Диофантовы уравнения второй степени

Проект посвящён изучению диофантовых уравнений второй степени. Мы надеемся, что участники проекта разовьют теорию, которая позволит им решать достаточно большой класс задач. Наиболее яркие из этих задач приведены ниже.

До промежуточного финиша мы будем работать с уравнениями второй степени в рациональных числах. Мы выпишем явный алгоритм, с помощью которого можно эффективно определить, имеет ли данное уравнение решение или нет. Как приложение развитой техники, мы докажем следующую теорему, принадлежащую Карлу Фридриху Гауссу.

Теорема (Гаусс)**.** Натуральное число представимо в виде суммы трёх квадратов, если и только если оно не представимо в виде $4^n(8m-1)$.

После промежуточного финиша мы сосредоточимся на уравнениях в целых числах от двух переменных. Мы научимся эффективно решать такие уравнения, используя карты квадратичных форм. Также мы докажем следующее утверждение.

Теорема (Дж. Конвей)**.** Существует единственный [1] однородный многочлен $f(x,y,z)$ степени 2, для которого уравнение $f(x,y,z)=m$ имеет решение для всякого $m=1,\ldots,30$ и не имеет решений при $m<0$.

Вводные задачи

В этой части мы собрали задачи на целочисленные квадратичные формы, которые могут быть решены с помощью единого и общего алгоритма решения квадратичных уравнений (который, как мы надеемся, будет построен участниками). Впрочем, все эти задачи могут быть решены и непосредственно. Заметим, что общего алгоритма решения диофантовых уравнений произвольной степени не существует и принципиально существовать не может (это 10-ая проблема Гильберта, решенная отрицательно Ю. Матиясевичем в 1970-м году).

Задачи 1–9.

Если какие-то из этих задач у Вас не получилось решить, скажем, за час — не огорчайтесь. Вы всегда можете вернуться к ним позднее, имея больше технических средств.

Квадратичные формы

Определение 1. Мы называем *квадратичной формой* однородный многочлен степени 2 от какого-то числа переменных. Примерами квадратичных форм являются многочлены

$$2x^2+2xy-y^2 \text{ и } x^2-xz+y^2-2z^2.$$

Для всякого натурального числа d мы обозначим через $\mathbb{Z}^d$ множество наборов из d целых чисел. Например, множество пар целых чисел обозначается нами $\mathbb{Z}^2$. Всякая квадратичная форма от двух переменных x,y задаёт функцию на $\mathbb{Z}^2$, т.е. сопоставляет каждой паре чисел (x,y) число $f(x,y)$. В дальнейшем, мы часто будем заменять элемент $(x,y)\in\mathbb{Z}^2$ одной буквой (скажем, v) и писать $f(v)$ вместо $f(x,y)$.

Определение 2. Мы будем говорить, что квадратичная форма *представляет целое число* n, если $\exists v\in\mathbb{Z}^d \mid f(v)=n$, или, что то же самое, если уравнение

$$f(x,y)=n$$

имеет решение в целых числах.

[1] Это утверждение формально неверно. Оно будет уточнено позже.

Задачи 10–11.

Определение 3. Мы назовём две квадратичные формы *эквивалентными.* если они представляют одно и то же множество целых чисел.

Задача 12.

С какими-то квадратичными формами работать проще, а с какими-то — сложнее. Хотелось бы найти для каждой квадратичной формы как можно более удобного представителя её класса эквивалентности (скажем, квадратичную форму вида $ax^2 + by^2$). Для этого полезно иметь какие-то разумные критерии того, когда две квадратичные формы эквивалентны. Более того, полезно иметь какие-то легко вычислимые инварианты квадратичных форм. Мы предложим некоторый набор таких инвариантов.

Определение 4. Квадратичная форма f называется *положительно определённой*, если $f(v) > 0$ для всякого $v \neq 0$. Квадратичная форма называется *неотрицательно определённой*, если $f(v) \geqslant 0$ для всякого $v \in \mathbb{Z}^2$. Наконец, квадратичная форма называется *неопределённой*, если $f(u) > 0$ и $f(v) < 0$ для некоторых $u, v \in \mathbb{Z}^2$.

Задача 13.

Расширенная арифметика: p-адические числа

В этой части проекта мы займёмся доказательствами следующей теоремы.

Теорема (Метатеорема)**.** Квадратное уравнение от произвольного числа переменных имеет решения в рациональных числах тогда и только тогда, когда к этому нет препятствий, связанных с остатками при делении на простые числа.

С помощью Метатеоремы мы докажем теорему (Гаусса) и следующую теорему Лежандра.

Теорема (Лежандр)**.** Всякое положительное целое число представимо в виде суммы четырёх квадратов целых чисел.

В проекте мы предлагаем подразбиение теоремы (как и теоремы Гаусса/Лежандра) на несколько подзадач, каждая из которых может быть решена самостоятельно. Для начала нам нужно придать какой-нибудь формальный смысл формально неопределённой (и неформально неверной) метатеореме.Начнём мы с примера, а именно со следующего утверждения, являющегося частным случаем метатеоремы.

Определение 5. Число m называется *квадратичным вычетом* в остатках при делении на n, если существует целое число t такое, что $m \equiv t^2 (\mathrm{mod}\ n)$.

Задачи 14–15.

Если НОД$(m, n) = 1$, то из условий a)-c) задачи 14 следует существование ненулевого рационального решения уравнения

$$ax^2 + by^2 = c.$$

Если НОД$(m, n) \neq 1$, то на пару (m, n) должны быть наложены дополнительные условия, связанные с простыми делителями НОД(m, n). Эти условия достаточно просты, но громоздки. Изящный способ записи этих условий связан с понятием p-адического числа. Для начала мы определим p-адические числа и выявим их простейшие ($\sim$ важнейшие) свойства.

Для каждого простого числа p определим $\mathbb{Z}_p$ как множество формальных выражений вида

$$a_0 + a_1 p + \ldots + a_n p^n + \ldots \quad (a_i \in \mathbb{Z}) \tag{1}$$

(число слагаемых может быть бесконечно). Два таких выражения считаются равными, если они совпадают с точностью до членов порядка p^n для любого n. К примеру,

$$1 = (p+1) - (p+1)p + (p+1)p^2 - (p+1)p^3 + \dots.$$

Выражения вида (1) можно складывать, вычитать и умножать. Таким образом, для каждого уравнения $f = 0$ с коэффициентами в целых числах можно рассматривать его решения в $\mathbb{Z}_p$ (=: целых p-адических числах). Следующая задача указывает на связь решений в целых числах и решений в целых p-адических числах.

Задача 16.

Целые p-адические числа представляют собой расширение понятия целого числа. Такое же p-расширение имеет и понятие рационального числа. Для каждого простого p определим $\mathbb{Q}_p$ как множество формальных выражений вида

$$a_{-k}p^{-k} + a_{-k+1}p^{-k+1} + \dots + a_n p^n + \dots \tag{2}$$

(k — произвольное целое число, $a_i \in \mathbb{Z}$). Очевидно, что всякое целое p-адическое число имеет вид (2) с $a_{-k} = ... = a_{-1} = 0$.

Для того, чтобы помочь участникам привыкнуть к понятию p-адического числа, ниже мы приводим несколько задач.

Задачи 17–26.

Теперь мы готовы к формальной версии Метатеоремы.

Теорема (Принцип Минковского-Хассе)**.** Квадратное уравнение $f = 0$ от нескольких переменных имеет решение в рациональных числах, если и только если оно имеет решения

а) в вещественных числах,

б) p-адических числах (:=$\mathbb{Q}_p$) для всякого простого числа p.

Задача 27.

Принцип Минковского-Хассе сводит решение уравнений в рациональных числах к решению тех же уравнений в числах p-адических. При этом подразумевается, что решать уравнения в числах p-адических много проще. Для начала мы сформулируем в виде набора задач алгоритм решения квадратного уравнения от двух переменных в p-адических числах. Начнём мы с однородного уравнения

$$z^2 - ax^2 - by^2 = 0. \tag{3}$$

Определение 6. Положим $(a, b)_p = 1$, если уравнение (3) имеет ненулевое решение в целых p-адических числах. В противном случае положим $(a, b)_p = -1$. Значение $(a, b)_p$ называется *символом Гильберта* пары (a, b) по отношению к простому числу p.

Таким образом, для решения уравнения (3) хочется научиться находить значения $(a, b)_p$.

Задачи 28–29.

Чтобы компактно записать явную формулу для символа Гильберта, нам потребуется *символ Лежандра* $\left(\frac{x}{p}\right)$, определённый для любых целого x и простого p. Он равен 1, -1 или 0 в зависимости от того, является x ненулевым квадратичным вычетом, невычетом или нулём по модулю p. Для нечётного простого p символ Лежандра вычисляется по формуле

$$\left(\frac{x}{p}\right) = x^{\frac{p-1}{2}} \pmod p.$$

Задачи 30–39.

Уравнения от двух переменных и карты

В этой части проекта мы разовьём технику, позволяющую эффективно решать в целых числах уравнение

$$E_m : ax^2 + bxy + cy^2 = m \tag{4}$$

от целых переменных x, y, где a, b, c, m — какие-то целые числа (параметры). Для этого мы сопоставим каждой квадратичной форме от двух переменных карту и выразим свойства уравнения (4) через свойства этой карты. Мы надеемся, что с помощью этого подхода участники проекта смогут также решить следующие (супер)задачи.

Задача 46 (Суперзадача)**.** Докажите, что если уравнение E_m имеет решения при каком-то положительном числе m, при каком-то отрицательном числе m и не имеет решений при $m = 0$, то для всякого m или E_m не имеет решений, или же E_m имеет бесконечно много решений.

Задача 47 (Суперзадача)**.** Верно ли, что если уравнение E_m имеет решения в целых числах при

$$m = \pm 1,\ \pm 2,\ \pm 3,$$

то E_m имеет решения при всяком целом числе m?

Задача 48 (Суперзадача)**.** Докажите, что если уравнения E_1, E_2, E_3, E_5 имеют решения в целых числах, то уравнение E_m имеет решения при каком-то $m < 0$.

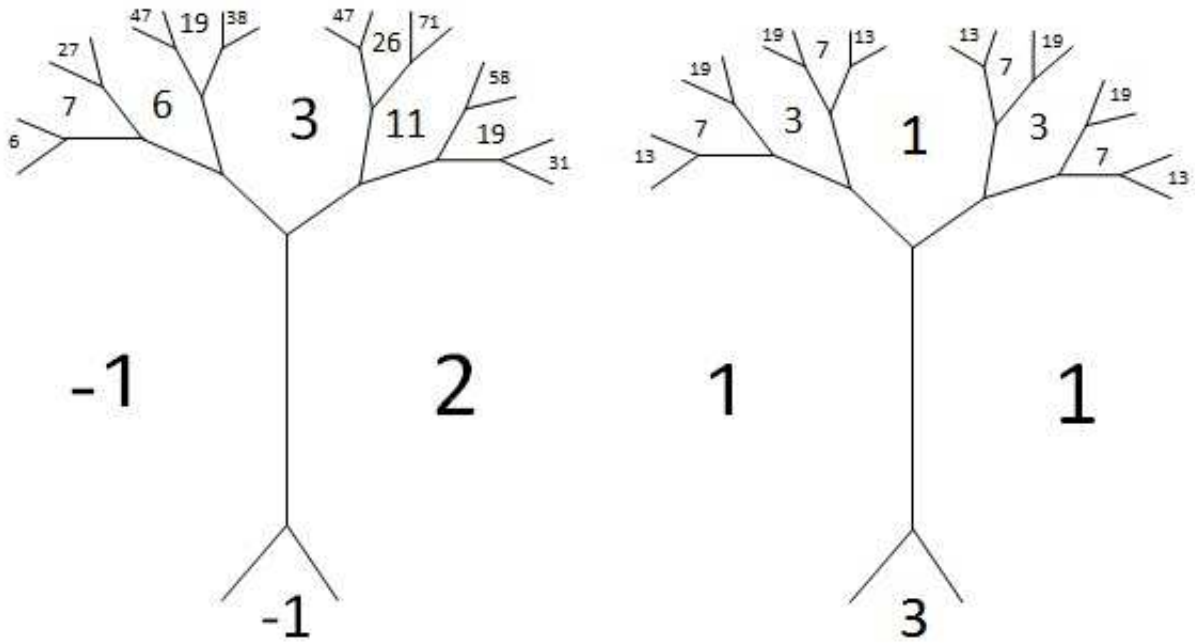
Начнём же мы с примера решения уравнения с помощью карты.

Пример работы с картами

Цель этого пункта — помахав руками, показать, что многочленам от двух переменных можно сопоставлять карты. К примеру, многочлены

$$2x^2 + 2xy - y^2 = 1 \text{ и } x^2 - xy + y^2 = 2$$

обладают картами



и из этих карт видно, что соответствующие уравнения не имеют решений в целых числах.

Рисуем картинку [2]

Для того, чтобы найти что-то общее среди множества чего-то очень разного, бывает полезно рассмотрение «всего и сразу» одновременно и снабжение этого «всего» какой-либо дополнительной структурой. В соответствии с этой стратегией для каждой квадратичной формы f мы рассмотрим все квадратичные формы, ей эквивалентные с точностью до так называемой линейной замены базиса, и снабдим их дополнительной структурой (мы разместим «точки» квадратичных форм на плоскости и соединим их отрезками). Для осуществления этого плана нам потребуются понятия базиса и супербазиса $\mathbb{Z}^2$.

Определение 7. *Базисом* $\mathbb{Z}^2$ называется такой набор $w_1, w_2 \in \mathbb{Z}^2$, что для любого $v \in \mathbb{Z}^2$ существуют числа $m, n \in \mathbb{Z}$, для которых

$$v = mw_1 + nw_2.$$

У нас было понятие эквивалентных форм. К сожалению, при работе с картами более правильным является следующее понятие.

Определение 8. Две формы f_1, f_2 называются *эквивалентными с точностью до линейной замены базиса*, если $\exists$ a, b, c, d, для которых $ad - bc = 1$ и

$$f_1(x, y) = f_2(ax + by, cx + dy).$$

Задачи 49–52.

Определение 9. *Супербазисом* $\mathbb{Z}^2$ называется набор $\{\pm w_1,\ \pm w_2,\ \pm(w_1+w_2)\}$, где $\{w_1, w_2\}$ — какой-то базис $\mathbb{Z}^2$. Назовём базис $\{w_1, w_2\}$ *специализацией* супербазиса $\{\pm w_1,\ \pm w_2,\ \pm(w_1 + w_2)\}$. Назовём супербазис $\{\pm w_1,\ \pm w_2,\ \pm(w_1 + w_2)\}$ *расширением* базиса $\{w_1, w_2\}$.

Упражнение 1. Выпишите все расширения данного базиса $\{w_1, w_2\}$. Выпишите все специализации данного супербазиса $\{\pm w_1,\ \pm w_2,\ \pm(w_1 + w_2)\}$.

Теперь мы готовы нарисовать карту квадратичной формы f. Начнём мы с той её части, что от f никак не зависит:

(1) каждому супербазису $\{\pm w_1,\ \pm w_2,\ \pm(w_1 + w_2)\}$ мы сопоставляем точку на плоскости (вершину будущего графа),

(2) каждому базису $\{w_1, w_2\}$ мы сопоставляем отрезок на плоскости (ребро графа), соединяющий точки-супербазисы

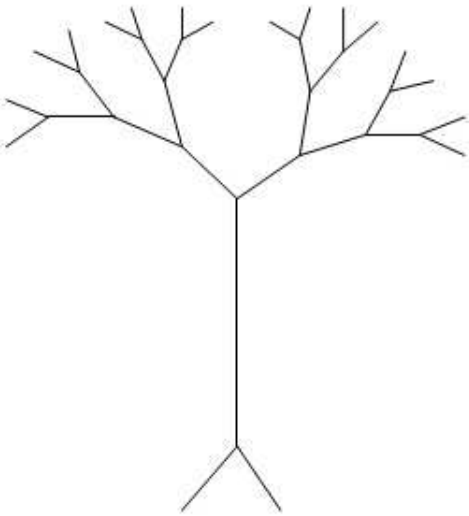
$$\{\pm w_1,\ \pm w_2,\ \pm(w_1 + w_2)\} \text{ и } \{\pm w_1,\ \pm w_2,\ \pm(w_1 - w_2)\},$$

(базисам $\{w_1, w_2\}$, $\{-w_1, w_2\}$, $\{w_1, -w_2\}$ и $\{-w_1, -w_2\}$ соответствует одно и то же ребро),

(3) каждому набору $w \in \mathbb{Z}^2$ мы сопоставляем область плоскости, границей которого являются отрезки-базисы, набор w содержащие (наборам w и $-w$ соответствует одна и та же область).

Оказывается, что всю эту картинку можно нарисовать на плоскости.

[2] Те, кто хочет сразу увидеть, как нарисовать карту квадратичной формы, могут заглянуть в дополнение к этой части проекта. А потом подумать о том, как же доказываются свойства этой самой карты.



(5)

Заметим, что (5) пока никак не зависит от квадратичной формы f. Мы напишем в каждой области (5) (а потом и рядом с каждым отрезком (5)) числа, и по этому набору чисел класс эквивалентности с точностью до линейной замены формы f будет однозначно восстанавливаться. Мы используем следующие правила.

(1) В области, соответствующей набору $w \in \mathbb{Z}^2$, мы напишем число $f(w)$.

(2) Рядом с отрезком I, соответствующим базису $\{w_1, w_2\}$, мы напишем положительное число, по модулю равное

$$f(w_1 + w_2) - f(w_1) - f(w_2).$$

Если $f(w_1 + w_2) > f(w_1 - w_2)$, началом отрезка I мы считаем точку-супербазис

$$\{\pm w_1,\ \pm w_2,\ \pm(w_1 - w_2)\},$$

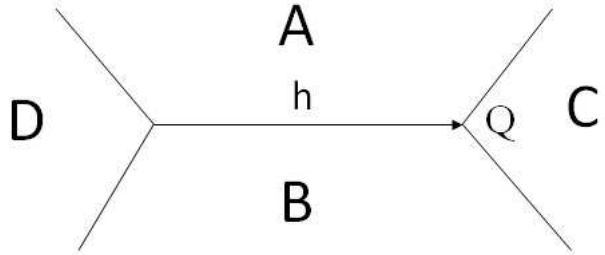
а концом считаем точку-супербазис $\{\pm w_1,\ \pm w_2,\ \pm(w_1+w_2)\}$. Если $f(w_1+w_2) < f(w_1-w_2)$ — то наоборот. Если $f(w_1 + w_2) = f(w_1 - w_2)$, то направление на I мы не задаём (и никакого числа рядом с I обычно не пишем).

Результат этой процедуры мы называем *ориентированной картой квадратичной формы* f. Если с числами около рёбер и их направлениями мы не заморачиваемся, то соответствующую картинку мы называем *картой квадратичной формы*. Для форм $2x^2 + 2xy - y^2$ и $x^2 - xy + y^2$ карты изображены на рисунках первой страницы проекта.

Упражнение 2. Нарисуйте (ориентированные) карты для квадратичных форм

$$f_1 = 3x^2 + 9xy + 7y^2, \quad f_2 = x^2 - 2y^2, \quad f_3 = x^2 - 3y^2.$$

В следующих двух задачах числа A, B, C, D, h относятся к картинке



Задачи 53–55.

Следующее определение является ключевым в решении большинства вопросов о положительно определённых квадратичных формах.

Определение 10. *Колодцем* называется вершина ориентированной карты квадратичной формы, все рёбра, инцидентные которой, направлены не к ней.

Задачи 56–60.

Нам бы хотелось обратить внимание на следующие несколько фактов:

1) идейно решения суперзадач 1, 2 и общего уравнения вида (4) близки к задачам 59, 60.

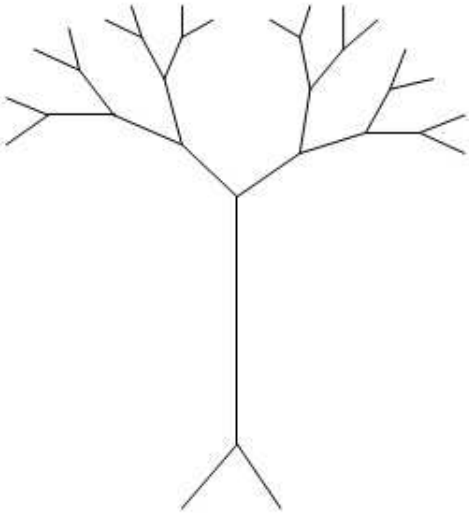
2) в тяжёлых трудовых математических буднях никто (кроме Вас самих) не будет писать для Вас ряд (достаточно простых) упражнений, который вёл бы к решению той или иной сколько-нибудь интересной задачи. Вам очень повезёт, если Вам (чаще всего, условно случайно) расскажут сколько-нибудь заметную часть нужных при решении задачи идей и приёмов.

3) цель данной конференции – познакомить Вас в той или иной форме с трудовыми математическими буднями.

Если вы ещё не догадались, к чему мы клоним, то на этом упражнения, помогающие Вам справиться с суперзадачами 1, 2, 3 и научиться решать общее уравнение вида (4), закончились. Пытаясь ещё немного облегчить Вашу участь, мы приготовили пару картинок, которые (может быть) могут Вам в (чём-нибудь) помочь или (что-нибудь) подсказать.

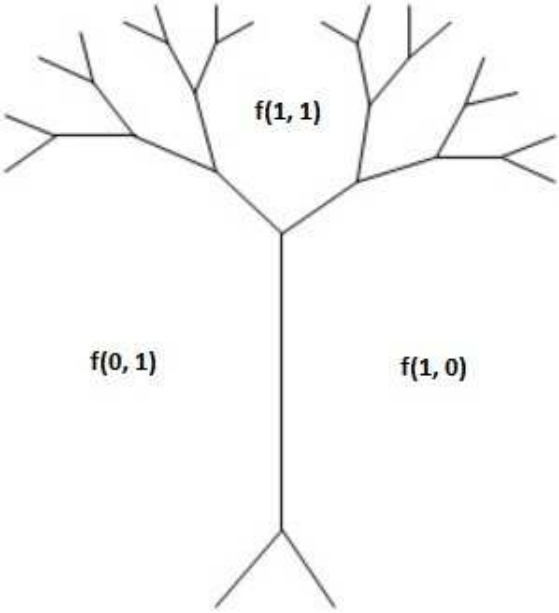
Рабоче-крестьянское описание карты квадратичной формы

Алгоритм $f \to \Gamma_f$ **:** Рассмотрим бесконечное плоское троичное дерево (т.е. нарисованный на плоскости связный граф без циклов, степень каждой вершины которого равна 3). Часть такого графа идёт ниже.



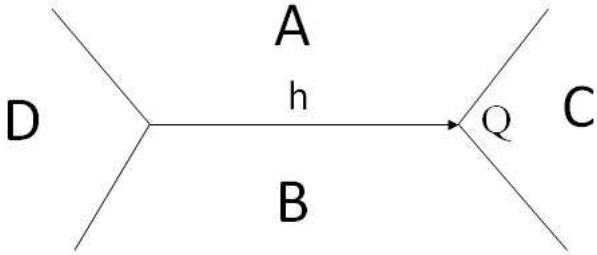
(6)

Рассмотрим какую-то вершину этого графа и впишем в три инцидентные ей грани числа $f(1,0)$, $f(0,1)$ и $f(1,1)$, как показано на рисунке.



(7)

Значения во всех остальных гранях определяются по правилу



. (8)

Правило 1: Если три значения на гранях около одного ребра (как показано на рисунке (8)) известны, то четвёртое определяется формулой $2(A+B)=C+D$.

Легко видеть, что это правило определяет карту Γ_f. Теперь по карте Γ_f мы построим ориентированную карту $\vec{\Gamma}_f$ по следующим правилам (см. рисунок (8)):

Правило 2: Над ребром h мы напишем число

$$|(A+B)-C| = |(A+B)-D|\,.$$

Правило 3: Если $C<D$, то мы заменяем ребро h на стрелку из C в D; если $C<D$, то мы заменяем ребро h на стрелку из D в C; если $C=D$, то мы оставляем ребро h неориентированным.

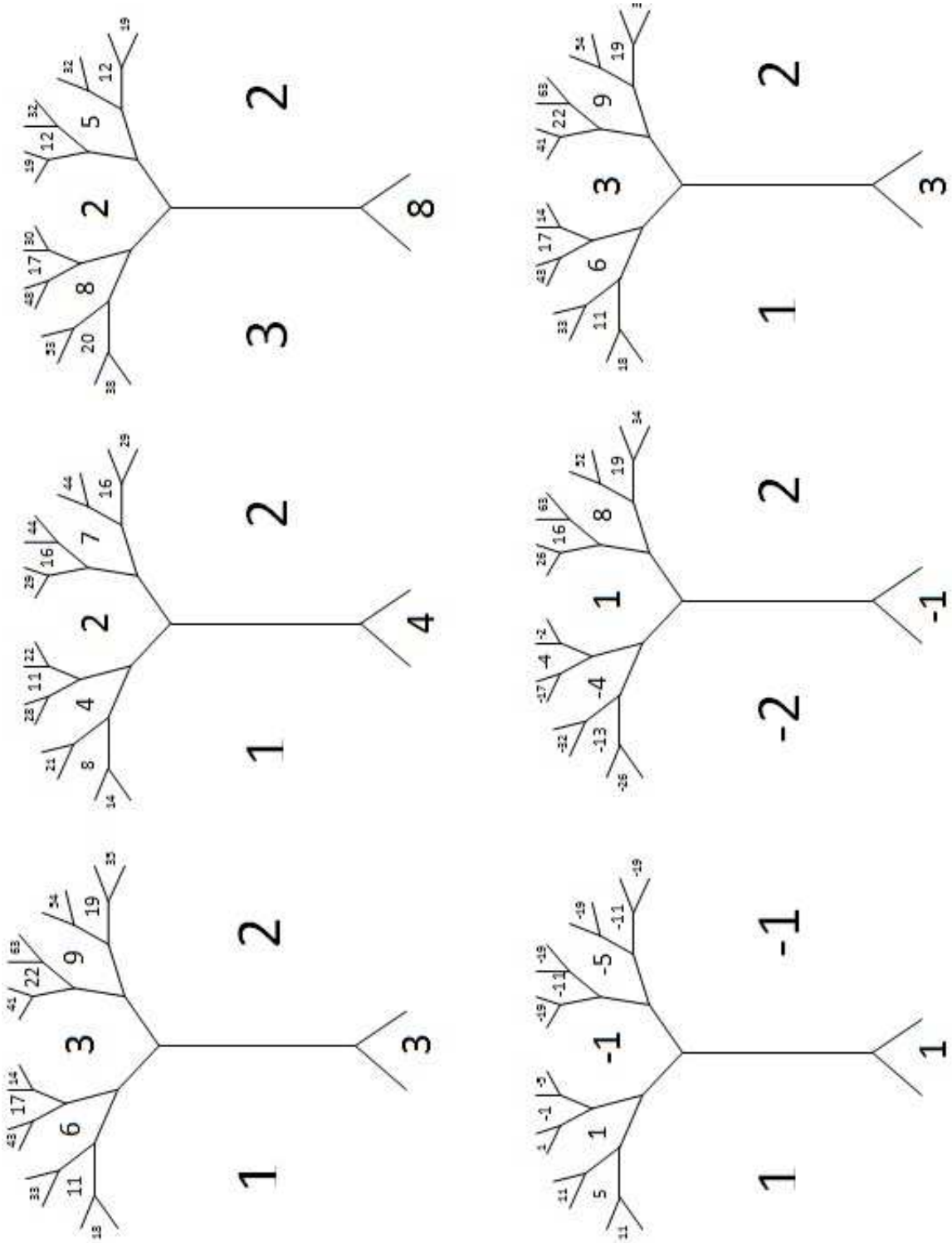
Свойства карты:

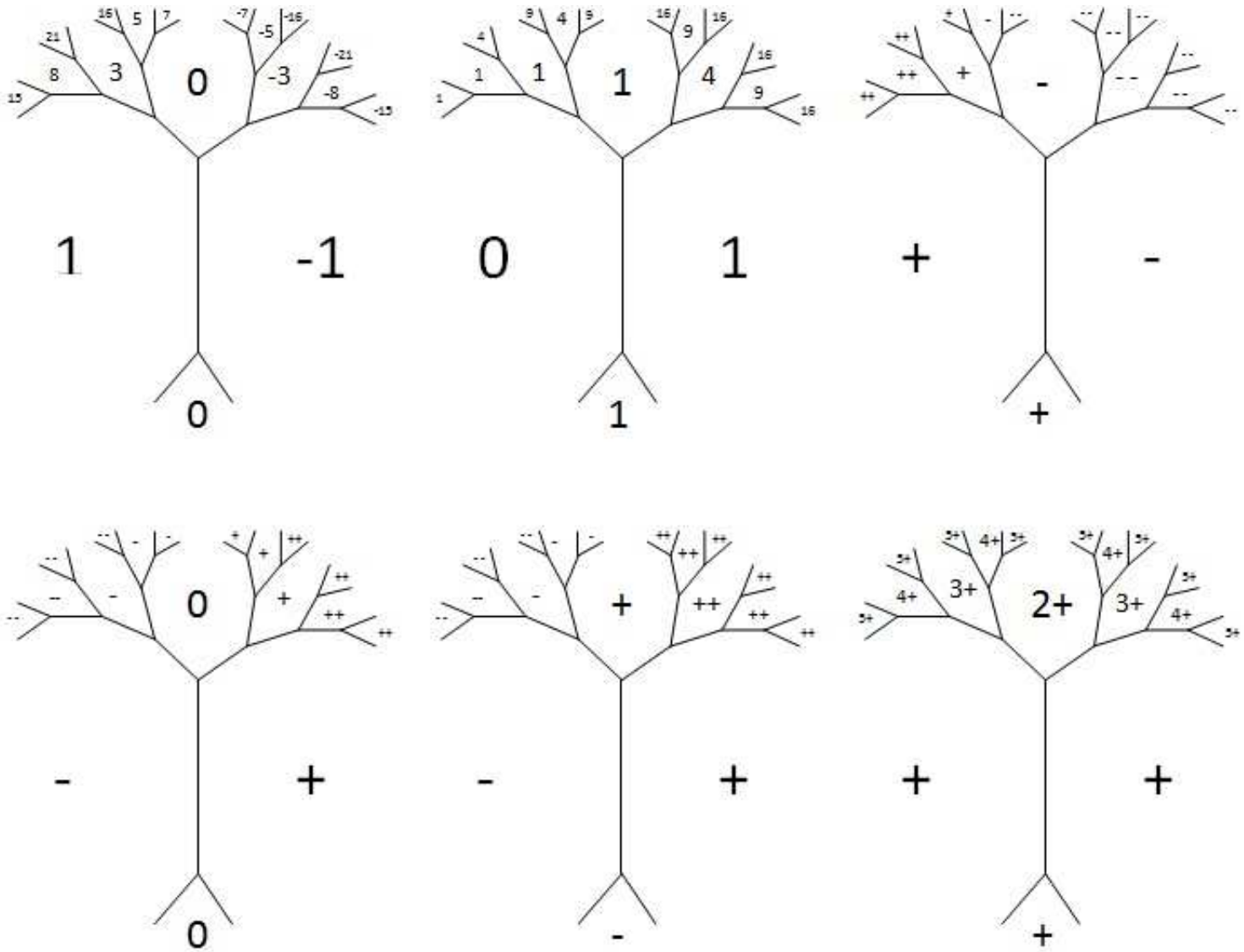
1) точкам графа Γ_f соответствуют квадратичные формы, эквивалентные форме f с точностью до линейной замены;

2) грани Γ_f находятся во взаимно однозначном соответствии с ненулевыми рациональными числами $\frac{m}{n}$;

3) внутри каждой грани написано число, равное значению $f(m,n)$ на соответствующей $\frac{m}{n}$ паре целых чисел (m,n);

4) квадратичные формы f и g эквивалентны с точностью до линейной замены, если и только карты Γ_f и Γ_g одинаковы.


1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41


1
-1
0
0
1
1
+
-
+
0
-
+
-
+
-
+
+
+