Цфасман М.А. Алгебраическая геометрия, теория чисел и их приложения к плотным упаковкам

4 мая 2000

В математике существуют периоды и области, которые вдруг начинают бурно развиваться и потом входят в сознание каждого. В теории чисел XX века таким обстоятельством является удивительная связь между числами и функциями, иными словами, между теорией чисел и алгебраической геометрией.

0.1 Числовые и функциональные поля

Теория чисел начинается с рассмотрения кольца целых чисел $\mathbb{Z}$. В этом кольце есть простые числа и простые идеалы (p). Все простые идеалы главные; любой простой идеал максимален. (Нулевой идеал следует рассматривать отдельно.) Фактор $\mathbb{Z}/(p)$ конечен (конечное поле).

Какие ещё кольца обладают такими же свойствами? Можно, например, обратить число 2, т.е. рассмотреть кольцо $\mathbb{Z}\left[\frac{1}{2}\right]$. Тогда исчезает идеал (2), а все остальные идеалы остаются. Можно обратить два числа: $\mathbb{Z}\left[\frac{1}{3}, \frac{1}{7}\right]$. Тогда исчезнут два идеала.

Такие кольца в некотором смысле меньше, чем $\mathbb{Z}$; точнее говоря, сами они больше, но идеалов у них меньше. Кольцо $\mathbb{Z}[i]$ тоже удовлетворяет тому свойству, что фактор по любому простому идеалу является конечным полем. Точно так же можно рассмотреть, например, кольца $\mathbb{Z}[\sqrt{2}]$ и $\mathbb{Z}[\sqrt[10]{1}]$.

Далеко не для всех таких колец любой простой идеал будет главным. Например, это неверно для кольца $\mathbb{Z}[\sqrt{-5}]$.

Теперь можно выделить следующий тип колец. Пусть R — коммутативное кольцо с единицей и без делителей нуля (целостное кольцо). Будем также предполагать, что кольцо нётерово, т.е. если есть строго возрастающая цепочка идеалов (не обязательно простых) $\mathfrak{a}_1 \underset{\neq}{\subset} \mathfrak{a}_2 \underset{\neq}{\subset} \dots$, то эта цепочка конечна. Кроме того, кольцо одномерно, т.е. если есть последовательность простых идеалов $(0) \underset{\neq}{\subset} \mathfrak{p} \subset \mathfrak{p}'$, то $\mathfrak{p} = \mathfrak{p}'$. Одномерность кольца эквивалентна тому, что любой ненулевой простой идеал максимален. Будем также предполагать, что кольцо R конечного типа над $\mathbb{Z}$, т.е. порождено над $\mathbb{Z}$ конечным числом элементов. Наконец, я потребую, чтобы фактор $R/\mathfrak{p}$ был не просто полем, а конечным полем.

Соответствующий кольцу R геометрический объект называется *спектром* кольца. Как множество спектр — все простые идеалы. На этом множестве есть топология (топология Зариского); замкнуты все конечные объединения замкнутых точек, а замкнутыми являются точки, соответствующие максимальным идеалам. Это можно представлять себе как кривую, точками которой являются максимальные идеалы. Кроме того, в стороне есть ещё точка (0), в замыкании которой лежит вся кривая (так называемая *общая точка*).

Какие ещё кольца удовлетворяют выписанным выше условиям? Например, этим условиям удовлетворяет кольцо $\mathbf{Z} = \mathbb{F}_q[t]$ — кольцо многочленов от одной переменной t над конечным полем.

Я напомню основные свойства конечных полей:

- $|\mathbb{F}_q| = q = p^n$, т.е. число элементов конечного поля является степенью простого числа;
- любое конечное тело является полем (т.е. коммутативно);
- мультипликативная группа $\mathbb{F}_q^*$ циклическая;
- для заданного q поле $\mathbb{F}_q$ единственно;
- любое подкольцо является полем, если в кольце есть единица, причём та же самая (естественно сказать, что $\mathbb{F}_q$ — поле размерности 0).
- группа Галуа алгебраического замыкания $\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$ есть $\hat{\mathbb{Z}}$ — проконечное пополнение группы целых чисел; из этого следует, что расширение данной степени единственно и всегда циклично;
- алгебраическое замыкание $\bar{\mathbb{F}}_q = \bigcup\limits_{m\geq 1} \mathbb{F}_{q^m}$.

Задача 0.1. *Содержит ли $\mathbb{F}_8$ подполе $\mathbb{F}_4$?*

Простые идеалы в $\mathbf{Z} = \mathbb{F}_q[t]$ имеют вид $\big(P(t)\big)$, где P — многочлен, неприводимый над $\mathbb{F}_q$. Если многочлен P неприводим и $\deg P = m$, то $\mathbf{Z}/\big(P(t)\big) = F_{q^m}$, т.е. фактор — конечное поле.

Если присоединить две независимые переменные, то фактор уже не обязательно будет конечным. Например, $\mathbb{F}_q[t,x]/(x) = \mathbb{F}_q[t]$ — бесконечное кольцо (даже не поле). Но если взять неприводимый многочлен $Q(t,x)$ от двух переменных, то факторкольцо $\mathbb{F}_q[t,x]/\big(Q(t,x)\big)$ обладает всеми теми свойствами, о которых говорилось раньше. В этом кольце не любой идеал будет главным, но такого требования и не было.

Обсудим подробнее последний пример. Уравнение $Q(t,x) = 0$ задаёт некоторую кривую. Кольцо $\mathbb{F}_q[t,x]/\big(Q(t,x)\big)$ — это кольцо регулярных рациональных функций на этой кривой (функция $R(t,x)/S(t,x)$ регулярна на кривой, если S не обращается в нуль в точках кривой; заметим, что точка кривой — это точка не обязательно с координатами из $\mathbb{F}_q$, а и из любого его алгебраического расширения). Здесь мы уже дошли до геометрии. Например, кольцо $\mathbb{F}_q[t, \sqrt{t^3-1}]$ соответствует эллиптической кривой $y^2 = t^3 - 1$.

О кривых над конечным полем часто бывает удобно думать, как о кривых над полем рациональных чисел с некоторыми небольшими отличиями. Когда есть кривая с рациональными коэффициентами, для нас естественно сначала рассмотреть её комплексные точки, затем вещественные, а уже затем рациональные. Для конечного поля это соответствует рассмотрению точек над его замыканием.

Факт 0.1. *Пусть кольцо R удовлетворяет тем свойствам, которые сформулированы на с. 1; K — его поле частных. Тогда либо* $\operatorname{char} K = 0$ *и* $[K : \mathbb{Q}] < \infty$ *(поле K является конечным расширением поля рациональных чисел), либо* $\operatorname{char} K = p$ *и* $[K : \mathbb{F}_q(t)] < \infty$ *(поле K является конечным расширением поля рациональных функций от одной переменной над полем $\mathbb{F}_q$). Более того, во втором случае существует единственное число q и единственная кривая X (гладкая и проективная) над полем $\mathbb{F}_q$, для которой $K = \mathbb{F}_q(X)$ (поле рациональных функций на X).*

Для тех, кто привык к комплексной геометрии, нужно сказать следующее. Можно взять поле $\bar{\mathbb{F}}_q(X)$ и рассмотреть только те функции, которые инвариантны относительно действия группы Галуа $\operatorname{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$. Равным образом, то, что на алгебраическом языке называется точкой степени m, на геометрическом языке есть орбита группы Галуа, состоящая из m точек.

Определение. *Поля K, описанные в факте 0.1, называют* глобальными. *В первом случае поля называют* числовыми, *а во втором* функциональными.

Кроме того, имеет место факт, который описывает подкольца в K интересующего нас типа. Чтобы его сформулировать, нужно напомнить определение целого алгебраического числа. Число $a \in K$ называют *целым*, если a — корень многочлена $x^m + a_1x^{m-1} + \dots + a_m$, где $a_i \in \mathbb{Z}$.

Факт 0.2. *Пусть $\mathcal{O}$ — кольцо целых в поле K, S — конечное множество простых идеалов в $\mathcal{O}$. Если обратить идеалы из S, то получим кольцо $\mathcal{O}_S$. В числовом случае кольца вида $\mathcal{O}_S$ в K — это в точности подкольца, удовлетворяющие условиям, сформулированным на с. 1.*

Задача 0.2. *Сформулируйте аналогичный результат в функциональном случае, как на алгебраическом, так и на геометрическом языке.*

Аналогия между числами и функциями не только удивительна, но и очень продуктивна. По этому поводу можно приводить много разных соображений. Я ограничусь одним примером.

В анализе известна дзета–функция Римана

$$\zeta_{\mathbb{Z}}(s) = \zeta_{\mathbb{Q}}(s) = \sum_{n>0} \frac{1}{n^s} = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}.$$

Ряд сходится при $\operatorname{Re} s > 1$. Задаваемую этим рядом функцию можно продолжить на всю плоскость; в точке 1 эта функция имеет простой полюс. Дзета–функция Римана удовлетворяет следующему функциональному уравнению. Рассмотрим функцию

$$\Lambda_{\mathbb{Q}}(s) = \pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta_{\mathbb{Q}}(s).$$

Тогда

$$\Lambda_{\mathbb{Q}}(1-s) = \Lambda_{\mathbb{Q}}(s).$$

Риман высказал гипотезу, что все нули дзета–функции, кроме тривиальных нулей в целых точках $-n$, лежат на прямой $\operatorname{Re} s = \frac{1}{2}$. Эта гипотеза не доказана. Для теории чисел эта гипотеза (и её различные обобщения) чрезвычайно важна.

Для любого кольца R описанного выше типа тоже можно построить аналогичную дзета–функцию

$$\zeta_R(s) = \sum_{\mathfrak{a}} \frac{1}{N(\mathfrak{a})^s} = \prod_{\mathfrak{p}} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1}.$$

Здесь $N(\mathfrak{a})$ — норма идеала $\mathfrak{a}$, т.е. количество элементов кольца $R/\mathfrak{a}$.

Функция $\zeta_R(s)$ явно зависит от кольца R: если обратить один из идеалов, то один из множителей выпадет. А вот соответствующая функция $\Lambda_R(s)$ уже будет зависеть только от поля частных K. Эту функцию можно обозначить $\Lambda_K(s)$.

Например, для поля $\mathbb{F}_q(t)$ функция Λ выглядит очень просто:

$$\Lambda_{\mathbb{F}_q(t)}(s) = \frac{1}{(1-q^{-s})(1-q^{1-s})}.$$

Более того, в функциональном случае она всегда имеет вид

$$\frac{P_X(q^{-s})}{(1-q^{-s})(1-q^{1-s})},$$

где P_X — многочлен степени $2g$ (удвоенный род гладкой кривой X, задающей функциональное поле).

В функциональном случае дзета–функция имеет весьма простой вид; для неё гипотеза Римана доказывается. Это типичная ситуация: в функциональном случае обычно задачи решаются проще, чем в числовом.

Аналогии между числовыми полями и функциональными не всегда прямые. Прежде всего ясно, что кольцу $\mathbb{Z}$ соответствует кольцо $\mathbf{Z} =$

$\mathbb{F}_q[t]$; для каждого q кольцо своё. Простому идеалу (p) соответствует простой идеал $\big(P(t)\big)$, где P — неприводимый многочлен. Для чисел есть функция $\operatorname{sgn}: \mathbb{Z} \setminus \{0\} \to \{\pm 1\}$. Её аналог $\operatorname{sgn}: \mathbf{Z} \setminus \{0\} \to \{\mathbb{F}_q^*\}$ устроен следующим образом: многочлену $Q(t)$ сопоставляется его старший коэффициент. В функциональном случае тоже можно определить аналоги чисел e и π; можно определить гамма–функцию. Этим очень много занимался L. Carlitz и его школа.

0.2 Упаковки шаров

Упаковки шаров меня интересуют не сами по себе, а как приложение той связи между теорией чисел и геометрией, о которой было только что рассказано.

Рассмотрим в евклидовом пространстве $\mathbb{R}^N$ непересекающиеся открытые шары одинакового радиуса. Такого рода объект называют *упаковкой шаров*. Чтобы задать упаковку шаров, достаточно задать радиус шаров и множество их центров $P \subset \mathbb{R}^N$. При этом радиус даже не обязательно задавать — мы всегда будем предполагать, что он максимальный допустимый, т.е. диаметр шаров равен $d = \min\limits_{x \neq y,\, x,y \in P} \|x - y\|$.

Есть задача о том, как плотнее всего паковать шары. Эта задача фигурирует в двух видах: для произвольного множества центров и для множества центров $L \subset \mathbb{R}^N$, которое является решёткой (дискретной аддитивной подгруппой в $\mathbb{R}^N$ полного ранга).

Плотность упаковки $\Delta(P)$ определяется как предел

$$\lim \frac{\text{объём шаров в коробке}}{\text{объём коробки}}.$$

Если такого предела не существует, то можно рассмотреть верхний (или нижний) предел.

В случае решётки фундаментальный параллелепипед содержит несколько частей разных шаров, из которых параллельными переносами складывается в точности один шар. Поэтому

$$\Delta(L) = \frac{V_N d^N}{2^N \operatorname{covol}(L)},$$

где V_N — объём шара радиуса 1, $\operatorname{covol}(L)$ — объём фундаментального параллелепипеда решётки L (кообъём решётки).

В малых размерностях плотнейшими решётками являются решётки, связанные с системами корней: A_1, A_2, A_3, D_4, D_5, E_6, E_7, E_8. Однако бесконечные семейства A_n и D_n (а также B_n и C_n, которые к ним сводятся) асимптотически плохи. Для них Δ ведёт себя как n^{-n}. Не исключено, что у них есть интересные подрешётки, но мы их не знаем.

В основном меня будет интересовать случай, когда N велико. Об асимптотике проще говорить. Если дано семейство решёток $\{L_N \subset$

$\mathbb{R}^N\}$, $N \to \infty$, то для него можно определить предельную плотность. При этом нельзя просто взять предел плотностей, потому что такой предел заведомо равен нулю. Сначала нужно угадать асимптотику зависимости максимальной плотности от размерности. А именно, для каждой решётки $L \subset \mathbb{R}^N$ определим число $\lambda(L)$ формулой

$$\Delta(L) = 2^{-\lambda(L)N}$$

и назовём его *логарифмической* плотностью. Теперь предельную логарифмическую плотность семейства можно определить так:

$$\lambda(\{L_N\}) = \limsup \lambda(L_N).$$

Семейство решёток $\{L_N\}$ называют *асимптотически хорошим*, если $\lambda(\{L_N\}) < \infty$.

Такое определение оправдано по следующим причинам. Известно, что для любого семейства $\{L_N\}$ выполняется неравенство $\lambda(\{L_N\}) \geq 0,5990\ldots$. Кроме того, известно, что существуют семейства $\{L_N\}$, для которых $\lambda(\{L_N\}) = 1$ (теорема Минковского). Эта теорема доказывается методом интегрирования по всем решёткам. Средняя асимптотическая плотность равна 1. Более того, в некотором смысле почти любое семейство решёток имеет логарифмическую плотность 1, т.е. 2^{-N} — типичная плотность решётки.

Вопрос о том, существуют ли семейства $\{L_N\}$, для которых $\lambda(\{L_N\}) < 1$, до сих пор открыт.

Придумать семейство решёток с конечной логарифмической плотностью не так уж просто. Те примеры, которые сразу приходят в голову, дают семейства решёток с бесконечной логарифмической плотностью. Первые в том или ином смысле явные примеры семейств решёток с конечной логарифмической плотностью были построены методами алгебраической геометрии и алгебраической теории чисел. Наиболее важны для этих целей конструкции из алгебраической теории чисел, предложенные, с совершенно иными целями, Дирихле и Дедекиндом.

Пусть K — числовое поле, причём $[K : \mathbb{Q}] = n = s + 2t$, где числа s и t определяются следующим образом. Число s равно количеству вложений $\sigma_i : K \to \mathbb{R}$, а число t равно количеству пар комплексно сопряжённых вложений $\tau_j : K \to \mathbb{C}$ (образы которых не лежат в $\mathbb{R}$). Нетрудно доказать, что размерность K над $\mathbb{Q}$ действительно равна $s + 2t$.

Рассмотрим теперь все вложения одновременно: $K \subset \mathbb{R}^s \times \mathbb{C}^t$. Отождествим $\mathbb{C}$ с $\mathbb{R}^2$, переводя $a + bi$ в $(a + b, a - b)$. Тогда $\mathbb{R}^s \times \mathbb{C}^t$ отождествляется с $\mathbb{R}^n$. Поле K вложено в $\mathbb{R}^n$ как аддитивная подгруппа, $\sigma : K \to \mathbb{R}^n$. Оказывается, что образ кольца целых $\mathcal{O}_K$ в $\mathbb{R}^n$ — решётка полного ранга. Чтобы оценить плотность этой решётки, нужно знать кообъём и минимальное расстояние между её точками. Для решётки минимальное расстояние — это минимальная длина вектора.

Определение. $\operatorname{covol}\mathcal{O}_K = \sqrt{|D_K|}$, *где* $|D_K|$ — *абсолютная величина дискриминанта поля* K. *(Для нас — это определение абсолютной величины дискриминанта.)*

Дискриминант — это некий очень важный параметр поля. Позже я скажу, в каких формулах он встречается.

Теперь поговорим о минимальной норме. Для простоты будем предполагать, что $t = 0$. Пусть $a \in \mathcal{O}_K$. Тогда

$$|\sigma(a)| = \sqrt{\sum \sigma_i(a)^2} \geq \sqrt{n\left(\prod \sigma_i(a)\right)^{2/n}} \geq \sqrt{n}.$$

Последнее неравенство следует из того, что число $\prod \sigma_i(a)$ целое, поскольку a — целое алгебраическое. Действительно, имеет место следующий факт.

Факт 0.3. *Если* a — *корень многочлена* $x^n + a_1x^{n-1} + \cdots + a_n$ *с целыми коэффициентами, то*

$$(-1)^n a_n = N_{K/\mathbb{Q}}(a) = \prod \sigma_i(a) \prod \left(\tau_j(a)\bar{\tau}_j(a)\right).$$

Полученная оценка минимальной нормы точная; она достигается для целого числа 1. Та же самая оценка верна и точна для любых полей. (Проверьте!) Векторы минимальной длины суть образы корней из единицы в поле K.

Итак, плотность решётки оценена через некоторые числовые инварианты поля (дискриминант и размерность над $\mathbb{Q}$). Теперь возникает задача построения семейств полей, для которых эта плотность велика. Пока я про эту задачу говорить не буду, потому что там используется существенно более тонкая теория чисел.

В теории алгебраических чисел есть фундаментальная теорема Дирихле о единицах; она описывает все обратимые элементы в кольце целых для любого конечномерного поля алгебраических чисел. Она доказывается с помощью рассмотрения некоторой другой решётки. Для построения предыдущей решётки использовалась аддитивная структура поля. Теперь нам понадобится мультипликативная структура. Чтобы перевести мультипликативную структуру в аддитивную, нужно взять логарифм. А именно, рассмотрим отображение $K^* \to \mathbb{R}^{s+t}$, заданное формулой

$$a \mapsto (\ln|\sigma_1(a)|, \ldots, \ln\left(\tau_1(a)\bar{\tau}_1(a)\right), \ldots).$$

Чтобы получить решётку, ограничим это отображение на $\mathcal{O}_K^*$ — множество единиц поля K. (Число $a \in K$ называют *единицей*, если $a \in \mathcal{O}_K$ и $a^{-1} \in \mathcal{O}_K$.) Оказывается, что образ множества $\mathcal{O}_K^*$ лежит в гиперплоскости $H = \{\sum x_i = 0\}$ и является в этой гиперплоскости решёткой полного ранга.

Нам нужно ещё одно важное теоретико-числовое понятие — *регулятор* поля K. Пусть L — это та решётка, которая только что была построена. Тогда регулятор R_K определяется формулой

$$\operatorname{covol}(L) = \sqrt{s+t}R_K.$$

Отображение $K^* \to \mathbb{R}^{s+t}$ имеет ядро, которое состоит их корней из единицы, лежащих в поле K.

Длину минимального вектора сейчас я считать не буду, потому что это сложно. Кроме того, я хочу рассказать некоторую конструкцию, позволяющую это сделать просто.

В этом месте нельзя не сделать отступление и не рассказать о следующем поразительном факте. Оказывается, что все встретившиеся нам числа связаны между собой следующим образом:

$$\operatorname*{Res}_{s=1} \zeta_K(s) = \frac{R_K h_K}{w_K \sqrt{|D_K|}}.$$

Здесь h_K — число классов идеалов поля K, которое определяется следующим образом. Идеалы в кольце целых поля K образуют мультипликативную группу. Фактор этой группы по подгруппе, состоящей из главных идеалов, конечен. Число элементов факторгруппы — это и есть h_K. Далее, w_K — число корней из единицы, лежащих в K.

Эта формула показывает, что значительная часть нужной нам информации содержится в дзета–функции. Именно работа с дзета–функцией позволяет всё посчитать.

Теперь нужно вспомнить то, с чего я начинал: алгебраические числа и алгебраические функции — это одно и то же. Мне будет проще говорить на геометрическом языке. Вам придётся мне поверить, что то, что я называю прямыми аналогиями, действительно таковыми является. Это легко проверяется, но у меня сейчас нет для этого времени.

Рассмотрим гладкую проективную неприводимую кривую X над полем $\mathbb{F}_q$. Пусть n — количество точек кривой, определённых над основным полем. Мы будем предполагать, что $n > 0$. Действовать по прямой аналогии здесь плохо. По прямой аналогии нужно было бы сказать, что K — рациональные функции, K^* — ненулевые рациональные функции, а нас интересуют целые рациональные функции, т.е. не имеющие полюсов. Но таких функций немного — только константы. Здесь нужно вспомнить, что некоторые идеалы можно обратить.

Пусть $S = X(\mathbb{F}_q)$ — множество точек кривой, определённых над основным полем. Рассмотрим кольцо $\mathcal{O}^*_{K,S}$, состоящее из рациональных функций на X, все нули и полюса которых лежат в S. При этом нужно помнить, что если расширить поле $\mathbb{F}_q$, то на кривой появятся точки, отличные от S. Аналог этой ситуации такой: у кривой может быть мало вещественных точек, но много комплексных.

Пусть $S = \{P_1, \dots, P_n\}$. Зададим отображение

$$\mathcal{O}^*_{K,S} \to \mathbb{Z}^n \subset \mathbb{R}^n,$$

сопоставив функции f набор $(a_1, \dots, a_n)$ коэффициентов её *дивизора* $\sum a_i P_i$, где

$$a_i = \begin{cases} k, & \text{если в точке } P_i \text{ функция } f \text{ имеет нуль кратности } k; \\ -k, & \text{если в точке } P_i \text{ функция } f \text{ имеет полюс кратности } k; \\ 0, & \text{если в точке } P_i \text{ у функции } f \text{ нет ни нуля, ни полюса.} \end{cases}$$

Как и в комплексном случае, выполняется равенство $\sum a_i = 0$, т.е. сумма кратностей нулей равна сумме кратностей полюсов. Это означает, что образ функции f лежит в гиперплоскости $H = \{\sum x_i = 0\}$. В числовом случае в образе отображения лежали только корни из единицы, и теперь в образе отображения лежат только корни из единицы, поскольку функции без нулей и полюсов — ненулевые константы.

Образ функции — это главный идеал; дивизоры и идеалы это более или менее одно и то же. Кообъём covol выражается через кообъём пересечения целочисленной решётки с гиперплоскостью H и через индекс нашей решётки в этой целочисленной решётке. (Решётки являются группами; индекс одной решётки в другой — это то же самое, что индекс подгруппы в группе.) Индекс не превосходит числа классов идеалов, поэтому

$$\operatorname{covol} \le h_K \operatorname{covol}(\mathbb{Z}^n \bigcap H) = h_K \sqrt{n}.$$

Из алгебраической геометрии известно, что h_K равно числу точек на $J_X(\mathbb{F}_q)$ (якобиане кривой, определённом над основным полем). Якобиан — это абелево многообразие (тор), так сказать, комплексной размерности g. Точек, определённых над конечным полем, на нём конечное число.

Мы оценили кообъём. Оценим теперь длину минимального вектора. Нам нужно оценить снизу число $\sqrt{\sum a_i^2}$. Число a_i целое, поэтому $a_i^2 \ge |a_i|$. Следовательно,

$$\sqrt{\sum a_i^2} \ge \sqrt{\sum |a_i|} = \sqrt{2 \sum_{a_i > 0} |a_i|} = \sqrt{2 \deg f}.$$

Равенство $\sum_{a_i>0} |a_i| = \deg f$ можно объяснить так. Число $\sum_{a_i>0} |a_i|$ равно количеству прообразов нуля при отображении f. Это число равно степени отображения f.

Мы приходим к задаче об оценке минимально возможной степени функции f. Прямую на прямую можно отобразить со степенью 1. Для любой кривой рода $g \ge 1$ требуется более высокая степень. Минимальную такую степень нужно оценить.

Эту оценку можно получить следующим образом. На $\mathbb{P}^1$ есть точки с координатами из основного поля; ясно, что $|\mathbb{P}^1(\mathbb{F}_q)| = q + 1$. Предположим, что $|X(\mathbb{F}_q)| = N$. Функция f определена над $\mathbb{F}_q$, поэтому она отображает $X(\mathbb{F}_q)$ в $\mathbb{P}^1(\mathbb{F}_q)$. Следовательно, $N \leq (q+1)\deg f$. Оценка для степени получена. Она, в свою очередь, даёт оценку минимальной длины вектора.

По полю K построена $(n-1)$-мерная решётка L_K (возможно, не единственная). Для этой решётки получена оценка плотности $\Delta(L_K) \geq \ldots$ снизу. Эта оценка включает некоторые параметры поля K.

Дальше начинается самое интересное — построение примеров решёток с большой плотностью. Сначала нужно понять, чего мы хотим от кривой (чтобы плотность соответствующей решётки была велика). Оказывается, что мы хотим, чтобы число $|X(\mathbb{F}_q)|$ было возможно больше при заданном роде. Пусть $|X(\mathbb{F}_q)| = n_X$. Известно следующее неравенство

$$n_X \leq q + 1 + 2g_X\sqrt{q}.$$

Оно вытекает из работ А. Вейля, связанных с дзета–функцией. Дринфельд и Влэдуц доказали более сильную асимптотическую оценку:

$$\lim_{g_X \to \infty} \frac{n_X}{g_X} \leq \sqrt{q} - 1.$$

Факт очень неожиданный, но его доказательство весьма просто. Более того, если q — квадрат, то есть пример семейства кривых, для которого

$$\lim_{g_X \to \infty} \frac{n_X}{g_X} = \sqrt{q} - 1.$$

Эти кривые берутся уже из более тонкой алгебраической геометрии. Задача об оценке числа точек кривой трудна потому, что точки на кривой неотличимы друг от друга. Чтобы точки стало легче считать, нужно каждой точке придать нечто индивидуальное. Это можно сделать, рассматривая не просто кривые, а модулярные кривые. Идея модулярных кривых, и вообще модулярных многообразий, заключается в следующем. Пусть E — кривая рода 1. Все кривые рода 1 параметризуются прямой $\mathbb{P}^1$. Можно рассматривать пары

$$(E, \text{дополнительные данные}).$$

Тогда возникает накрытие кривой E пространством параметров, точками которого служат эллиптические кривые с дополнительными данными, которые называют *структурой уровня*. Так получается много разных кривых, род которых при изменении структуры уровня может стремиться к бесконечности. В случае конечной характеристики среди всех эллиптических кривых выделяются *суперсингулярные кривые*. Оказывается, что для любой естественной (не буду уточнять, что это такое) структуры уровня все точки, которые лежат над суперсингулярными эллиптическими кривыми, определены хотя и не над самим исходным полем, но над его расширением степени 2. А именно, если исходное поле $\mathbb{F}_{\sqrt{q}}$, то все точки модулярных кривых будут определены над $\mathbb{F}_q$. Оказывается, что этих точек будет очень много. Таков один из способов построения кривых.

В числовом случае этот способ не действует. Одна из важных нерешённых задач в этой области связана с построением башен полей, которые в каком-то смысле были бы аналогичны модулярным кривым.

В числовом случае приходится обходиться другими средствами — *теорией полей классов*. В теории полей классов строят так называемые *башни Голода–Шафаревича*. Это название связано с тем, что Голод и Шафаревич разрешили в отрицательном смысле проблему Гильберта, построив бесконечную последовательность неразветвлённых абелевых расширений

$$K_0 \subset K_1 \subset K_2 \subset \dots$$

Например, для $K_0 = \mathbb{Q}\left(\cos\frac{2\pi}{11}, \sqrt{-46}\right)$ такая башня даёт семейство решёток с $\lambda(\{L_N\}) \approx 2,22$. Это число больше 1, но результат не такой уж плохой. Когда начинали заниматься построением плотных упаковок, то без использования алгебраической геометрии и теории чисел семейства решёток с конечным λ построить вообще не удалось, а для нерешётчатых упаковок было построено семейство с $\lambda = 6$.

В геометрическом случае, используя модулярные кривые, можно добиться лучших результатов. Там есть два типа конструкций. Одна — буквально та, о которой я говорил. А в другой рассматривается некоторая её подрешётка, связанная с дивизором. В первом случае нужно взять $q = 9$, а во втором $q = 47^2$. Соответственно, получим $\lambda \approx 1,87$ и $\lambda \approx 1,39$.

В математике известно много других решёток. Например, если взять эллиптическую кривую над числовым или функциональным полем, то её целые точки образуют решётку. Элкис и Шиода посчитали плотность возникающих решёток. Оказалось, что асимптотически эти решётки плохи, но поразительно хороши в размерностях между 100 и 1000. Многие табличные рекорды плотности оказались таким образом побиты.

Здесь собрались представители различных областей математики. Мой призыв: в вашей области наверняка встречаются решетки — не поленитесь проверить их на плотность, может быть, вы найдёте новые интересные семейства.