Уравнение Пелля в квадратичных кольцах

Чемокос Олег Алексеевич

Санкт-Петербургский государственный университет
Кафедра статистического моделирования

Научный руководитель: к.ф.-м.н., доц. Зильберборд И. М.

Рецензент: к.ф.-м.н., доц. Антипов М. А.

Санкт-Петербург
2021г.

Постановка задачи

Уравнение Пелля:

$$x^2 - my^2 = 1,$$

где m — натуральное число, не являющееся квадратом.

- Классическая задача: описать множество всех решений уравнения в кольце целых чисел $\mathbb{Z}$.
- Задачи настоящей работы:
  - Описать множество всех решений уравнения в кольце $\mathbb{Z}[\sqrt{n}] = \{a + b\sqrt{n} \mid a, b \in \mathbb{Z}\}$, где $n \in \mathbb{Z}$.
  - Придумать конструктивный алгоритм построения этих решений.

Области применения

- Классическое уравнение Пелля известно со времен Древней Греции и имеет важное значение в теории диофантовых уравнений.
- Обобщенное уравнение Пелля ($x^2 - my^2 = N$) возникает в квантовой теории информации.
- Уравнение Пелля-Абеля (оно же уравнение Пелля в кольце многочленов) имеет связь с задачами проективной геометрии и дифференциальным уравнением колебания струны.

Классическая задача

Классическая задача широко известна и описана во многих работах, например, в работе А.О. Гельфонда «Решение уравнений в целых числах».

Известные результаты

- Алгебраическая структура: решения образуют группу, изоморфную $\mathrm{C}_2 \times \mathbb{Z}_+$, причем минимальное положительное $(x, y > 0)$ решение уравнения является свободным образующим.
- Конструктивное построение: решения уравнения находятся как числитель и знаменатель подходящих для $\sqrt{m}$ цепных дробей.

Вырожденные случаи решений уравнения $x^2 - my^2 = 1$ в кольце $\mathbb{Z}[\sqrt{n}]$

- Если $n < 0$, или $m = ng^2$, или $n = mg^2$, то группа решений уравнения в кольце $\mathbb{Z}[\sqrt{n}]$ совпадает с группой целочисленных решений.
- Если $n = g^2$ при некотором целом g, то все решения уравнения в кольце $\mathbb{Z}[\sqrt{n}]$ принимают вид $(a - yg, y, b - vg, v)$, где числа a и b целые и удовлетворяют классическому уравнению Пелля, 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 $ny^2 - mu^2 = 1$.

Основной полученный результат

В случае, когда не выполняется ни одно из условий вырожденности, были получены следующие результаты:

- Алгебраическая структура:

Теорема

Группа решений уравнения Пелля в кольце $\mathbb{Z}[\sqrt{n}]$ *изоморфна* $\mathrm{C}_2 \times \mathbb{Z}^+ \times \mathbb{Z}^+$.

- Конструктивное построение: разработан конструктивный алгоритм для поиска пары свободных образующих.

План доказательства: алгебраическая структура

- Сводим уравнение к уравнению $\mathrm{N}t = 1$ в кольце $\mathbb{Z}[\sqrt{m}][\sqrt{n}]$ как расширении $\mathbb{Z}[\sqrt{n}]$, откуда сразу же получаем групповые свойства.
- Применяя теорему Дирихле о единицах конечного расширения $\mathbb{Q}$, находим оценку сверху для ранга группы решений.
- Доказав существование двух свободных подгрупп с тривиальным пересечением, находим оценку снизу для ранга группы решений.
- Уточняем оценку сверху и получаем точное значение ранга.

План доказательства: конструктивное построение

- Сводим уравнение к системам параметрических уравнений вида $kx^2 - ty^2 = 1$, где k и t — целые параметры, а x и y — целые переменные.
- Используя теорию представления чисел бинарными квадратичными формами, описанную в работе «Теория чисел» Боревича З.И. и Шафаревича И.Р., получаем необходимые и достаточные условия существования решений уравнения из предыдущего пункта.
- Построив эпиморфизм между группами решений параметрических систем и решениями исходного уравнения, получаем соответствие между их образующими.

Алгоритм поиска образующих

- 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 $x_v = \sqrt{(x_v^{(0)} \pm 1)/2x_m}$, $x_u = \sqrt{(x_u^{(0)} \pm 1)/2x_m}$, $y_u = y_u^{(0)}/2x_v$, $y_v = y_v^{(0)}/2x_u$ при одинаковом знаке перед единицей. Если проверки прошли, то останавливаемся.

- В качестве одного из свободных образующих берем $(x_v^{(0)}, 0, y_u^{(0)} 0)$. В качестве второго свободного образующего берем $(x_m x_u x_v, y_m y_u y_v, x_u y_u, x_v y_v)$ или $(x_u^{(0)}, 0, 0, y_v^{(0)})$ в зависимости от успешности проверки предыдущего пункта.

Задача 1

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

Решение

- $(x_v^{(0)}, y_u^{(0)}) = (3, 2)$, $(x_u^{(0)}, y_v^{(0)}) = (5, 2)$.
- 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

- $(x_v^{(0)}, y_u^{(0)}) = (9801, 1820)$, $(x_u^{(0)}, y_v^{(0)}) = (19603, 2574)$.
- 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
$(x_m x_u x_v, y_m y_u y_v, x_u y_u, x_v y_v) = (6930, 4901, 1287, 910)$.

Итоги

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

- Если $n < 0$, или $m = ng^2$, или $n = mg^2$, то она совпадает с группой целочисленных решений.
- Если $n = g^2$ при некотором целом g, то все решения принимают вид $(a - yg, y, b - vg, v)$, где числа a и b целые и удовлетворяют классическому уравнению Пелля, 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 $ny^2 - mu^2 = 1$.
- В остальных случаях она изоморфна $\mathrm{C}_2 \times \mathbb{Z}^+ \times \mathbb{Z}^+$.

Кроме того, для невырожденного случая был построен конструктивный алгоритм поиска образующих.