1}$$

Здесь и далее $m > 0$ и n целые, не являющиеся квадратом параметры.

Уравнение Пелля в кольце $\mathbb{Z}[\sqrt{n}]$ — то же, что и (1.1), но теперь $a, b \in \mathbb{Z}[\sqrt{n}]$. Равносильное ему уравнение Пелля в кольце $\mathbb{Z}[\sqrt{n}][\sqrt{m}]$:

$$(x + y\sqrt{n})^2 - m(u + v\sqrt{n})^2 = 1, \text{ где } x, y, u, v \in \mathbb{Z}. \tag{1.2}$$

И, наконец, система уравнений, равносильная (1.2):

$$\begin{cases} xy = muv \\ x^2 + ny^2 - mu^2 - mnv^2 = 1 \end{cases}, \text{ где } x, y, u, v \in \mathbb{Z}. \tag{1.3}$$

Глава 2

Известные результаты

2.1. Решения образуют группу

Приведем здесь доказанные факты в случае классической постановки задачи. 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 — взятие нормы в $\mathbb{Z}[\sqrt{m}]$.

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. То, что произведение пар является решением, сразу следует из того, что $\mathrm{N}(t_1t_2) = \mathrm{N}t_1\mathrm{N}t_2$ для любых $t_1, t_2 \in \mathbb{Z}[\sqrt{m}]$. Нейтральным является элемент $(1, 0)$, а обратным к (a, b) — элемент $(a, -b)$ (проверяется непосредственно). Коммутативность ясна, так как кольцо $\mathbb{Z}[\sqrt{m}]$ — подмножество поля $\mathbb{R}$. □

2.2. 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 $x_0 \leq x_1$, то $y_0 \leq y_1$, поскольку $x^2 = 1 + my^2$. Таким образом, можно говорить 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]. □

2.3. 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 1. *Рангом абелевой группы G называется мощность базиса свободной подгруппы F такой, что факторгруппа G/F является группой кручения.*

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.*

Глава 3

Полученные результаты

3.1. Группа решений

Введем на множестве упорядоченных четверок 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 этих множеств. Поскольку уравнение (1.2) равносильно $\mathrm{N}t = 1$, где $t \in \mathbb{Z}[\sqrt{m}][\sqrt{n}]$, а N — взятие нормы в $\mathbb{Z}[\sqrt{m}][\sqrt{n}]$ как расширении над $\mathbb{Z}[\sqrt{n}]$, то получаем утверждение, аналогичное утверждению (1):

Утверждение 3. *Четверки (x, y, u, v), являющиеся решением уравнения (1.2), 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 (1.3) сразу следует, что количество отрицательных компонент в решении всегда четно. Более того:

Утверждение 4. *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 будем полагать, что все символы соответствуют некоторым положительным целым числам.

Заметим также, что, кроме $(1, 0, 0, 0)$, решений с нечетным количеством нулей быть не может. Это, опять же, сразу следует из первого уравнения системы (1.3). Также не может существовать решений вида $(0, y, 0, v)$, так как в таком случае третье уравнение системы (1.3) 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 (1.3). Таким образом, приходим к выводу о возможных видах решений:

Утверждение 5. *Все положительные решения уравнения (1.2) 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. Случай $\mathbf{m} = \mathbf{n}$

Докажем, что в этом случае уравнение (1.2) равносильно уравнению (1.1) при $a = x$, $b = u$, которые уже подробно изучены и не являются предметом данной работы.

Действительно, исходя из возможных видов решений, легко уменьшить этот список до 2-х видов. Заметим, что решений вида $(x, 0, 0, v)$ не существует, поскольку им соответствует уравнение $x^2 - m^2v^2 = 1$, не имеющее решений, когда и x, и v ненулевые. Значит, не существует и решений вида $(0, y, u, 0)$, поскольку их четная степень является решением и имеет вид $(x, 0, 0, v)$. Таким образом, остаются решения вида $(x, 0, u, 0)$, которые соответствуют классическому уравнению Пелля, и решения вида (x, y, u, v), то есть остается лишь убедиться в отсутствии последних.

Домножим второе уравнение системы (1.3) на y^2 и заменим слагаемое x^2y^2 на $m^2u^2v^2$, исходя из первого уравнения этой же системы. Получим уравнение

$$m^2u^2v^2 + my^4 - mu^2y^2 - m^2v^2 = y^2, \tag{3.1}$$

причем левая часть этого уравнения делится на m, значит, делится и правая. То есть $m \mid y^2$, а значит, и $m \mid y$ (здесь можно считать, что m свободно от квадратов, иначе множитель m, являющийся квадратом, можно внести внутрь $(u + v\sqrt{m})^2$ в изначальном уравнении и сделать соответствующую замену переменных, и это, как будет видно дальше, никак не повлияет на ход рассуждений).

Пусть теперь $y = km$. Подставляя это выражение в (3.1), а также разделив обе его части на m^2 и сгруппировав переменные, получим теперь уравнение

$$(v^2 - mk^2)(u^2 - m^2k^2) = k^2. \tag{3.2}$$

Поскольку $k \mid uv$, можно записать $k = sr$, где $s \mid u$, а $r \mid v$. Подставляя это выражении в (3.2) и деля все на k^2, получим уравнение

$$\left(\left(\frac{v}{r}\right)^2 - ms^2\right)\left(\left(\frac{u}{s}\right)^2 - m^2r^2\right) = 1, \tag{3.3}$$

которое не имеет решений, если все переменные ненулевые.

3.4. Структура группы решений в вещественном случае

Рассмотрим норму N кольца $\mathbb{Z}[\sqrt{n}][\sqrt{m}]$ как расширения над кольцом $\mathbb{Z}$. 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 $(x + y\sqrt{n} + u\sqrt{m} + v\sqrt{mn})(x + y\sqrt{n} - u\sqrt{m} - v\sqrt{mn})(x - y\sqrt{n} + u\sqrt{m} - v\sqrt{mn})(x - y\sqrt{n} - u\sqrt{m} + v\sqrt{mn}) = 1$. Далее, положив здесь $\sigma_1(t)\sigma_2(t) = \sigma_3(t)\sigma_4(t) = 1$, получим уравнение Пелля в виде (1.2). Таким образом, группа решений уравнения Пелля образует подгруппу в группе единиц кольца $\mathbb{Z}[\sqrt{n}][\sqrt{m}]$, а значит, в случае положительного n заключаем:

Лемма 1. *Если $n \in \mathbb{N}$, то группа решений уравнения Пелля (1.2) конечно порождена, причем ее ранг не превосходит 3-х.*

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-м $(r = 4, s = 0)$, откуда немендленно следует нужное утверждение. □

Докажем теперь более обстоятельный результат, позволяющий целиком описать групповую структуру решений в случае положительного n:

Теорема 3. *Если $n \in \mathbb{N}$, то ранг r группы решений уравнения Пелля (1.2) равен 2-м. Периодическая же часть группы состоит из решений* $(\pm 1, 0, 0, 0)$. *Иными словами, группа решений уравнения Пелля (1.2) изоморфна группе* $\mathrm{C}_2 \times \mathbb{Z}_+ \times \mathbb{Z}_+$.

Доказательство. Докажем сперва неравенство $r \geq 2$:

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 $r \leq 2$:

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 (1.2), 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 (1.2).

Профакторизуем группу единиц кольца $\mathbb{Z}[\sqrt{n}][\sqrt{m}]$ по подгруппе решений. Заметим, что элементы вида $(x, y, 0, 0)$ замкнуты 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, а значит, ранг подгруппы решений строго меньше ранг группы единиц 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 $\mathbb{R}$. $\square$

3.5. Структура группы решений в комплексном случае

Обратим теперь внимание на комплексный случай, а именно: будем теперь искать решения уравнения Пелля (1.2) в кольце $\mathbb{Z}[\sqrt{n}][\sqrt{m}]$, при $n < 0$. В этом случае получается совсем простой результат для свободных образующих:

Теорема 4. *Если $-n \in \mathbb{N}$, то группа решений уравнения Пелля (1.2) циклическая с точностью до корней из единицы.*

Доказательство. Поскольку группа решений уравнения Пелля (1.2) является подгруппой группы единиц кольца $\mathbb{Z}[\sqrt{n}][\sqrt{m}]$, то по теореме Дирихле о единицах сразу получаем, что ранг подгруппы решений не превосходит единицы ($r = 0, s = 2$). То, что он не меньше единицы, сразу следует из того, что решения вида $(x, 0, u, 0)$ никак не зависят от параметра n. $\square$

При этом можно было бы ожидать, что корни из единицы не ограничиваются ± 1, как в вещественном случае, но, изучая подробнее этот вопрос, можно прийти к противоположному выводу:

Теорема 5. *Периодическая часть группы решений уравнения Пелля (1.2) состоит из решений* $(\pm 1, 0, 0, 0)$. *Иначе говоря, она изоморфна* C_2.

Доказательство. Вещественный случай, когда $n \in \mathbb{N}$, обсуждался в теореме 3 и не требует пояснений. Рассмотрим теперь комплексный случай с $-n \in \mathbb{N}$. Тем не менее, для удобства будем считать, что $n \in \mathbb{N}$, а уравнение Пелля рассматривается в кольце $\mathbb{Z}[\sqrt{-n}][\sqrt{m}]$.

Для начала разберемся с корнями четной степени. Формально написав уравнение $(x, y, u, v)^2 = (1, 0, 0, 0)$ получим систему уравнений:

$$\begin{cases} x^2 - ny^2 + mu^2 - mnv^2 = 1 \\ xy + muv = 0 \\ xu - nyv = 0 \\ xv + yu = 0 \end{cases} \quad , \text{ где } x, y, u, v \in \mathbb{Z}.$$

Учитывая уравнение $xy = muv$, которое остается неизменным и в комплексном случае, а также три последних уравнения системы выше, приходим к тому, что 3 координаты из 4-х должны равняться нулю. Таким образом, сразу получаем, что решениями системы выше могут быть только элементы $(\pm 1, 0, 0, 0)$. Предположим теперь, что порядок элемента равен $2k$. Это означает, что должно выполняться уравнение $(x, y, u, v)^k = (-1, 0, 0, 0)$. Если k четно, то придем к системе выше, где первое уравнение заменится на $x^2 - ny^2 + mu^2 - mnv^2 = -1$. Очевидно, что такая система не имеет решений, поскольку если 3 координаты из 4-х равны нулю, то не имеет решений первое уравнение системы.

Осталось рассмотреть два уравнения вида $(x, y, u, v)^{2k+1} = (\pm 1, 0, 0, 0)$. Ранее в доказательстве теоремы 3 у нас уже было утверждение, что всякое произведение вида $(xs_1, ys_2, us_3, vs_4)(x, y, u, v)^2$ имеет вид (xs_1, ys_2, us_3, vs_4), где s_i — положительные целые числа. В нашем случае результат сохраняется, только теперь числа s_i не обязательно положительные. Таким образом, уравнения $(x, y, u, v)^{2k+1} = (\pm 1, 0, 0, 0)$ имеют вид $(xs_1, ys_2, us_3, vs_4) = (\pm 1, 0, 0, 0)$, откуда сразу имеем, что $|x| = 1$. Далее вспомним, что для комплексного корня из единицы z имеет место равенство $\mathrm{N}z = 1$, что равносильно $(\operatorname{Re} z)^2 + (\operatorname{Im} z)^2 = 1$, где под N понимается обычная комплексная норма. Отсюда же сразу следуют неравенства $|\operatorname{Re} z| \leq 1$, $|\operatorname{Im} z| \leq 1$. Неравенство $|\operatorname{Re} z| \leq 1$ можно записать в виде $|x + u\sqrt{m}| \leq 1$, что сразу приводит к тому, что $u = -x$ (причем только при $m \leq 3$) или $u = 0$. В случае $u = -x$ уравнение $(\operatorname{Re} z)^2 + (\operatorname{Im} z)^2 = 1$ не имеет решений, а в случае $u = 0$ неизбежно приходим к решениям $(\pm 1, 0, 0, 0)$. $\square$

Заключение

В ходе проведенной работы группа решений уравнения Пелля в кольце $\mathbb{Z}[\sqrt{n}]$ была описана с точностью до изоморфизма:

- При $n > 0$ она изоморфна $C_2 \times \mathbb{Z}_+ \times \mathbb{Z}_+$.
- При $n < 0$ она изоморфна $C_2 \times \mathbb{Z}_+$.

Вместе с этим результатом было установлено, что уравнение Пелля в кольце $\mathbb{Z}[\sqrt{n}]$ эквивалентно системам уравнений в целых числах, каждое из которых имеет вид $kx^2 - sy^2 = 1$. Эти результаты будут приведены на следующем этапе, а также будет проделана работа по изучению разрешимости таких уравнений и конструктивному построению их решений.

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.