В. И. Арнольд

ДИНАМИКА, СТАТИСТИКА И ПРОЕКТИВНАЯ ГЕОМЕТРИЯ ПОЛЕЙ ГАЛУА

Москва
Издательство МЦНМО
2005

УДК 511
ББК 22.13
А84

Арнольд В. И.

А84 Динамика, статистика и проективная геометрия полей Галуа. — М.: МЦНМО, 2005. — 72 с.

ISBN 5-94057-222-7

В этой книге, являющейся записью прочитанной автором 13 ноября 2004 года лекции для школьников Малого мехмата МГУ, рассказано об удивительных недавно открытых связях алгебраической теории полей Галуа с теорией динамических систем, хаоса и статистики с одной стороны и с геометрией проективных структур на множествах из конечного числа точек — с другой.

Бóльшая часть этих новых открытий обнаружена экспериментальным путём, а возникшие при этом гипотезы во многих случаях ещё не доказаны, хотя и их понимание, и их эмпирическая проверка легко доступны школьникам, особенно владеющим компьютером.

Ждут пытливых исследователей и многие теоретические вопросы — например, напрашивающийся вопрос о том, чем выделяется подгруппа проективных перестановок в полной группе всех перестановок конечного множества, каковы специальные геометрические свойства проективных перестановок дюжины точек, отличающие эти перестановки от непроективных.

ББК 22.13

Владимир Игоревич Арнольд

Динамика, статистика и проективная геометрия полей Галуа

Подписано в печать 6.12.2005 г. Формат $60 \times 90\ ^1/_{16}$. Бумага офсетная. Печать офсетная. Печ. л. 4,5. Тираж 3000 экз. Заказ № .

Издательство Московского центра
непрерывного математического образования
119002, Москва, Большой Власьевский пер., 11. Тел. 241-74-83.

Отпечатано с готовых диапозитивов в ФГУП «Полиграфические ресурсы».

ISBN 5-94057-222-7

ОГЛАВЛЕНИЕ

§ 1
ЧТО ТАКОЕ ПОЛЕ ГАЛУА?

Поля Галуа — это поля из конечного числа элементов. Они относятся к небольшому набору самых фундаментальных объектов математики, при помощи которых описываются все другие математические структуры и модели.

Всем известный пример подобных фундаментальных объектов — простые числа, $p = 2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots, 997, \ldots$, т. е. целые положительные числа, делящиеся нацело только на два целых числа: на себя и на единицу (которую простым числом не считают).

Первый же естественно-научный вопрос, возникающий при рассмотрении простых чисел, уже довольно труден: *конечно ли количество простых чисел*, или же последовательность простых чисел продолжается неограниченно? Ответ на этот вопрос получен несколько тысячелетий назад: *последовательность простых чисел не ограничена*, *самого большого простого числа нет.*

Это видно, например, из того, что большое число

$$(2 \cdot 3 \cdot 5 \cdot \ldots \cdot p) + 1$$

даёт в остатке единицу при делении на каждое простое число до p включительно, а потому не делится ни на одно из них. Из этого следует, что это большое число имеет простой делитель, больший чем p, а значит, *наибольшего простого числа не может существовать.*

Это замечательное математическое рассуждение оставляет для естествоиспытателя открытым главный вопрос: *насколько часто* встречаются простые числа в натуральном ряду, растут ли интервалы между ними по мере роста чисел? Насколько велико миллионное простое число?

Первым естествоиспытателем, занявшимся этими вопросами, был Лежандр, исследовавший в XVIII веке все простые числа до миллиона и заметивший следующий *закон убывания плотности простых чисел*: среднее расстояние между последовательными простыми числами, близкими к числу n, растёт с ростом n как $\ln n$ (натуральный логарифм, т. е. логарифм при основании $e = 2{,}71828...$). Например, $\ln 10 \approx 2{,}3$, а в районе значения $n = 10$ среднее расстояние между последовательными простыми числами немного больше двух ($7 - 5 = 2$, $11 - 7 = 4$, $13 - 11 = 2$). Поблизости от числа $n = 100$ последовательность простых состоит из чисел 89, 97, 101, 103, так что среднее расстояние между соседями есть $4\frac{2}{3}$, тогда как $\ln 100 = 2 \ln 10 \approx 4{,}6$.

Разумеется, наличие «близнецов» (пар простых чисел с разностью 2) препятствует постоянному росту самого расстояния с ростом чисел, но *среднее* расстояние может расти с n, даже если число пар близнецов и бесконечно (так что существуют сколь угодно большие близнецы — эта знаменитая гипотеза о бесконечности числа пар близнецов, до сих пор не доказанная и не опровергнутая, считается одной из важнейших задач теории чисел).

К сожалению, наблюдения Лежандра не были признаны математиками за научное достижение, так как он «ничего не доказал, а только рассмотрел миллионы примеров» (и обобщил полученные в этих примерах эмпирические статистические данные), вовсе не умея строго перейти к пределу при неограниченном возрастании числа n.

Колмогоров не раз говорил мне о своих исследованиях гидродинамической турбулентности: «Не ищите там теорем, их нет, я ничего не умею выводить из исходных для этой теории уравнений Навье—Стокса. Мои результаты об их решениях *не доказаны*, *а верны* — что гораздо важнее всех доказательств».

Первым оценил достижение Лежандра русский математик Чебышёв. Прежде всего он доказал, что если изучаемое среднее расстояние между близкими к n простыми числами и не ведёт себя асимптотически как $\ln n$, то оно всё же в среднем отличается от такого выражения *не более чем в конечное число раз*, т. е. заключено между $c_1 \ln n$ и $c_2 \ln n$ (с явно найденным постоянными, $c_1 < c_2$).

Позже он доказал больше: если колебания между указанными границами «затухают» при увеличении числа n, так что устанавливается асимптотика $c \ln n$ среднего расстояния между близкими к n простыми числами, то *постоянная c может быть только единицей*.

Это ещё не *доказывает* асимптотики Лежандра, так как не исключает возможности вечно продолжающихся колебаний между $c_1 \ln n$ и $c_2 \ln n$ без установления предельного режима $c \ln n$.

Но не прошло и ста лет после открытия Лежандра, как два знаменитых математика, француз Адамар и бельгиец Валле Пуссен, доказали затухание этих колебаний, т. е. *существование* предельной асимптотики $c \ln n$.

С тех пор считается, что Адамар и Валле Пуссен сделали великое открытие — обнаружили статистический закон распределения больших простых чисел.

С моей точки зрения приписывать это открытие Адамару и Валле Пуссену — сильная несправедливость. Ведь эти (действительно замечательные) математики доказали только *существование* некоторого (равного неизвестному им c) предела. И открытие естественно-научного факта (пропорционального в среднем величине $\ln n$ роста расстояния между

последовательными простыми числами), и вычисление предела c (равного на самом деле 1) — и то и другое сделано не ими, а Лежандром и Чебышёвым, которым и принадлежит на самом деле великое открытие, описанное выше.

В предлагаемых лекциях для школьников я буду следовать скорее Лежандру, чем Адамару: я расскажу об экспериментальных числовых наблюдениях, которые подсказывают новые (поразительные) законы природы, но которые далеко не сразу превращаются в теоремы. Я думаю, что в некоторых случаях доказательств придётся ждать сотню-другую лет (как это произошло и с законом распределения простых чисел), хотя сами открытия новых законов могут быть доступны школьникам (не обязательно владеющим компьютерной техникой, которая всё же может помочь в экспериментальном поиске эмпирических законов, хотя я её и избегал, когда искал те факты, о которых пойдёт речь ниже).

Наряду с простыми числами, другой яркий пример фундаментальных математических объектов — *правильные многогранники* (называемые также «платоновыми телами», так как их открыл не Платон), рис. 1.1. Их пять: тетраэдр, октаэдр, куб, икосаэдр (имеющий 20 треугольных граней, на что указывает греческое числительное «икос») и додекаэдр (имеющий «додека» = 12 пятиугольных граней и использованный Кеплером для описания «четвертым законом Кеплера» распределения радиусов планетных орбит Солнечной системы).

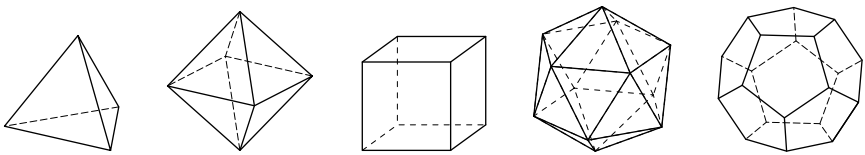


Рис. 1.1. Правильные многогранники

Правильные многогранники неожиданно оказались ответственными за на вид никак не связанную с ними область физики — теорию *оптических каустик*, доставляющую объяснение радуги (с её угловым радиусом 42°, рис. 1.2) с одной стороны и, например, теорию скапливания галактик в крупномасштабной структуре Вселенной — с другой.

Колмогоров говорил, что особенную красоту математическим теориям придаёт именно обнаруживаемое ими *сходство между на вид совершенно разными явлениями природы* (например, сходство между теориями электрического и магнитного полей, доставляемое уравнениями Максвелла).

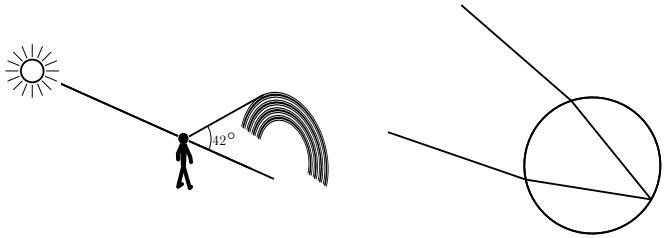


Рис. 1.2. Происхождение радуги

В отличие от описанных выше примеров, поля Галуа пока ещё не нашли физических (или иных естественно-научных) приложений. Я верю, что эти приложения со временем будут найдены, и хотел бы приблизить это время своим геометрическим изложением теории полей Галуа (в духе описания естественно-научных объектов, скорее чем в стиле алгебраически-аксиоматических сверхабстрактных исследований, господствующем в этой алгебраической теории).

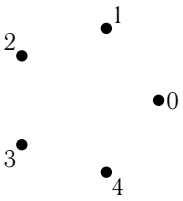


Рис. 1.3. Конечная окружность: поле Галуа $\mathbb{Z}_5$

Простейшим примером поля Галуа является *поле вычетов по модулю простого числа* p (т. е. остатков от деления на p)

$$\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z},$$

рис. 1.3. Например, при $p = 2$ получаем поле двух элементов

$$\mathbb{Z}_2 = \{0, 1\},$$

с обычной арифметикой Митрофанушки:

$$0+0=0, \quad 0+1=1+0=1, \quad 1+1=0,$$
$$0\cdot 0=0\cdot 1=1\cdot 0=0, \quad 1\cdot 1=1.$$

Эта «бинарная» арифметика лежит в основе действующих в двоичной системе компьютеров, так что простейшее поле Галуа имеет массу приложений:

$$(\text{поле } \mathbb{Z}_2) \Rightarrow (\text{компьютеры}).$$

Общее понятие поля совершенно аналогично: две операции (сложения и умножения) удовлетворяют обычным условиям коммутативности, ассоциативности, дистрибутивности, и вдобавок в поле можно делить на любой отличный от 0 элемент.

Остатки от деления на 3 образуют поле $\mathbb{Z}_3$ из трёх элементов (в котором $\frac{1}{2} = 2$, так как $2 \cdot 2 = 1$ для остатков от деления на 3).

Напротив, остатки от деления на 4 поля не образуют, так как элемент 2 не имеет обратного (остаток $2x$ принимает значения 0 и 2, но не равен 1 ни при каком остатке x).

Оказывается, всё же существует поле из четырёх элементов (операции в котором отличны от сложения и умножения остатков). Найти операции в этом поле — интересная и полезная (хотя и не трудная) школьная задача.

Конечные поля называются *полями Галуа* потому, что он открыл их следующие 2 замечательные свойства.

1. Число элементов конечного поля — не любое натуральное число, а число вида p^n, где p — простое число (притом любое), а n — натуральное число (тоже любое).

Таким образом, существуют поля из

$$2,\ 3,\ 4,\ 5,\ 7,\ 8,\ 9,\ 11,\ 13,\ 16,\ 17,\ 19,\ 23,\ 25,\ 27$$

элементов, но нет полей с числами элементов

$$6,\ 10,\ 12,\ 14,\ 15,\ 18,\ 20,\ 21,\ 22,\ 24,\ 26.$$

2. Поле из p^n элементов определяется своим числом элементов однозначно (с точностью до изоморфизма).

Например, компьютер, использующий поле $\mathbb{Z}_2$ в Москве, и другой компьютер, работающий в Петербурге, могут использовать разные копии этого поля. Скажем, в Петербурге элементы поля $\mathbb{Z}_2$ можно было бы обозначить буквами α и β, а операции определить таблицей

$$\alpha + \alpha = \beta + \beta = \beta, \quad \alpha + \beta = \beta + \alpha = \alpha,$$
$$\alpha \cdot \alpha = \alpha, \quad \alpha \cdot \beta = \beta \cdot \alpha = \beta \cdot \beta = \beta.$$

Но заданное этой таблицей поле изоморфно обычному московскому полю вычетов (отличаясь от него только обозначениями, $\alpha \sim 1$, $\beta \sim 0$).

Независимость сущности явлений от обозначений является основой теории относительности и всей релятивистской физики.

Доказательство приведённой теоремы существования и единственности поля из p^n элементов я приводить не буду, а расскажу зато, *как описать операции в этом поле*. Странным образом, я не встречал приведённого ниже естественно-научного описания полей Галуа в литературе.

В каждом поле есть элемент 0 (нуль), прибавление которого к любому элементу не меняет «увеличиваемый» на 0 элемент. Все остальные элементы образуют *мультипликативную группу поля* (группу по умножению), так как на них можно делить.

Оказывается, *эта группа всегда является циклической*: существует такой (*примитивный*) элемент A, что все (ненулевые) элементы поля суть его степени, $\{A, A^2, A^3, \ldots, A^{z-1}\}$ для поля из $z = p^a$ элементов.

Доказывать это утверждение я не буду (хотя это доказательство не слишком трудно), так как оно лишь дополняет объясняемую ниже структуру полей аксиомофильским добавлением: *никаких других конечных полей, кроме изученных ниже полей с циклической мультипликативной группой, не бывает.*

Иными словами, можно при желании считать, что мы добавили к определению конечного поля (коммутативности обеих операций, их ассоциативности, дистрибутивности и т. д.) ещё одну аксиому: существование «*первообразного» элемента* A, степенями которого исчерпываются все ненулевые элементы поля. Именно к таким полям будут относиться все дальнейшие построения, именно они будут нас ниже интересовать.

Тот факт, что *никаких других конечных полей нет*, является (приятным) добавлением к излагаемой ниже содержательной теории, но сама она от этого свойства системы аксиом поля не зависит (и именно преувеличенное внимание к подобным малосущественным деталям исследований зависимости аксиом делает алгебраически-абстрактные построения математиков ненужно трудными и враждебными для естествоиспытателей).

Например, геометрия *плоскости Лобачевского* — это просто геометрия внутренности круга, в которой *точками Лобачевского* называются точки, расположенные строго внутри ограничивающей круг окружности (называемой *абсолютом* и в плоскость Лобачевского не входящей), а *прямыми Лобачевского* называются хорды абсолюта (рис. 1.4).

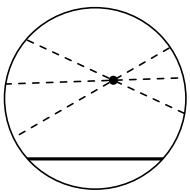


Рис. 1.4. Плоскость Лобачевского

Легко убедиться, что эти объекты (составляющие так называемую «*модель Клейна*») удовлетворяют всем аксиомам геометрии Евклида («через любые две точки проходит одна и только одна прямая» и т. д.), кроме лишь

«аксиомы параллельных»: ведь *через любую точку плоскости Лобачевского* (т. е. точку круга внутри абсолюта) *проходит не одна прямая Лобачевского*, *не пересекающая фиксированную прямую Лобачевского* (т. е. хорду абсолюта), *не проходящую через рассматриваемую точку*, *а бесконечное их множество* (рис. 1.4).

К этим (очевидным) естественно-научным фактам добавляется (трудная) теорема аксиомофилов: *никакой другой плоскости Лобачевского*, *кроме описанной модели Клейна*, *не существует* (с точностью, конечно, до изоморфизма: теорема утверждает, что из аксиом плоскости Лобачевского вытекает изоморфность этой плоскости модели Клейна).

Интересно, что сам Лобачевский вовсе не доказал своего основного естественно-научного (и замечательного) утверждения: *аксиома параллельных геометрии Евклида не зависит от остальных*, *т. е. не может быть выведена из них*.

Изобретённая после работы Лобачевского модель, описанная выше, как раз это и *доказывает*: ведь *если бы из неверности аксиомы параллельных Евклида можно было бы извлечь противоречие* (что и означает доказательство этой аксиомы), *то противоречивой была бы и модель*, *то есть противоречие нашлось бы и в геометрии Евклида* (*хорд одного круга*).

Доказательства фундаментальных фактов часто проще аксиомофильских деталей, заполняющих математические учебники.

§ 2
КАК УСТРОЕНЫ ПОЛЕ ГАЛУА И ЕГО ТАБЛИЦА

Умножение в поле Галуа с n элементами 0 и $\{A^k\}$, $1 \leqslant k \leqslant n-1$, сводится просто к сложению «логарифмов» (показателей k) по модулю $n-1$ (остатков от деления k на $n-1$):

$$0 \cdot A^k = 0, \quad A^k \cdot A^l = A^{k+l}$$

(если $k+l > n-1$, то можно, не меняя остатка при делении на $n-1$, заменить эту сумму на $k+l-(n-1)$), чтобы сделать показатель степени меньшим, чем n).

Остаётся определить операцию сложения. Обозначая элемент A^k поля значком k, мы приходим к следующей «*тропической*» *операции* «$*$» над этими «логарифмами» элементов поля:

$$A^k + A^l = A^{k*l}.$$

[Недавно возникший термин «*тропическая*» (т. е. экзотическая) математика используется всякий раз, когда «уровень» алгебраических операций понижается так, что умножение становится сложением, а сложение переходит в «тропическое сложение» низшего уровня, относительно которого обычное сложение столь же дистрибутивно, как дистрибутивно обычное умножение по отношению к обычному сложению: $x(y+z) = xy + xz$, $x + (y * z) = (x+y) * (x+z)$.

Примером такого тропического сложения является операция «взятие максимума», $x * y = \max(x, y)$ для вещественных чисел.

Эту тропическую операцию можно было бы получить из обычного сложения логарифмированием, соединённым с квантово-механическим «коротковолновым предельным переходом» при стремлении к нулю длины волны h: определение

$$\frac{x *_h y}{h} = \ln(e^{x/h} + e^{y/h})$$

задаёт тропическую операцию $*_h$, которая переходит в $\max(x, y)$ при $h \to 0$.

Хотя всё сказанное очевидно, из него следует нетривиальный «тропический» вывод: заменяя умножения сложениями и сложения максимумами, можно преобразовать многие формулы и теоремы анализа (вроде теории рядов Фурье) в (неочевидные) «тропические» факты теории линейного программирования и выпуклого анализа.]

Рассмотрим для простоты случай поля F из $z = p^2$ элементов. Оно содержит «скалярные» элементы $1, 2 = 1+1, \ldots$ Поскольку поле конечно,

одна из сумм повторится. Значит, некоторая сумма m слагаемых 1 (являющаяся разностью повторившейся суммы и её повторения) есть нуль, $m = 1 + \ldots + 1 = 0$. Пусть m — наименьший нулевой скаляр.

Докажем, что $m = p$. Действительно, объявим любой элемент x эквивалентным любому элементу $x + 1 + \ldots + 1$ (с числом единиц $\leqslant m$). Классы эквивалентности состоят, каждый, из m элементов и попарно не пересекаются, поэтому число скаляров m является делителем числа p^2 элементов поля. Следовательно, m есть либо p, либо p^2.

Второй случай невозможен. Действительно, рассмотрим скалярный элемент $x = 1 + \ldots + 1$ с p слагаемыми. Он не имеет в поле из p^2 элементов обратного элемента, поскольку никакое целое число pq не может дать при делении на p^2 в остатке 1. Значит, $x = 0$, так что число скаляров $m = p$.

Рассмотрим элемент 1 и примитивный элемент A нашего поля. Повторяя каждое из них слагаемым не более p раз, мы получим p^2 сумм $uA + v1$. Все эти суммы — различные элементы нашего поля (иначе мы получили бы в нём $A = -(v/u)1$, поэтому все элементы поля были бы скалярными суммами единиц, что невозможно, так как таких сумм, как мы выше доказали, всего p, а не p^2). Итак, *поле из p^2 элементов состоит в точности из всех линейных комбинаций*

$$F = \{uA + v1\} \quad \text{с коэффициентами} \quad u \in \mathbb{Z}_p,\ v \in \mathbb{Z}_p.$$

В этом смысле мы можем расположить все элементы поля в квадрате размера $p \times p$ (или, лучше, в «конечном торе» $\mathbb{Z}_p^2$, являющемся плоскостью над полем $\mathbb{Z}_p$, рис. 2.1).

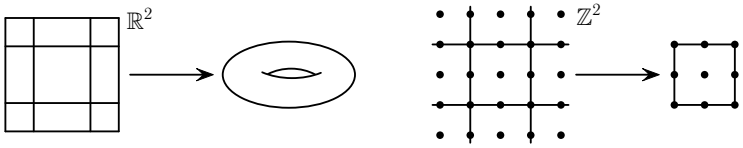


Рис. 2.1. Непрерывный тор и конечный тор из четырех точек

Мы получили, такими образом, заполнение $z = p^2$ клеточек этого конечного тора p^2 символами — «логарифмами» $\{\infty; 1, \ldots, z-1\}$ (где символ k, который можно считать остатком от деления на $z - 1$, изображает элемент A^k поля F, а символ ∞ изображает ноль этого поля)[1].

[1] Школьники — слушатели лекции предложили мне считать логарифмом нуля *минус* бесконечность, но я не согласен на это, так как не уверен, что $A > 1$ в F.

Полученное заполнение описывает «тропическую» операцию $*$ над логарифмическими символами k. А именно, сумма элементов поля с символами k и l

$$A^k = u'A + v'1, \quad A^l = u''A + v''1$$

есть $(u'+u'')A + (v'+v'')1 = A^{k*l}$. Поэтому *номер $k*l$ заполняет в таблице векторную сумму мест, заполненных номерами k и l: операция сложения в поле F из $z = p^2$ элементов описывается векторным сложением мест складываемых элементов в построенной таблице поля* (рис. 2.2).

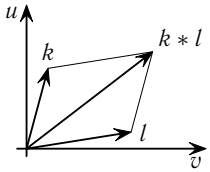


Рис. 2.2. Тропическое сложение показателей k и l в таблице поля

Итак, для описания поля достаточно явно вычислить места (u_k, v_k) всех элементов

$$A^k = u_k A + v_k 1 \quad (1 \leqslant k \leqslant z-1)$$

в таблице поля.

Это вычисление является (лёгким) аналогом построения чисел Фибоначчи, описывающих закон размножения кроликов, $a_{k+2} = a_{k+1} + a_k$. Действительно, пусть в поле

$$A^2 = \alpha A + \beta 1. \qquad (*)$$

Тогда мы находим в нашем поле соотношение

$$A^3 = A(\alpha A + \beta 1) = \alpha(\alpha A + \beta 1) + \beta A = (\alpha^2 + \beta)A + \alpha\beta 1.$$

Точно так же доказывается рекуррентное соотношение, последовательно вычисляющее места элементов A^k в таблице поля,

$$u_{k+1} = \alpha u_k + v_k, \quad v_{k+1} = \beta u_k.$$

Таким образом, два вычета α и β по модулю p (два остатка от деления на p) последовательно определяют места (u_k, v_k) всех элементов поля в его таблице.

Остаётся только выбрать значения параметров α и β. Их нужно выбрать так, чтобы, во-первых, $A^{p^2-1} = 1$, то есть чтобы $u_{p^2-1} = 0, v_{p^2-1} = 1$,

а во-вторых, чтобы вектор (u_k, v_k) из остатков от деления на p отличался от вектора $(0,1)$ при всех предыдущих значениях k $(1 \leqslant k < p^2 - 1)$.

В принципе для выбора α и β достаточно перебрать все p^2 возможных пар остатков (α, β). Этот перебор даже не слишком долог. Например, для $p = 5$ обоим выписанным условиям удовлетворяет уже пара $\alpha = \beta = 2$.

Но можно ещё сильно сократить этот перебор, используя *треугольник Паскаля и биномиальные коэффициенты*. А именно, решение выписанных рекуррентных соотношений выражается через биномиальные коэффициенты (это легко доказать) так:

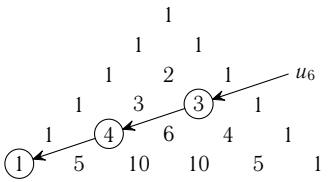
$$u_k = \sum \alpha^s \beta^t C_{s+t}^t,$$

где показатели степеней s и t связаны условием однородности выражения для коэффициента u_k по A, вытекающим из соотношения $(*)$. Это соотношение доставляет веса

$$\deg \alpha = 1, \quad \deg \beta = 2,$$

откуда для $\deg u_k = k - 1$ находим условие однородности $s + 2t = k - 1$, связывающее показатели s и t в слагаемых предыдущей формулы для величины u_k.

Для примера, при $k = 6$ мы получаем из треугольника Паскаля



выражение величины u_6 в виде суммы трёх слагаемых веса 5,

$$3\alpha\beta^2 + 4\alpha^3\beta + 1\alpha^5.$$

Пользуясь этим алгоритмом, я быстро вычислил места всех 24 ненулевых элементов A^k поля из 5^2 элементов. Они заполнили таблицу этого поля,

u					
4	**13**	15	**5**	16	20
3	**7**	10	9	14	**23**
2	**19**	**11**	2	21	22
1	**1**	8	4	**17**	3
0	∞	24	18	6	12
	0	1	2	3	4 v

Пример. $A^{10} = 3 \cdot A + 1 \cdot 1,\ A^{19} + A^8 = A^{10}$.

Замечание. Отмеченный знаком «$\circ$» центр симметрии обладает следующим (легко доказываемым) свойством: если k и l расположены в таблице симметрично относительно этого знака, то $k - l = 12 \pmod{24}$.

Например, $21 - 9 = 12$, $17 - 5 = 12$, $24 - 12 = 12$ $(= (z-1)/2$ для поля из z элементов).

Причиной этой симметрии является очевидное тождество $A^{12} = -1$ (т. е. $u_{12} = 0$, $v_{12} = 4$). Указанная симметрия сокращает вычисление таблицы поля вдвое (достаточно вычислить u_k и v_k при $k \leqslant z/2$), $z = p^n$ — число элементов поля).

Смысл нашей таблицы можно объяснить ещё так. Оператор умножения элементов поля на A^k действует на плоскости таблицы линейно:

$$A^k 1 = u_k A + v_k 1,$$
$$A^k A = u_{k+1} A + v_{k+1} 1.$$

Поэтому матрица этого линейного оператора на плоскости с координатами u и v в её базисе $(1, A)$ имеет вид

$$(A^k) = \begin{pmatrix} v_k & v_{k+1} \\ u_k & u_{k+1} \end{pmatrix}.$$

Для $k = 1$ это матрица

$$(A) = \begin{pmatrix} 0 & \beta \\ 1 & \alpha \end{pmatrix} \quad \left(= \begin{pmatrix} 0 & 2 \\ 1 & 2 \end{pmatrix} \text{ при } p = 5 \right).$$

Уравнение $(*)$ есть просто характеристическое уравнение этой матрицы. А так как умножение на A^k есть k-кратное умножение на A, то матрица (A^k) есть k-я степень матрицы (A).

Стало быть, *наша конструкция таблицы поля доставляет представление поля из p^2 элементов матрицами второго порядка $(A)^k$, элементы которых лежат в $\mathbb{Z}_p$ (являются остатками от деления на p)*.

Операции поля представлены просто как матричное сложение и матричное умножение:

$$(A)^k \cdot (A)^l = (A)^{k+l},$$
$$(A)^k + (A)^l = (A)^{k*l}.$$

Для поля из $z = p^n$ элементов аналогичная конструкция даёт представление поля матрицами порядка n с элементами из $\mathbb{Z}_p$.

Для $p=7$, 11 и 13 вычисления, совершенно аналогичные приведённым выше в случае $p=5$, приводят к следующим ответам:

$$(A)=\begin{matrix} p=7 \\ \begin{pmatrix}0 & 2\\ 1 & 2\end{pmatrix}\end{matrix};\quad \begin{matrix} p=11 \\ \begin{pmatrix}0 & 3\\ 1 & 1\end{pmatrix}\end{matrix};\quad \begin{matrix} p=13 \\ \begin{pmatrix}0 & 2\\ 1 & 4\end{pmatrix}\end{matrix}.$$

Таблица поля из $p^2=49$ элементов (элементы таблицы — остатки mod 48).

$p=7$

u								
6	**25**	44	**7**	30	3	45	42	
5	9	**35**	28	**29**	39	26	14	
4	**17**	**37**	22	36	34	**43**	**47**	
3	**41**	**23**	**19**	10	12	46	**13**	
2	33	38	2	15	**5**	4	**11**	
1	**1**	18	21	27	6	**31**	20	
0	∞	48	32	40	16	8	24	
	0	1	2	3	4	5	6	v

Таблица поля из $p^2=121$ элементов (элементы таблицы — остатки mod 120).

$p=11$

u											
10	**61**	**11**	15	76	22	**43**	78	**53**	62	56	105
9	25	42	95	**17**	99	26	40	20	106	69	**7**
8	**13**	94	14	**83**	115	8	87	30	57	28	5
7	**109**	4	6	104	**59**	70	**101**	33	63	**91**	110
6	**37**	32	**29**	**19**	52	**107**	81	38	54	118	111
5	**97**	51	58	114	98	21	**47**	112	**79**	**89**	92
4	**49**	50	**31**	3	93	**41**	10	**119**	44	66	64
3	**73**	65	88	117	90	27	68	55	**23**	74	34
2	85	**67**	9	46	80	100	86	39	**77**	35	102
1	**1**	45	116	2	**113**	18	**103**	82	16	75	**71**
0	∞	120	84	72	48	96	36	108	12	24	60
	0	1	2	3	4	5	6	7	8	9	10	v

Таблица поля из $p^2 = 169$ элементов (элементы таблицы — остатки mod 168).

$p = 13$

u													
12	**85**	45	161	165	**13**	76	58	**47**	158	122	**23**	166	64
11	15	**145**	**143**	88	91	52	**95**	**121**	111	96	6	162	156
10	141	10	132	**101**	**79**	114	49	54	**103**	**53**	120	46	69
9	**113**	51	75	**41**	**73**	26	18	104	21	92	150	86	**25**
8	**127**	32	39	40	100	87	164	**55**	106	**89**	35	**65**	118
7	**71**	152	108	33	62	**151**	**31**	50	9	144	44	**167**	147
6	**155**	63	**83**	128	60	93	134	**115**	**67**	146	117	24	68
5	**43**	34	**149**	119	**5**	22	**139**	80	3	16	124	123	116
4	**29**	**109**	2	66	8	105	20	102	110	**157**	**125**	159	135
3	57	153	130	36	**137**	**19**	138	133	30	**163**	**17**	48	94
2	99	72	78	90	12	27	**37**	**11**	136	7	4	**59**	**61**
1	**1**	148	82	**107**	38	74	**131**	142	160	**97**	81	77	129
0	∞	168	98	56	28	42	154	70	126	112	140	14	84
	0	1	2	3	4	5	6	7	8	9	10	11	12

v

Замечание. Хотя поле однозначно определяется числом своих элементов, его *таблица* не определяется однозначно этим числом, так как она зависит от того, какой именно элемент поля был выбран в качестве мультипликативной образующей A циклической группы ненулевых элементов поля. А именно, вместо примитивного элемента A можно было бы выбрать другой примитивный элемент, $\widetilde{A} = A^k$ (для примитивности этого элемента нужно только, чтобы число k было взаимно просто с числом $z - 1$ в случае поля из z элементов). Примитивные элементы образуют «группу Эйлера» Г. Влияние выбора элемента A на таблицу и на дальнейшие построения обсуждается ниже, в § 7: эти вопросы приводят к замечательным фактам проективной геометрии конечных множеств (§ 6 и § 7). Примитивные элементы в таблицах полужирные.

§ 3

ХАОТИЧНОСТЬ И СЛУЧАЙНОСТЬ ЧИСЕЛ ТАБЛИЦЫ ПОЛЯ ГАЛУА

При взгляде на приведённые выше таблицы полей Галуа возникает впечатление, что их заполнения числами от 1 до $z-1$ (где z — число элементов поля, т. е. p^2 в наших четырёх примерах) составляют своего рода *таблицы случайных чисел*: зная, где стоит в таблице число k, трудно найти место числа $k+1$.

При попытке точно сформулировать эти естественно-научное наблюдение хаотичности в виде математического утверждения возникают сотни гипотез. Вероятно, бóльшая часть из них станет со временем набором интересных доказанных теорем (хотя сегодня это достигнуто лишь в небольшом числе случаев).

Общая схема формулировки гипотез о «случайности» заполнения таблицы поля состоит в следующем. Настоящие случайные заполнения обладают родом свойств, доказываемых в теории вероятностей и в теории случайных процессов. Выберем для проверки «случайности» чисел таблицы одно из таких свойств и проверим, насколько точно оно выполняется для «псевдослучайных» чисел таблицы поля.

Гипотеза, к которой приводит выбранный признак случайности, состоит в том, что выбранный критерий по мере роста простого числа p начинает выполняться таблицей поля из $z=p^n$ элементов (например, при фиксированном значении n) все более точно, так что в пределе, при $p\to\infty$, он выполняется совсем точно.

Таким образом, для математической формулировки гипотезы нужно точно указать выбранный критерий. Поскольку признаков случайности очень много, получается много гипотез. Я обсужу сейчас только несколько простейших примеров (которые уже оказываются интересными и нетривиальными, несмотря на свою простоту и элементарность: проверить эти гипотезы эмпирически, при фиксированном p, может любой школьник, даже без помощи компьютера).

Начнём с примера: предположим, что вся таблица поля разбита на две непересекающиеся части, и посмотрим, сколько из чисел k, заполняющих таблицу, попадает в первую часть, G, а сколько во вторую.

Для случайного заполнения число N попаданий в область G среди m выбранных чисел пропорционально объёму (в двумерном случае площади) области G:

$$\frac{N}{m}\approx\frac{|G|}{z},$$

(где z — полное число клеток таблицы, то есть $z = p^2$ для поля из p^2 элементов).

Разумеется, при $m = z$ выписанной приближённое равенство выполнено в таблице поля точно, так как в каждую клеточку области G (составленной из клеточек таблицы) наблюдается ровно одно попадание.

Поэтому для формулировки гипотезы о равномерном распределении элементов $\{A^k\}$ в поле следует брать не всю эту геометрическую прогрессию, а только её часть. Выберем для этого число θ строго между 0 и 1 и рассмотрим начальную часть геометрической прогрессии $\{A^k\}$, в которой $m \approx \theta n$ членов ($1 \leqslant k \leqslant m$). Тогда получается следующая

Гипотеза о равнораспределённости геометрической прогрессии в поле Галуа из $z = p^n$ элементов:

$$\lim_{p \to \infty} \frac{N}{m} = \frac{|G|}{z}, \tag{1}$$

где N есть число попаданий m первых элементов A^k поля из z элементов в область G.

Показатель n я здесь фиксировал, хотя можно рассматривать и пределы при $z \to \infty$, не фиксируя n.

Пример. Для поля из $z = p^2 = 25$ элементов выберем в качестве области G первые два ($v = 0, 1$) столбца таблицы поля, так что $|G| = 10$.

Из геометрической прогрессии $\{A^k\}$ возьмём первую половину $1 \leqslant k \leqslant$ $\leqslant (12 = m)$.

Тогда (посчитанное по приведённой выше таблице поля) число попаданий есть $N = 5$. Степень нарушения допредельного критерия равнораспределённости для выбранного критерия (1) в этом случае оказывается такой:

$$\frac{N}{m} - \frac{|G|}{z} = \frac{5}{12} - \frac{10}{25} = \frac{1}{60}.$$

То есть, хотя простое число $p = 5$ и не велико, распределение уже довольно равномерно.

Доказательства предельного соотношения (1) в общем виде я не знаю, но ниже (в §§ 4 и 5) обсуждаю некоторые его варианты, которые удаётся доказать.

В качестве других критериев случайности, кроме критерия (1), можно предложить, например, следующие.

Пусть поле разбито на две непересекающиеся области,

$$F = G \cup H,$$

числа элементов которых равны, соответственно,

$$|F| = z, \quad |G| = rz, \quad |H| = sz \quad (\text{где } r + s = 1).$$

Для случайной последовательности выборов точек A_k поля F *частоты переходов* из G в G, из G в H, из H в G и из H в H при увеличении номера точки на 1 суть r^2, rs, sr, s^2.

Для геометрической прогрессии $\{A^k\}$ (которую в этом случае можно и не укорачивать: $1 \leqslant k < z$) естественно ожидать таких же частот четырёх событий переходов

$$(A^k \in G,\, A^{k+l} \in G), \quad (A^k \in G,\, A^{k+l} \in H) \quad \text{и т. д.}$$

Гипотеза о перемешивании геометрической прогрессии $\{A^k\}$ в поле из $z = p^n$ элементов.

Числа $N(G,G)$, $N(G,H)$, $N(H,G)$ и $N(H,H)$ значений k, для которых реализуются переходы $(A^k \in G,\, A^{k+l} \in G)$, $(A^k \in G,\, A^{k+l} \in H)$ и т. д., асимптотически пропорциональны частотам $(r^2,\, rs,\, sr,\, s^2)$ переходов в случайной последовательности,

$$\lim_{\substack{p\to\infty \\ l\to\infty}} \frac{N(G,G)}{z} = r^2, \quad \lim_{\substack{p\to\infty \\ l\to\infty}} \frac{N(G,H)}{z} = rs, \ldots$$

Ещё один критерий случайности доставляет *вариация*: *различие показателей k в соседних клетках таблицы*. Например, можно сосчитать сумму $\sum$ всех модулей разностей $|k-l|$ или же сумму расстояний $\rho(k,l)$ соседних чисел таблицы для её случайного заполнения числами k от 1 до z с одной стороны и для её заполнения, доставляемого таблицей поля Галуа из z элементов, с другой.

Асимптотическое отличие первой или второй (они различаются) величины $\sum$ для поля от её же математического ожидания при случайном заполнении предположительно убывает (в смысле относительной ошибки) с ростом простого числа p (или с ростом числа $z = p^n$ элементов поля). При этом соседство надо понимать в торической геометрии таблицы ($u = 4$ соседствует с $u = 0$ при $p = 5$).

Сходным образом, можно было бы оценить в качестве другого варианта вариации удалённость расположения в таблице соседних чисел k и $k+1$ циклической (замкнутой) или обычной последовательности, составляя сумму расстояний

$$\rho = \sum_k \rho(k, k+1).$$

При вычислении этих расстояний тоже естественно не забывать о торической геометрии заполняемой числами k таблицы $\mathbb{Z}_p^n$. Например, для $(p = 7,\, n = 1)$ расстояния для заполнения семи последовательных мест таблицы значениями $k = (1542376)$ доставляют сумму

$$\rho = 3+1+2+1+3+1+2 = 13, \text{ тогда как } \sum = 4+1+2+1+3+1+2,$$

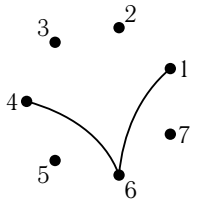


Рис. 3.1. Равные двойке расстояния между точками на конечном торе

так как $\rho(3,7)=3$ и $\rho(6,1)=2$ в торической геометрии. На этой циклической последовательности семи остатков от деления на 7 «вариация ρ» принимает значение 13.

Здесь снова гипотеза случайности таблицы поля состоит в близости (при больших p или z) вычисленных по таблице поля из p^n элементов значений суммы расстояний ρ (между местами показателей k и $k+1$ в таблице поля) к математическому ожиданию такой же суммы ρ для случайного заполнения таблицы (причём можно использовать и циклические последовательности длины m с m расстояниями-слагаемыми, и незамкнутые обычные, с их $m-1$ расстояниями между соседними членами).

В качестве других критериев случайности образованной элементами A^k системы точек таблицы можно рассмотреть такие характеристики набора первых m точек прогрессии, как минимальный радиус r шаров с центрами в этих точках, покрывающих вместе всю торическую таблицу, или максимальный радиус R шара, не содержащего ни одной точки рассматриваемой прогрессии (рис. 3.2). Наблюдаемые в таблице поля величины $r(m)$ и $R(m)$ интересно сравнить с такими же характеристиками m случайных точек: гипотеза хаотичности таблицы поля состоит в близости этих величин (вычисленных для поля и для случайных точек), например, при $m \approx \theta z$, где фиксировано $0<\theta<1$ и $z=p^n$ — число элементов поля, причём p (или z) стремится к бесконечности.

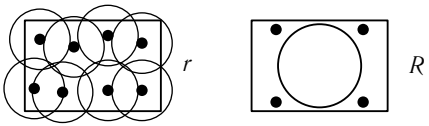


Рис. 3.2. Покрывающие и пустые шары набора точек

Ещё одной характеристикой случайности набора m точек таблицы является *радиус перколяции*, определяемый следующей конструкцией.

Окружим каждую точку набора шаром радиуса r. Если радиус достаточно мал, то по объединению этих шаров нельзя пересечь всю таблицу (от одного края до противоположного, так, чтобы на торе получился нестягиваемый путь), а если радиус достаточно велик, то такое «просачивание через шаровые дефекты» (называемое перколяцией) становится возможным (терминология заимствована из исследований течи в сосудах, вызванной дефектами материалов) (рис. 3.3).

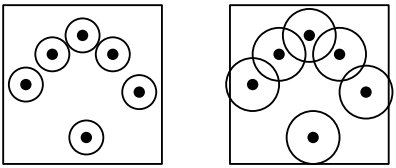


Рис. 3.3. Возникновение перколяции при увеличении радиуса дефектов

Критическое значение радиуса $r(m)$, при котором впервые происходит переход от ситуации непросачивания к просачиванию, называется *радиусом перколяции* (при столь больших дефектах в своём материале сосуд начинает течь).

Гипотеза перколяционной хаотичности распределения m точек прогрессии $\{A^k\}$ в таблице поля состоит в близости величины радиуса перколяции $r(m)$ для этой прогрессии к аналогичной величине для такого же числа m независимо случайно набросанных в таблицу точек (например, при $m \approx \theta z$, где $0 < \theta < 1$ фиксировано, в поле из большого числа $z = p^n$ элементов).

Здесь, как и раньше, подразумевается предельный переход при $p \to \infty$ (или при $z \to \infty$) к случаю поля из большого числа элементов.

Вместо шаров радиуса r в этой конструкции можно также рассматривать в роли «дефектов» наборы членов геометрической прогрессии с не слишком удалёнными друг от друга номерами, $\{A^k : |k - k_0| \leqslant \rho\}$ (и аналогичную величину для последовательности m случайно набросанных в таблицу точек, A_k): эти квазиперколяционные радиусы $\rho(m)$ *гипотеза квазиперколяционной стохастичности* таблицы поля тоже предполагает сближающимися для $m \approx \theta z$ первых точек таблицы поля из $z = p^n$ элементов (где $0 < \theta < 1$ фиксировано, а p или z стремится к бесконечности).

Разумеется, можно придумать много других признаков случайности таблицы, и каждый такой признак приводит к (интересной?) гипотезе эргодического характера, которую можно проверять экспериментально, и которую в случае её подтверждения эмпирическими данными можно и пытаться доказывать. Интересно, например, исследовать, насколько хаотически

расположены следи всех элементов поля его первообразные элементы, (т. е. насколько случайны полужирные k в таблице поля).

Вся возникающая теория является своеобразной теоретико-числовой конечной версией эргодической теории автоморфизмов тора, где хаотичности и перемешивание прогрессии $\{A^k\}$ изучается для сохраняющих объёмы линейных диффеоморфизмов A тора T^n. Разница состоит только в том, что континуальный тор T^n заменён в нашем случае состоящим из конечного числа z точек «тором» $\mathbb{Z}_p^n$, а предел при $k \to \infty$, определяющий временные средние в теории динамических систем, заменён в нашем случае предельным переходом при стремлении к бесконечности числа $m \approx \theta z$ рассматриваемых точек орбиты динамической системы (при стремлении к бесконечности простого числа p или числа $z = p^n$ точек конечного тора). Перколяционная хаотичность не рассмотрена, кажется, и в теории автоморфизмов непрерывного тора.

§ 4
РАВНОМЕРНОЕ РАСПРЕДЕЛЕНИЕ ГЕОМЕТРИЧЕСКОЙ ПРОГРЕССИИ ВДОЛЬ КОНЕЧНОГО ОДНОМЕРНОГО ТОРА

Существует два основных способа ставить задачу: *французский способ* состоит в том, чтобы сформулировать вопрос *наиболее общим образом*, т. е. так, чтобы его *нельзя было бы далее обобщить* без потери смысла, в то время как *русский способ* состоит в том, чтобы сформулировать его в *том простейшем случае*, *который нельзя далее упростить*, не лишая вопрос его основного содержания[1]. Гипотезы о псевдослучайности таблиц конечных полей я попытался сформулировать в § 3 выше на французский лад.

Рассмотрим теперь русский вариант первой из этих гипотез — гипотезы о равномерном распределении геометрической прогрессии в поле Галуа из p^n элементов. С этой целью ограничимся простейшим полем, $\mathbb{Z}_p$ (составленным из остатков от деления на простое число p), состоящим из всего p элементов, т. е. рассмотрим случай $n=1$ общей теории § 3.

Чтобы упростить формулы, будем считать простое число p нечётным, а в качестве области G возьмём первую половину ненулевых элементов поля, $\{c: 1 \leqslant c \leqslant (p-1)/2\}$, $|G| = (p-1)/2$.

В качестве отрезка геометрической прогрессии остатков от деления на p мы рассмотрим её первые $m = (p-3)/2$ членов,

$$\{A^k: 1 \leqslant k \leqslant m\}.$$

Такой выбор «половины» прогрессии ($\theta \approx 1/2$) объясняется тем, что по малой теореме Ферма $A^{p-1} = 1$, поэтому $A^k = -1$ при $k = (p-1)/2$, так что этот член прогрессии не случаен, а случайности можно ожидать при меньших k, т. е. для $k \leqslant m$.

Вычисляя эти отрезки прогрессий остатков от деления на p для $p = 5, 7, 11$ и 13, мы должны прежде всего указать для каждого p первообразные элементы A (для каждого из которых наименьший период T прогрессии остатков равен именно числу $p-1$, а не меньшему числу-делителю). Вот эти прогрессии и периоды T для $p=5$:

A	прогрессия $\{A^k\}$	T	N	$\sum$
1	1, 1, 1, 1	1		
2	2, 4, 3, 1	4	1	$2+1+2+1=6$
3	3, 4, 2, 1	4	0	$1+2+1+2=6$
4	4, 1, 4, 1	2		

[1] Чебышёв много общался с французами, особенно с Лиувиллем, но никогда не говорил с ними о математике, чтобы не повредить оригинальности русского подхода к делу.

Первообразными (*примитивными*) являются здесь элементы $A=2$ и $A=3$, они выделены полужирным шрифтом.

В графе N указано число попаданий отрезка из первых $m=(p-3)/2$ членов прогрессии в область G (число меньших или равных $(p-1)/2$ среди первых m остатков). При $p=5$ мы получаем $m=1$, $(p-1)/2=2$, поэтому $N(A=2)=1$, $N(A=3)=0$.

В графе $\sum$ указана сумма расстояний между последовательными элементами прогрессии в $\mathbb{Z}_5$ (считая эту последовательность циклической, т. е. включая в сумму и расстояние от её последнего члена до первого).

В этом случае критерий равномерной распределённости среди ненулевых остатков от деления на p даёт погрешности (разности наблюдённого и пространственного средних)

$$A=2: \quad \frac{N}{m}-\frac{|G|}{z-1}=\frac{1}{1}-\frac{2}{4}=\frac{1}{2},$$
$$A=3: \quad \frac{N}{m}-\frac{|G|}{z-1}=\frac{0}{1}-\frac{2}{4}=-\frac{1}{2}.$$

Как видно, критерий равномерного распределения приближённо выполнен с погрешностью, равной $1/2$ по модулю в обоих случаях. При этом в среднем (по выбору примитивного элемента A) критерий выполнен даже точно:

$$\frac{\overline{N}}{m}=\frac{|G|}{z-1},$$

где $\overline{N}=(\sum N(A))/(\text{число примитивных элементов } A)=(1+0)/2$.

Аналогичные вычисления для $p=7$ дают следующую таблицу ответов.

$$p=7:\ m=2,\ |G|=3,\ z=7.$$

A	прогрессия $\{A^k\}$	T	N	$\sum$
1	$1,1,\ldots$	1		
2	$2,4,1,\ldots$	3		
3	$3,2,6,4,5,1,\ldots$	6	2	$1+3+2+1+3+2=12$
4	$4,2,1,\ldots$	3		
5	$5,4,6,2,3,1,\ldots$	6	0	$1+2+3+1+2+3=12$
6	$6,1,\ldots$	2		

(расстояние от 1 до 5 в $\mathbb{Z}_7$ равно 3).

Следовательно, среднее число попаданий равно

$$\overline{N}=\frac{2+0}{2}=1, \quad \frac{\overline{N}}{m}=\frac{1}{2},$$

в то время как пространственное среднее есть

$$\frac{|G|}{z-1} = \frac{3}{6} = \frac{1}{2}.$$

Итак, критерий равномерного распределения в среднем по выбору A опять выполнен точно.

В случае $p = z = 11$ ответы таковы:

$$m = 4,\ |G| = 5,\ z - 1 = 10,$$

A	прогрессия $\{A^k\}$	T	N	$\sum$
1	$1, 1, \ldots$	1		
2	$2, 4, 8, 5, 10, 9, 7, 3, 6, 1$	10	3	30
3	$3, 9, 5, 4, 1, \ldots$	5		
4	$4, 5, 9, 3, 1, \ldots$	5		
5	$5, 3, 4, 9, 1, \ldots$	5		
6	$6, 3, 7, 9, 10, 5, 8, 4, 2, 1$	10	1	30
7	$7, 5, 2, 3, 10, 4, 6, 9, 8, 1$	10	3	30
8	$8, 9, 6, 4, 10, 3, 2, 5, 7, 1$	10	1	30
9	$9, 4, 3, 5, 1, \ldots$	5		
10	$10, 1, \ldots$	2		

Из этой таблицы следует, что среднее число попаданий доставляет статистику

$$\overline{N} = \frac{3+1+3+1}{4} = 2, \quad \frac{\overline{N}}{m} = \frac{1}{2},$$

в то время как пространственное среднее имеет значение

$$\frac{|G|}{z-1} = \frac{5}{10} = \frac{1}{2},$$

так что критерий равномерной распределённости при $p = 11$ выполнен точно в среднем по A (погрешность же для индивидуальных значений A равна $1/4$ по модулю).

В случае $p = z = 13$ аналогичные вычисления дают числа

$$m = 5, \quad |G| = 6, \quad z - 1 = 12.$$

Таблица прогрессий имеет в этом случае вид

A	прогрессия $\{A^k\}$	T	N	$\sum$
1	$1, 1, \ldots$	1		
2	$2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1$	12	4	42
3	$3, 9, 1, \ldots$	5		
4	$4, 3, 12, 9, 3, 1, \ldots$	5		
5	$5, 12, 8, 1, \ldots$	5		
6	$6, 10, 8, 9, 2, 12, 7, 3, 5, 4, 11, 1$	12	2	42
7	$7, 10, 5, 9, 11, 12, 6, 3, 8, 4, 2, 1$	12	1	42
8	$8, 12, 5, 1, \ldots$	4		
9	$9, 3, 1, \ldots$	3		
10	$10, 9, 12, 3, 4, 1, \ldots$	2		
11	$11, 4, 5, 3, 7, 12, 2, 9, 8, 10, 6, 1$	12	3	42
12	$12, 1, \ldots$	2		

В этом случае наблюдённое (среднее по четырём первообразным остаткам A) число попаданий есть

$$\overline{N} = \frac{4+2+1+3}{4} = 2\frac{1}{2}, \quad \text{так что} \quad \frac{\overline{N}}{m} = \frac{1}{2},$$

при пространственном среднем

$$\frac{|G|}{z-1} = \frac{6}{12} = \frac{1}{2}.$$

Итак, при $p = 13$ критерий равномерного распределения тоже точно выполнен (в среднем по A).

Погрешности же для индивидуальных значений ($A = 2, 6, 7, 11$) равны, соответственно, (3/10, $-1/10$, $-3/10$ и $1/10$).

Теорема. *Критерий равномерного распределения первых* $m = \frac{p-3}{2}$ *членов прогрессии* $\{A^k\}$ *среди ненулевых остатков от деления на* p *всегда точно выполнен* (*в среднем по* A) *для области* $G = \{1 \leqslant c \leqslant |G| = \frac{p-1}{2}\}$ *в* $\mathbb{Z}_p$ (*где* p *— любое нечётное простое число*).

Иными словами, если

$$\overline{N} = \left(\frac{\sum N(A)}{\text{число первообразных элементов } A} \right), \quad \text{то} \quad \frac{\overline{N}}{m} = \frac{|G|}{z-1} = \frac{6}{12} = \frac{1}{2}.$$

Доказательство. Вместе с первообразным остатком A от деления на p первообразным является и обратный остаток $B = A^{-1}$.

Лемма. *Имеет место тождество*

$$N(A)+N(B)=m.$$

Доказательство леммы. Поскольку $A^{p-1}=A^{2m+2}=1$, то отрезки $\{1\leqslant k\leqslant m\}$ и $\{1\leqslant l\leqslant m\}$ прогрессий A^k и $B^l=A^{p-1-l}$ заполняют по разу почти всю прогрессию A^i, $1\leqslant i\leqslant p-1$: исключены только два её «тривиальных» (не «случайных») члена, $A^{p-1}=1$ и $A^{m+1}=-1$.

В том числе они содержат по разу все элементы c области G, $\{2,3,\ldots,m+1\}$, кроме $c=1$. Следовательно, сумма чисел $N(A)$ и $N(B)$ попаданий обоих отрезков в область G составляет m, что и доказывает лемму.

Из леммы следует равенство числу $m=(p-3)/2$ среднего по A числа попаданий, $\overline{N}$. Действительно, весь набор первообразных остатков A состоит из α (непересекающихся) пар $\{A,B\}$, где $AB=1$. Каждая такая пара даёт в сумму чисел попаданий $\sum N(A)$ вклад m по лемме. Поэтому вся эта сумма равна αm, откуда находим среднее по A число попаданий $\overline{N}=(\sum N(A))/(2\alpha)=(m\alpha)/(2\alpha)=m/2$. Стало быть, $N/m=1/2$, что и доказывает теорему.

Из приведённых выше таблиц видно, что во всех рассмотренных примерах вариация $\sum=\sum\rho(A^k,A^{k+1})$ всей периодической прогрессии из $p-1$ точки на целочисленной окружности $\mathbb{Z}_p$ составляет величину

$$\sum=\frac{p^2-1}{4},$$

независимо от выбора первообразного остатка A.

Это тождество верно и для любого p. Будем обозначать (для $x\in\in\mathbb{Z}_p$) $\rho(x,0)=|x|$, (так что при $p=5$ $|1|=|4|=1$, $|2|=|3|=2$). Тогда $\rho(A^k,A^{k+1})=|A^k(A-1)|$. Но $\{A^k(A-1)\}=\{A^k,1\leqslant k<p\}$ как подмножество в $\mathbb{Z}_p$, поэтому $\sum=2\sum\limits_{r=1}^{c}r=2c(c+1)/2$, где $c=\dfrac{p-1}{2}$, откуда $\sum=c(c+1)=(p^2-1)/4$.

Средняя вариация $\overline{\sum}$ случайно выбранной на конечной окружности $\mathbb{Z}_5$ циклической последовательности из $p-1=4$ точек легко вычисляется. В качестве последовательностей достаточно взять те 6, которые начинаются с 1:

$$(1,2,3,4),\ (1,2,4,3),\ (1,3,2,4),\ (1,3,4,2),\ (1,4,2,3),\ (1,4,3,2).$$

Их вариации $\sum$ (учитывая, что в $\mathbb{Z}_5$ имеем $\rho(4,1)=2$) составляют, соответственно, (5, 6, 7, 6, 7, 5). Поэтому среднее значение вариации случайной

циклической последовательности из 4 точек конечной окружности $\mathbb{Z}_5$ есть $\overline{\sum} = 6$.

Итак, вычисленные выше вариации циклических геометрических прогрессий степеней первообразных остатков A (от деления на $p = 5$), $\sum(A) = 6$, совпадают со средней вариацией $\overline{\sum}$ случайной циклической последовательности (такой же длины, $p - 1 = 4$). Это ещё раз подтверждает квазислучайность таблицы поля из $p = 5$ элементов.

С ростом простого числа p средняя вариация $\overline{\sum}$ случайной последовательности из $p - 1$ точки конечной окружности $\mathbb{Z}_p$ растёт как $p^2/4$. В этом убеждают следующие соображения.

Расстояние между двумя случайно выбранными точками этой окружности принимает значения от 1 до $(p - 1)/2$. Его среднее значение имеет, как легко сосчитать, величину, близкую к $p/4$. Поэтому сумма всех таких расстояний между последовательными точками нашей последовательности (их $p - 1$) составляет примерно $p^2/4$ (с малой относительной ошибкой).

Итак, приведённые выше вычисления вариаций $\sum$ циклических геометрических прогрессий длины $p - 1$ в полях $\mathbb{Z}_p$ при $p \leqslant 13$ подтверждают гипотезу о квазислучайности таблицы конечного поля с p элементами.

Замечание (о сложности логарифмической функции). Хаотичность распределения геометрической прогрессии вычетов приводит к интересным фактам и гипотезам теории алгоритмической сложности. Если a — примитивный вычет по модулю p, то каждый вычет x по модулю p имеет форму a^k. Гипотеза о сложности состоит в том, что *вычисление «логарифма» $k(x)$ вычета x является сложной вычислительной задачей.*

Чтобы определить *величину сложности*, нужно расклассифицировать функции (определенные на конечном множестве и имеющие конечное число значений) в соответствии со «степенью сложности» определяющей функцию формулы. Чтобы точно определить число, измеряющее сложность, рассмотрим простейший случай бинарных функций

$$f\colon (\mathbb{Z}/n\mathbb{Z}) \to (\mathbb{Z}/2\mathbb{Z}).$$

Такую функцию можно рассматривать как последовательность $(x_1, \ldots, x_n)$ из n элементов, каждый из которых равен либо 0, либо 1.

Число таких последовательностей равно 2^n. Они образуют векторное пространство $(\mathbb{Z}_2)^n$ над $\mathbb{Z}_2 = \mathbb{Z}/2\mathbb{Z}$. Мы можем считать эти функции вершинами куба размерности n.

Для измерения сложности функции x рассмотрим, вслед за Ньютоном, функцию «первой разности» y, определенную как последовательность n вычетов по модулю 2

$$y(k) = x(k + 1) - x(k) \pmod 2.$$

Поскольку аргумент k является остатком от деления на n, мы получаем именно n разностей n чисел, считая, что за последним членом последовательности x идет первый, так что $x(n+1)=x(1)$. Этот переход к циклическим последовательностям позволяет избавиться от краевых эффектов и делает дальнейшие формулировки более простыми.

Пример. Из последовательности $x=(1,0,0,1,1)$ получается последовательность разностей $y=(1,0,1,0,0)$ (так как $y_5=x_1-x_5=0$).

Оператор взятия первых разностей является линейным (гомоморфизмом абелевой группы в себя),

$$A\colon \mathbb{Z}_2^n \to \mathbb{Z}_2^n.$$

Сложность точки $x\in\mathbb{Z}_2^n$ будет вычисляться в терминах последовательности высших разностей

$$A^t(x)\in\mathbb{Z}_2^n \quad (t=1,2,\ldots).$$

Пример. Для постоянной функции x мы находим $A(x)=A^t(x)=0$.

Для многочлена x степени d, $x(k)=a_0k^d+\ldots+a_d$, мы получаем $A^t(x)=0$ для любого $t>d$.

Ниже мы будем исследовать спектральные свойства оператора A.

Естественно считать постоянные простейшими функциями, многочлены меньшей степени считать менее сложными, чем многочлены более высокой степени, а неполиномиальные функции считать более сложными объектами, чем все многочлены. (Я не буду формулировать следующие очевидные шаги классификации, привлекающие экспоненты и решения дифференциальных уравнений — читатель может по-разному построить свою иерархию сложности функций от x в зависимости от своих потребностей.)

Гипотеза состоит в том, что *определенные выше логарифмические функции сложны*. Я не буду доказывать эту гипотезу, но приведу много подтверждающих её примеров.

Другая гипотеза утверждает, что *большинство из 2^n функций, составляющих куб $\mathbb{Z}_2^n$, ведут себя подобно случайным последовательностям* (по меньшей мере асимптотически при $n\to\infty$).

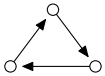
Я не буду доказывать эту гипотезу, но обсуждаемые ниже примеры доставляют сложные функции, ведущие себя в численных экспериментах совершенно так же, как и случайные последовательности. Я надеюсь, что это свойственно сложным функциям вообще, а не только тем специальным случаям, которые мы рассмотрим ниже.

Чтобы понять, в каких пределах может меняться сложность, начнем с общего исследования оператора взятия разностей $A\colon \mathbb{Z}_2^n\to\mathbb{Z}_2^n$.

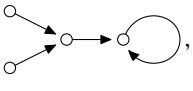
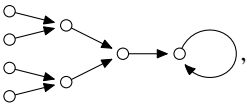
Как и всякое отображение конечного множества в себя, оператор A разбивает множество $\mathbb{Z}_2^n$ на инвариантные «компоненты связности».

Мы будем рассматривать эти компоненты как графы с направленными ребрами (покидающее точку x ребро ведет в точку Ax).

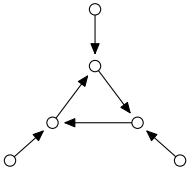
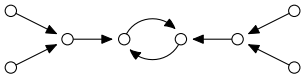
Каждая связная компонента графа отображения содержит ровно один притягивающий цикл O_m (длина цикла, $m \geqslant 1$ — целое число):

$O_1 =$  , $O_2 =$  , $O_3 =$  , $\ldots$

Кроме цикла компонента содержит еще деревья, притягиваемые вершинами цикла. Нам потребуются бинарные деревья T_{2^n} с 2^n вершинами:

$T_2 =$  , $T_4 =$  , $T_8 =$  , $\ldots$

Мы будем обозначать через $O_m * T_{2^m}$ компоненту, в которой цикл O_m притягивает дерево T_{2^m} к каждой своей вершине: $O_1 * T_{2^m} = T_{2^m}$, а дальнейшие «произведения» имеют вид

$O_3 * T_2 =$  , $O_2 * T_4 =$  , $\ldots$

Теорема 1. *Граф разностного опреатора* $A\colon \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ *при* $n \leqslant 12$ *имеет вид, описанный в следующей таблице*:

n	число компонент	циклы и деревья	$A^u = A^v$
2	1	$(O_1 * T_4)$	$A^2 = 0$
3	2	$(O_3 * T_2) + (O_1 * T_2)$	$A^4 = A$
4	1	$(O_1 * T_{16})$	$A^4 = 0$
5	2	$(O_{15} * T_2) + (O_1 * T_2)$	$A^{16} = A$
6	4	$2(O_6 * T_4) + (O_3 * T_4) + (O_1 * T_4)$	$A^8 = A^2$
7	10	$9(O_7 * T_2) + (O_1 * T_2)$	$A^8 = A$
8	1	$(O_1 * T_{256})$	$A^8 = 0$
9	6	$4(O_{63} * T_2) + (O_3 * T_2) + (O_1 * T_2)$	$A^{64} = A$
10	10	$8(O_{30} * T_4) + (O_{15} * T_4) + (O_1 * T_4)$	$A^{32} = A^3$
17	4	$3(O_{341} * T_2) + (O_1 * T_2)$	$A^{342} = A$
12	24	$20(O_{12} * T_{16}) + 2(O_6 * T_{16}) + (O_3 * T_{16}) + (O_1 * T_{16})$	$A^{76} = A^4$

Доказывается эта теорема прямыми вычислениями. Например, при $n = 2$ число вершин равно $2^2 = 4$, и разностный оператор, по определению, действует так:

$$A(0,0) = (0,0), \quad A(0,1) = (1,1), \quad A(1,0) = (1,1), \quad A(1,1) = (0,0).$$

Поэтому граф состоит всего из одной компоненты,

$$T_4 = \begin{matrix} (0,1) \searrow \\ \\ (1,0) \nearrow \end{matrix} (1,1) \longrightarrow (0,0) \circlearrowright \tag{4.1}$$

Обозначим через δ линейный оператор сдвига последовательности, определенный формулой $(\delta x)_k = x_{k+1}$. Тогда мы находим $A = 1 + \delta$, $\delta^n = 1$. Поэтому при $n = 3$ мы получаем, последовательно,

$$A = 1 + \delta, \quad A^2 = 1 + 2\delta + \delta^2 = 1 + \delta^2,$$
$$A^3 = 1 + \delta + \delta^2 + \delta^3 = \delta + \delta^2, \quad A^4 = \delta + \delta^2 + \delta^2 + \delta^3 = 1 + \delta = A.$$

Граф для A сразу получается из этих тождеств, даже без перебора всех 8 значений x, так как при $A^4 = A$ циклы имеют периоды 1 или 3.

Многие очевидные свойства графов таблицы легко доказываются и в более общей ситуации. Например, при всяком $n = 2^m$ мы находим $A^n = 0$, поскольку все биномиальные коэффициенты C_n^i четны при $i \neq 0, n$:

$$A^n = 1 + \delta^n = 1 + 1 = 0 \pmod 2.$$

Теперь мы определим место логарифмических функций в этой таблице. Явные вычисления показывают, что их сложности близки к максимально возможной сложности бинарной функции (при фиксированном значении n).

Для примитивного вычета a по модулю p мы определим «логарифм вычета k» формулой теоремы Ферма,

$$a^{\log_a k} = k \pmod p.$$

Приводя этот целочисленный логарифм по модулю два, мы получаем бинарную функцию со значениями

$$x(k) = \log_a k \pmod 2 \in \mathbb{Z}/2\mathbb{Z}$$

для значений $1, 2, \ldots, p - 1 = n$ аргумента k.

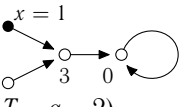
Пример. При $p = 7$, $a = 3$, мы получаем последовательность

$$\log_3 k = (0, 2, 1, 4, 5, 3), \quad x(k) = (0, 0, 1, 0, 1, 1).$$

Таким образом мы находим для первообразного корня a последовательность из $n = p - 1$ приведенных по модулю 2 логарифмов, $x \in \mathbb{Z}_2^n$. Ниже мы вычислим сложность, определенную графами теоремы 1, для этих бинарных последовательностей.

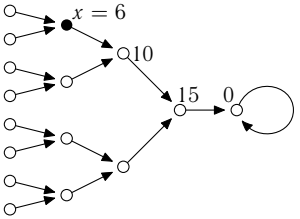
Теорема 2. *Приведенные по модулю 2 логарифмы x последовательных вычетов по модулю p имеют (при $p \leqslant 13$) следующие значения (в обозначениях графов операций взятия разности предыдущей теоремы со значением $n = p - 1$):*

$p = 3$
$n = 2$



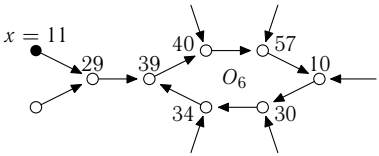
$(x \in T_4,\ a = 2)$,

$p = 5$
$n = 4$



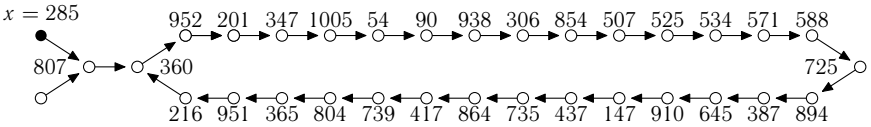
$(x \in T_{16},\ a = 2$ или $3)$,

$p = 7$
$n = 6$



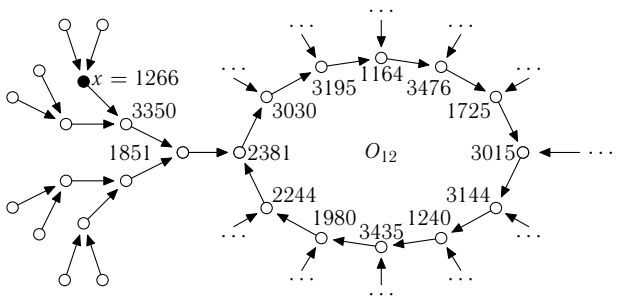
$(x \in (O_6 * T_4),\ a = 3$ или $5)$,

$p = 11$
$n = 10$



$(x \in (O_{30} * T_4),\ a = 2,6,7$ или $8)$,

$p = 13$
$n = 12$



$(x = 1266 \in (O_{12} * T_{16}),\ a = 2, 6, 7$ или $11)$.

В этом описании мы для краткости обозначаем бинарную последовательность $x = (x_1, \ldots, x_n) \in \mathbb{Z}_2^n$ её «бинарно-десятичным» числом

$$2^{n-1}x_1 + 2^{n-2}x_2 + \ldots + x_n.$$

Например, число $x = 285$ (при $p = 11$, $n = 10$) обозначает последовательность

$$(0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$$

из десяти бинарных цифр числа $285 = 256 + 16 + 8 + 4 + 1$.

Доказательства утверждений теоремы 2 представляют собой конечные, но длинные вычисления. В простейшем случае $p = 3$, $a = 2$, геометрическая прогрессия $(2^k) = (1, 2) \pmod 3$, где $k = 1, 2$, доставляет логарифмы

$$\log_2 1 = 0, \quad \log_2 2 = 1.$$

Последовательность x (приведенных по модулю два логарифмов) имеет вид $(x_1 = 0, x_2 = 1)$. Согласно формуле (4.1), положение точки x в графе такое, как указано в теореме 2.

Для бóльших значений p (особенно для $p = 11$ и 13) вычисления длиннее. Чтобы их ускорить, удобно профакторизовать множество циклических последовательностей x по модулю группы вращений $\mathbb{Z}/n\mathbb{Z}$ конечной окружности, на которой определена функция x. Например, в случае $n = 4$ мы отождествляем последовательности $(0, 1, 0, 0)$ и $(0, 0, 0, 1)$. Послкольку операторы δ и A коммутируют с этими вращениями, их можно применять и к профакторизованным последовательностям x (неизвестно где начинающимся). При этом число x для факторизации удобно считать вычетом по модулю $2^n - 1$ (чтобы операция δ свелась к умножению на 2, несмотря на перенос последней единицы на первое место).

Тем самым вычисления сокращаются примерно в n раз (для n повернутых копий последовательности x можно ничего нового не вычислять).

Полезно также вычислить ядро оператора A^t (скажем, при большом t). Это ядро представляет те вершины графа, которые лежат на бинарном дереве с корнем в нуле (составляющей всегда одну из компонент графа и доставляющей также деревья, притягивающиеся к вершинам циклов путем сложения с ядром в векторном пространстве $\mathbb{Z}_2^n$). Это соображение объясняет однородность графов теоремы 1: все притягивающиеся к вершинам циклов деревья изоморфны друг другу.

Объединение самих циклов представляет образ линейного оператора A^t при больших t. Циклы периода T можно найти, решая относительно $y = A^t x$ уравнение $A^T y = y$ (где t соответствует бинарному дереву из 2^t вершин).

Описанные длинные вычисления приводят ко всем таблицам теоремы 2, и её сравнение с теоремой 1 показывает, что сложность логарифмической функции почти максимальна (при каждом данном n) по сравнению с другими бинарными функциями на n-точечном множестве.

Наши вычисления доказывают это только при $n \leqslant 12$, но гипотеза, что такая сложность логарифмов сохранится и при больших значениях n, кажется вполне правдоподобной.

Аналогичные теоремы (и гипотезы) естественно рассмотреть и для функций с недвоичными значениями, например, для функций, значения которых являются остатками от деления на некоторое число q:

$$x \in (\mathbb{Z}/(q\mathbb{Z}))^n, \quad x_k \in \mathbb{Z}_q.$$

К сожалению, я не могу угадать ответов для таких обобщений теоремы 1 (даже для рассмотренного выше случая $q = 2$ при больших значениях n).

Таблицы теоремы 1 показывают довольно хаотическую зависимость графов от числа n, но даже усредненные асимптотики таких их параметров, как число циклов, длины циклов и размеры деревьев при стремлении n к бесконечности не только не доказаны, но и не найдены эмпирически. Было бы естественно попытаться угадать эти усредненные асимптотики, проводя при больших значениях n компьютерные эксперименты (хотя бы до $n = 100$ или до $n = 1000$).

Все эти теоремы и гипотезы переносятся со случая полей $\mathbb{Z}_p$ на общие поля Галуа почти буквально, но я ограничился простейшим случаем поля из p элементов (а иногда даже бинарным случаем $p = 2$), предполагая, что недостающая здесь теория сложности конечных объектов должна быть разработана сперва в простейшем случае.

Автор благодарен И. Шпарлинскому (из вычислительного отдела университета Макари в Сиднее), который, прочитав предварительную рукопись настоящей книги, доказал некоторые из обсуждавшихся выше гипотез и исправил опечатки в формулировках некоторых из них.

§ 5
АДИАБАТИЧЕСКИЙ АНАЛИЗ РАСПРЕДЕЛЕНИЯ ГЕОМЕТРИЧЕСКОЙ ПРОГРЕССИИ ОСТАТКОВ

Не проводя строгого доказательства, я намечу здесь соображения, объясняющие асимптотическую равномерность распределения последовательности остатков от деления на p членов геометрической прогрессии $\{A^k,\ 1 \leqslant k \leqslant \theta p\}$ среди всех ненулевых остатков от деления на p (где A — первообразный остаток, $0 < \theta < 1$ фиксировано, а простое число p велико).

Попытаемся определить число N остатков членов прогрессии от деления на p, попадающих в интервал $(G:\ 1 \leqslant c \leqslant \mu p)$ значений c. С этой целью перейдём к логарифмам, чтобы сделать геометрическую прогрессию арифметической: $\ln A^k = l_k = ka$, где $a = \ln A$.

Условие $A^k \pmod p \in G$ записывается в терминах логарифмов в виде включения числа l_k в один из интервалов следующей системы (рис. 5.1)

$$l_k \in \bigcup \Delta_j,$$

где Δ_j — интервал между логарифмами членов двух арифметических прогрессий,

$$\Delta_j = \{l:\ \ln(jp) < l \leqslant \ln(jp + \mu p)\}.$$

Длина интервала Δ_j есть

$$|\Delta_j| = \ln \frac{jp + \mu p}{jp} = \ln\left(\frac{j+\mu}{j}\right) = \ln\left(1 + \frac{\mu}{j}\right) \approx \frac{\mu}{j} \quad \text{(при больших } j\text{)}.$$

Суммарная длина $D(\mu)$ всех этих интервалов составляет величину порядка $\mu \sum \frac{1}{j}$, причём номера j нужных в этой конечной сумме интервалов

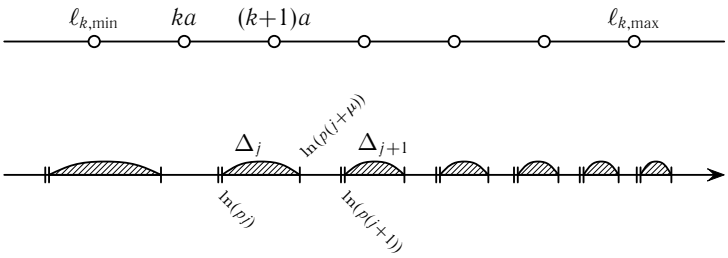


Рис. 5.1. Адиабатическое приближение неравномерной последовательности логарифмов арифметической прогрессией

определяются наибольшим и наименьшим значениями логарифмов l_k членов изучаемой прогрессии.

Это приводит к приближённой формуле $D(\mu) \sim \mu \ln(j_{\max})$, где $j_{\max} \to \infty$ при $p \to \infty$, с малой относительной погрешностью.

В то же время суммарная длина всего интервала оси l, в котором лежат наши логарифмы, l_k, составляет $D(\mu = 1) \sim \mu \ln(j_{\max})$ (также с малой относительной погрешностью).

Арифметическая прогрессия $\{l_k\}$ распределяется на оси l равномерно (по теореме Вейля о равнораспределённости дробных долей членов арифметической прогрессии).

Это соображение подсказывает, что число N попаданий точек l_k в объединение интервалов Δ_j должно быть асимптотически пропорционально той доле, которую сумма длин этих интервалов составляет от всего рассматриваемого отрезка оси l, т. е. должно быть асимптотически пропорционально отношению $D(\mu)$ к $D(1)$.

Мы приходим, таким образом, к заключению, что при $p \to \infty$ следует ожидать асимптотического поведения

$$\frac{N}{\theta p} \to \left(\frac{D(\mu)}{D(1)} \sim \mu \right)$$

числа попаданий, которое и означает равнораспределённость остатков от деления на p членов геометрической прогрессии $\{A^k,\ 1 \leqslant k \leqslant \theta p\}$ (поскольку G составляет μ-ю часть от $\mathbb{Z}_p$).

Замечание 1. Учёт следующих членов разложения $\ln(1+x) \approx x - \frac{x^2}{2} + \ldots$ при малых x приводит к выводу об отклонении числа попаданий вверх: $N > \theta\mu(p-1)$.

Замечание 2. Наши (впрочем, не вполне строгие) рассуждения можно рассматривать как адиабатическую замену логарифмической последовательности (чисел $\ln(jp) = \ln p + \ln j$ и интервалов Δ_j, начинающихся в этих точках) арифметической прогрессией (чисел или интервалов, соответственно); см. рис. 5.1 на стр. 36.

В действительности «шаг» $\ln(j+1) - \ln j = \ln \frac{j+1}{j} \sim \frac{1}{j}$ логарифмической последовательности медленно убывает с ростом j, так что эта последовательность не точно совпадает с арифметической прогрессией (а лишь близка к ней на довольно больших интервалах изменения j, если дать разности адиабатически приближающей $\ln j$ арифметической прогрессии соответствующее интервалу изменения целого числа j значение).

Если бы логарифмическая последовательность точно была арифметической прогрессией, наш вывод был бы строго обоснован теоремой Вейля о равномерном распределении дробных долей элементов арифме-

тической прогрессии. Таким образом, для обоснования нашего вывода остаётся лишь оценить погрешность адиабатического приближения (или же модифицировать доказательства теоремы Вейля, для чего нужно было бы исследовать поведение коэффициентов Фурье характеристической функции объединения интервалов Δ_j).

При $p=997$, $\theta=1/2$, $\mu=1/2$, $A=7$ я вычислил число попаданий $N=279>\theta\mu(p-1)=249$ и следовало бы проверить экспериментально, будет ли N приближаться к $\theta\mu(p-1)$ при росте p без усреднения по A. Интересно было бы даже исследовать дисперсию отклонения числа попаданий $N(A)$ от его среднего значения $\theta\mu(p-1)$, вычисленного в § 4: из оценок дисперсии уже могла бы вытекать сходимость к 1 отношения $N(A)/\theta\mu(p-1)$ для большинства первообразных остатков A даже в том случае, если бы этой сходимости n не было для некоторых редких значений A.

Отличие величины $D(\mu)/D(1)$ от $1/2$ при $\mu=1/2$ составляет в приведённом примере (где $p=997$, $A=7$, $\theta=1/2$) величину

$$\frac{\sum\ln(1+1/2k)}{\sum\ln(1+1/k)}-\frac{1}{2}=\frac{\ln(2k+1)!!-\ln(2k!!)}{\ln(k+1)}-\frac{1}{2},$$

где $k\approx 7^{498}$.

Добавление. Другой способ установить асимптотически равномерное распределение последовательности остатков от деления на p членов геометрической прогрессии $\{A^k,\ 1\leqslant k\leqslant\theta p\}$ среди всех остатков от деления на p (где A первообразный остаток, число θ, $0<\theta<1$, фиксировано, а простое число p стремится к бесконечности) состоит в следующем.

Рассмотрим мультипликативную группу

$$\mathbb{Z}_p=\{z\in\mathbb{C}\colon z^p=1\}.$$

Функции на этой группе будем разлагать в ряд Фурье по характерам,

$$e_0\equiv 1,\ e_1=z,\ \ldots,\ e_{p-1}=z^{p-1}.$$

Умножение остатков от деления на p на A записывается в этих обозначениях как отображение $f\colon\mathbb{Z}_p\to\mathbb{Z}_p$, где $f(x)=x^A$. На функциях это отображение действует по формуле

$$f^*e_k=e_{A^k}.$$

Функция e_0 инвариантна, а остальные $p-1$ гармоника e_k переставляются циклически преобразованием f^*, поскольку остаток A первообразен.

Для установления равномерного распределения докажем стремление к нулю временных средних от непостоянных гармоник Фурье, т. е. стремление к нулю функций

$$\widehat{e}_k = \sum_{t=0}^{T-1} \frac{(f^*)^t e_k}{T}.$$

Поскольку остаток A первообразный, перестановка f^* гармоник e_k, $k \neq 0$, циклическая (порядка $p-1$).

Чтобы изучить функции $\widehat{e}_k$, сделаем преобразование Фурье ещё раз, перенумеровав эти гармоники в порядке следования их номеров k в числе остатков цикла $\{A^t\}$. С этой целью рассмотрим мультипликативную группу

$$\mathbb{Z}_{p-1} = \{w_t = e^{2\pi i t/(p-1)}\},$$

где $0 \leqslant t < p-1$. Соответствующие гармоники

$$E_0, \ldots, E_{p-2} \colon \mathbb{Z}_{p-1} \to \mathbb{C}$$

задаются формулой $E_r(w) = w^r$.

Циклическая перестановка f^* действует на $\mathbb{Z}_{p-1}$ по формуле $Fw_t = f^* w_t = w_{t+1} = \varepsilon w_t$, где $\varepsilon = w_1 = e^{2\pi i/(p-1)}$.

Поэтому действие перестановки F на гармоники задаётся формулой

$$F^* E_r = \varepsilon^r E_r.$$

Следовательно, для временного среднего каждой гармоники мы получаем явное выражение

$$\widehat{E}_r := \frac{1}{T} \sum_{t=0}^{T-1} (F^*)^t E_r = \frac{1}{T}(1 + \varepsilon^r + \varepsilon^{2r} + \ldots + \varepsilon^{(T-1)r}) E_r = \frac{1}{T} \frac{\varepsilon^{Tr} - 1}{\varepsilon^r - 1} E_r.$$

В последнем случае мы считали $r \neq 0$; в случае $r = 0$ имеем среднее $\widehat{E}_r = E_0 = 1$.

При $r \neq 0$ функция $\widehat{E}_r$ стремится к 0 при $T \to \infty$, поэтому *временное среднее любой функции на группе $\mathbb{Z}_{p-1}$ стремится при $T \to \infty$ к её пространственному среднему по всей группе.*

Применим этот вывод для вычисления временных средних $\widehat{e}_k$ от гармоник e_k, где $k \neq 0$. Соответствующее пространственное среднее по группе $\mathbb{Z}_{p-1}$ легко вычисляется:

$$\frac{1}{p-1} \left(\sum_{t=0}^{p-1} (f^*)^t e_k \right) = \frac{1}{p-1} \sum_{k=1}^{p-1} e_k = -\frac{1}{p-1} e_0$$

(поскольку $\sum\limits_{k=0}^{p-1} e_k = 0$ по теореме Виета для уравнения $z^p = 1$).

Итак, при $p \to \infty$ среднее значение $\widehat{e}_k$ (где $k \neq 0$) стремится к нулю.

Следовательно, временное среднее по отрезку геометрической прогрессии $\{A^t\}$ от любой фиксированной комбинации гармоник на группе $\mathbb{Z}_p$ стремится при $p \to \infty$ к её пространственному среднему. Применяя это к характеристической функции изучаемой части G группы $\mathbb{Z}_p$, мы получаем предельное равномерное распределение отрезка прогрессии при $p \to \infty$.

Остаётся лишь обосновать переход к сумме растущего с p числа гармоник, нужного для аппроксимации характеристической функции G в $\mathbb{Z}_p$.

Замечание. В наших исследованиях асимптотической равнораспределённости при $p \to \infty$ мы фиксировали область G в вещественном торе T^n (измеримую по Жордану), а затем изучали число N попаданий членов длинной изучаемой последовательности в соответствующую область $G(p)$ на конечном n-мерном торе $\mathbb{Z}_p^n$ (область, состоящую из конечного, но растущего с p, числа точек).

Вероятно, наряду с естественно возникающими областями (вроде полос $0 \leqslant u \leqslant d$ в T^2), можно было бы брать и гораздо более сложные множества $G(p)$, например, потребовав, чтобы координата u точек области $G(p)$ в $\mathbb{Z}_p^2$ была чётной.

Гипотеза состоит в том, что выражающая равнораспределённость асимптотика числа попаданий при $p \to \infty$ сохраняется и для таких нерегулярных «областей», в предположении, что принадлежность к изучаемой области $G(p)$ определяется *не слишком сложным* алгоритмом.

Доказанных теорем этого рода я не знаю (даже и для распределения дробных долей членов арифметической прогрессии на окружности), хотя на возможность их существования указывает, например, теорема Сколема о нулях рекуррентных последовательностей $\{a_t\}$: *эти нули* $\{t : a_t = 0\}$ *образуют лишь конечное число арифметических прогрессий на оси* t (какова бы ни была рекуррентная последовательность).

Эргодическая сущность предполагаемых теорем этого рода состоит в том, что «*достаточно хаотическая» динамика препятствует предсказуемости любых алгоритмически просто вычислимых свойств траектории.*

Замечание. Рассмотренное выше в этом параграфе равномерное распределение отрезков геометрической прогрессии вдоль одномерного конечного тора $\mathbb{Z}_p$ может оказаться полезным и для исследования степени равномерности распределения отрезков геометрических прогрессий в конечных полях, имеющих большое число $z = p^n$ элементов, принадлежащих n-мерному тору.

Дело в том, что отображение $k \mapsto A^k$ взаимно однозначно отображает множество ненулевых остатков от деления на число $z - 1$ на множество ненулевых элементов поля из z элементов (n-мерного тора).

Поэтому из знания распределения *арифметической* прогрессии $\{tr,\ t=1,2,3,\dots\}$ в *одномерном* конечном торе $\mathbb{Z}_{z-1}$ можно извлечь информацию о распределении геометрической прогрессии $\{B^t,\ t=1,2,\dots\}$, где $B=A^r$, по n-мерному тору.

В частности, для исследования асимптотики числа попаданий N отрезка геометрической прогрессии $\{B^t\}$ в область G поля из z элементов достаточно знать асимптотику числа попаданий отрезка арифметической прогрессии $\{tr,\ t=1,2,\dots\}$ в полный прообраз $f^{-1}G$ области G при описанном выше взаимнооднозначном отображении $k\mapsto A^k$ (которое мы обозначим теперь через f).

В этом смысле для доказательства равномерности распределённости отрезка $\{B^t\}$ геометрической прогрессии в n-мерном (конечном) торе было бы достаточно доказать [выражающую равномерное распределение арифметической прогрессии $\{tr\}$ в одномерном конечном торе] пропорциональность числа попаданий в область её мере, но доказать это нужно не только для областей-подинтервалов в $\mathbb{Z}_{z-1}$, но и для других областей, заданных не слишком сложными алгоритмами (например, для множества $f^{-1}(G)$, где G — интересующая нас область на торе).

Хотя арифметическая прогрессия исследуется легче, чем геометрическая, прямому применению предыдущих одномерных результатов мешает не только довольно сложное строение нужных «одномерных» областей $f^{-1}(G)$, но и то, что нужный «одномерный» тор $\mathbb{Z}_{z-1}$ состоит из не простого числа точек (равного p^n-1), так что указанные одномерные результаты формально неприменимы (хотя получить их нужное обобщение на случай любого конечного одномерного тора представляется не слишком трудным).

§ 6
ПРОЕКТИВНЫЕ СТРУКТУРЫ ДЛЯ ПОЛЕЙ ГАЛУА

Алгебра поля Галуа имеет замечательный геометрический аналог, подобный тому, как обычная проективная геометрия (в том числе геометрия поверхностей второй степени и конических сечений) является изоморфной геометрической версией линейной алгебры (в том числе теории квадратичных форм). Вычисления собственных чисел всегда проще в алгебраической версии, но понимание сути дела достигается только при геометрическом анализе главных осей.

Гёте говорил, что «математики подобны французам: они всё переводят на свой язык, и получается *совсем не то*».

Я опишу теперь геометрический вариант алгебры поля Галуа: теорию проективных структур конечных множеств и действия на них групп «преобразований Фробениуса» возведения в степень, $\Phi_k(x) = x^k$.

Напомним сперва, что такое проективная прямая. Рассмотрим *все проходящие через точку* 0 *прямые на обычной плоскости* $\mathbb{R}^2$.

Многообразие всех таких прямых одномерно и диффеоморфно окружности. Вот как в этом убедиться. Если описывать точки плоскости декартовыми координатами (u, v), то прямая задаётся, вообще говоря, уравнением вида $u = \lambda v$ с некоторой (характеризующей прямую) постоянной λ (см. рис. 6.1). Постоянная λ называется *аффинной координатой на проективной прямой* (на множестве всех проходящих через точку 0 прямых плоскости).

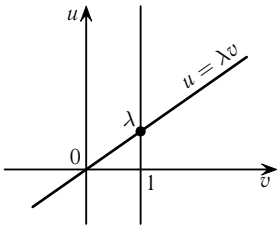


Рис. 6.1. Проективная прямая и аффинная координата λ на ней

Но, подобно тому, как одно полушарие не покрывает весь земной шар на карте полушарий, аффинная координата λ определена не для всех проходящих через точку 0 прямых на плоскости. А именно, вертикальная прямая ($v = 0$ рисунка 6.1) не задаётся уравнением $u = \lambda v$ ни при каком λ, поэтому говорят, что она является дополняющей ось λ бесконечно удалённой точкой проективной прямой (с естественным обозначением, $\lambda = \infty$).

Эта «бесконечно удалённая» точка ничем не отличается от остальных («конечных») точек проективной прямой, так же как проходящие через точку 0 прямые на плоскости все одинаковы (и, например, переводятся одна в другую поворотами плоскости).

При другом выборе исходной системы координат на плоскости (например, $\widetilde{u}=v, \widetilde{v}=u$) получилась бы другая аффинная координата ($\lambda=\widetilde{u}/\widetilde{v}$ в нашем примере) и другая «бесконечно удалённая» точка ($\widetilde{\lambda}=\infty$) на проективной прямой, которая теперь соответствует новой прямой ($\widetilde{v}=0$) на исходной плоскости, то есть «бесконечно удалённой» оказывается теперь горизонтальная, а не вертикальная прямая рисунка 6.1.

Зато в окрестности вертикальной прямой рисунка 6.1 (соответствующей значению $\widetilde{\lambda}=0$ в нашем примере) аффинная координата $\widetilde{\lambda}$ ($=1/\lambda$ в нашем примере системы координат с волной) регулярно параметризует проективную прямую. Следовательно, при стремлении аффинной координаты λ к плюс или минус бесконечности (в любую сторону) мы приходим в одно и то же место ($\widetilde{\lambda}=0$) в многообразии проходящих через точку 0 плоскости прямых (называемом вещественной проективной прямой и обозначаемом через $\mathbb{R}P^1$). Поэтому вещественная проективная прямая диффеоморфна окружности (рис. 6.2):

$$\mathbb{R}P^1 \sim S^1.$$

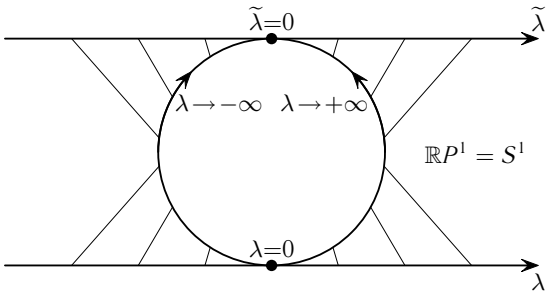


Рис. 6.2. Вещественная проективная прямая как окружность

При других выборах новых систем координат (быть может, не прямоугольных) на плоскости новая аффинная координата $\widetilde{\lambda}$ выражалась бы через старую дробно-линейно:

$$\widetilde{\lambda}=\frac{a\lambda+b}{c\lambda+d}, \tag{1}$$

поскольку на плоскости новые координаты линейно выражаются через старые ($\widetilde{u}=au+bv$, $\widetilde{v}=cu+dv$).

Здесь две новые оси координат не должны совпадать между собой, поэтому $ad \neq bc$.

Заданное формулой (1) преобразование оси λ называется проективным. Ось λ нужно дополнить при его определении бесконечно удалённой точкой, так что получится проективная прямая (окружность), и формула (1) определит её диффеоморфизм на себя.

Разумеется, в алгебре этой геометрии соответствуют соглашения ($\widetilde{\lambda} = \infty$ при $c\lambda + d = 0$), ($\widetilde{\lambda} = a/c$ при $\lambda = \infty$).

Совершенно аналогичным путём определяется вещественное проективное $(n-1)$-мерное пространство $\mathbb{R}P^{n-1} = (\mathbb{R}^n \setminus 0)/(\mathbb{R} \setminus 0)$ — это множество прямых, проходящих через точку 0 в пространстве $\mathbb{R}^n$. Аффинную карту можно построить из системы координат $(u_1, \ldots, u_n)$ в $\mathbb{R}^n$ так: если $u_n \neq 0$, то построим вектор $\lambda \in \mathbb{R}P^{n-1}$ с координатами $\lambda_1 = u_1/u_n, \ldots, \lambda_{n-1} = u_{n-1}/u_n$, т. е. рассмотрим точку λ пересечения прямой с гиперплоскостью $u_n = 1$ как точку аффинной карты, изображающей эту прямую (см. рис. 6.1).

Чтобы исчерпать все прямые, проходящие через ноль в пространстве $\mathbb{R}^n$, потребуется n таких аффинных карт, представленных n гиперплоскостями $\{u_n = 1\}$, $\{u_{n-1} = 1\}$, $\ldots$, $\{u_1 = 1\}$. Например, при $n = 2$ потребуется две аффинных карты (λ и $\widetilde{\lambda}$ на рис. 6.2).

Соответствующие изменению координат в $\mathbb{R}^n$ $(n = m+1)$ дробно-линейные преобразования задаются в $\mathbb{R}P^m$ следующим обобщением формул (1):

$$\widetilde{\lambda}_j = \frac{a_{j,1}\lambda_1 + a_{j,2}\lambda_2 + \ldots + a_{j,m}\lambda_m}{b_1\lambda_1 + b_2\lambda_2 + \ldots + b_m\lambda_m}, \quad \text{при } j = 1, \ldots, m$$

(надо обратить внимание на независимость знаменателя от номера j исследуемой координаты).

На геометрическом языке эти алгебраические формулы означают проективные преобразования, получающиеся, например, при $m = 2$ при проектировании одной плоскости в пространстве на другую выходящими из общего центра лучами (рис. 6.3).

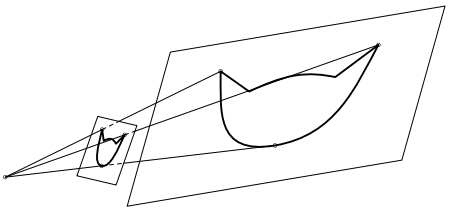


Рис. 6.3. Проективное преобразование кошки

Поэтому описываемая теория является основой и геометрии проектирований, переводящих прямые в прямые, и теории перспективы (где параллельные друг другу рельсы «пересекаются в бесконечно удалённой точке на горизонте»).

Великий итальянский художник Учелло (чьё имя означает «птичка»), одним из первых занявшийся строго математически правильным рисованием перспективных изображений, ответил жене, убеждавшей его оставить свои чертежи, чтобы идти спать: «сейчас приду — *какая прекрасная перспектива*», имея в виду свой замечательный рисунок.

Чтобы освоиться с этой проективной геометрией, стоит доказать следующие факты.

1. *Вещественная проективная плоскость не ориентируема*; вещественные проективные пространства $\mathbb{R}P^m$ ориентируемы при нечётных m и неориентируемы при чётных положительных m.

2. Дополнение к малому кругу на вещественной проективной плоскости диффеоморфно листу Мёбиуса (каковую поверхность Мёбиус ради этого и открыл).

Комплексные проективные пространства $\mathbb{C}P^m$ определяется так же как вещественные, но начиная с комплексного векторного пространства $\mathbb{C}^n$ (где, по-прежнему, $n = m + 1$). Точками этого комплексного проективного пространства являются проходящие через 0 комплексные прямые комплексного векторного пространства.

Аффинные координаты и проективные преобразования определяются теми же формулами, что и в вещественном случае (именно в этом преимущество алгебраистов: они вправе применять свои формулы к объектам, совершенно не сходным с теми, для которых эти формулы открыты, а если результат оказывается неверным, то они постулируют его, как (якобы) верный для своих «идеальных» объектов, исследованием которых и заменяют трудные изучения исходных объектов).

Всё же можно благополучно сделать всё это для проективных пространств и преобразований. Например, комплексная проективная прямая $\mathbb{C}P^1$ получается из обычной оси комплексного переменного λ добавлением одной бесконечно удалённой точки. Она вещественно диффеоморфна сфере S^2 и называется сферой Римана.

В окрестности «бесконечно удалённой» точки $\lambda = \infty$ аффинной (комплексной, как и λ) координатой служит функция $\widetilde{\lambda} = 1/\lambda$.

Комплексные прямые, проходящие через точку 0 комплексного пространства $\mathbb{C}^n$, пересекают сферу с центром в нуле (которая задаётся уравнением $\sum |u_k|^2 = 1$ и диффеоморфна S^{2n-1} в $\mathbb{R}^{2n}$) по окружности S^1 (тогда как вещественные прямые в $\mathbb{R}^n$, проходящие через 0, пересекают сферу S^m (где $m = n - 1$, $\sum |u_k|^2 = 1$) в двух точках, образующих «сферу» S^0).

В то время как вещественное проективное пространство $\mathbb{R}P^m$ можно получить из этой сферы S^m, отождествив в ней все пары диаметрально противоположных, т. е. вещественно пропорциональных друг другу,

точек,

$$\mathbb{R}P^m = S^m/S^0,$$

комплексное проективное пространство, $\mathbb{C}P^m$, *можно получить из сферы* S^{2n-1} (*где* $n=m+1$), *склеив в одну точку каждую окружность* S^1, *по которой эта сфера пересекает комплексную проходящую через ноль прямую* (все точки этой окружности попарно пропорциональны и получаются из любой одной из них умножением на все комплексные числа модуля 1):

$$\mathbb{C}P^m = S^{2m+1}/S^1.$$

Вещественно-четырехмерное многообразие $\mathbb{C}P^2$ получается из комплексной плоскости $\mathbb{C}^2$ добавлением бесконечно удалённой комплексной прямой $\mathbb{C}P^1$, т. е. добавлением сферы Римана:

$$\mathbb{C}P^2 = \mathbb{C}^2 \cup S^2.$$

Его можно также описать, как многообразие специальных больших окружностей $S^1 \subset S^3$. Специальная окружность образована пересечением трёхмерной сферы в комплексной плоскости в $\mathbb{C}^2$ с проходящей через 0 комплексной прямой. Поэтому специальная окружность составлена комплексно-пропорциональными друг другу точками сферы S^3:

$$\mathbb{C}P^2 = S^3/S^1.$$

Интересно отметить, что разные специальные окружности в гладко расслоённой на них трёхмерной сфере S^3 расположены специальным образом: их попарный коэффициент зацепления равен единице (для любой пары специальных окружностей).

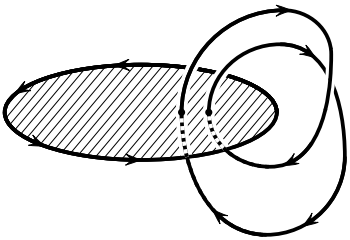


Рис. 6.4. Две кривые с равным двум коэффициентом зацепления

Коэффициент зацепления двух непересекающихся гладких замкнутых ориентированных кривых в ориентированном евклидовом трехмерном пространстве или в ориентированной трёхмерной сфере определяется как индекс пересечения одной из этих гладких кривых с гладкой ориентированной поверхностью, границей которой является вторая кривая (рис. 6.4).

Ориентации играют здесь следующую роль: ориентирующий поверхность репер в точке края составлен из касательного к краю вектора,

ориентирующего эту кривую-край, за которым следует направленный внутрь поверхности вектор.

Точки пересечения второй кривой с поверхностью, краем которой является первая кривая, доставляют индекс пересечения при их счёте со знаками: точка пересечения считается положительной, когда репер из трех векторов пространства, состоящий их двух векторов, ориентирующих поверхность, за которыми следует вектор, ориентирующий пересекающую поверхность кривую, ориентирует пространство положительно.

Коэффициент зацепления не зависит от выбора затягивающей кривую поверхности, нужно только, чтобы она нигде не касалась второй кривой. От выбора порядка кривых он тоже не зависит.

Расслоение трёхмерной сферы на описанные специальные окружности называется *расслоением Хопфа* $S^3 \to \mathbb{C}P^2$ (со слоем S^1) и является краеугольным камнем многих областей математики.

Если представлять себе трёхмерную сферу как евклидово трёхмерное пространство, пополненное одной бесконечно удалённой точкой, то расслоение Хопфа становится разбиением трёхмерного евклидова пространства на прямую и расслоение оставшейся области на замкнутые кривые с попарными коэффициентами зацепления, равными единице.

Хотя я умею рисовать это разбиение, я не стану здесь его показывать, чтобы не лишать читателя удовольствия нарисовать его самостоятельно.

Вместо этого мы займёмся теперь перенесением описанной выше в вещественном и в комплексном случаях теории проективных пространств и преобразований на случай, когда роль чисел играют остатки от деления на простое число p: мы определим *конечные проективные пространства* $P^m(\mathbb{Z}_p)$, вполне аналогичные вещественным многообразиям $\mathbb{R}P^m$ и комплексным многообразиям $\mathbb{C}P^m$.

Начнём с конечной проективной прямой $P^1(\mathbb{Z}_p)$. Она определяется как множество проходящих через нуль прямых на конечной плоскости $\mathbb{Z}_p^2$. Через координаты (u, v) на плоскости (являющиеся теперь остатками от деления на p) уравнение прямой записывается в обычном виде, $u = \lambda v$, но теперь «аффинная координата» $\lambda \in \mathbb{Z}_p$ также является остатком от деления на p. Чтобы получить все прямые, нужно добавить к этим p значениям аффинной координаты λ ещё одно значение, обозначаемое символом ∞ (для включения «вертикальной» прямой $v = 0$: ведь $\lambda = u/v$, когда v не нуль).

Итак, *конечная проективная прямая* $P^1(\mathbb{Z}_p)$ *состоит из* $p+1$ *точки*:

$$|P^1(\mathbb{Z}_p)| = p + 1.$$

Проективные преобразования,

$$\lambda \mapsto \frac{a\lambda + b}{c\lambda + d}, \tag{1}$$

(где $a, b, c, d \in \mathbb{Z}_p$, причём $ad - bc \neq 0$) являются перестановками этой $p+1$ точки, но отнюдь не любыми перестановками.

Действительно, симметрическая группа $S(p+1)$ всех перестановок $p+1$ точки нашей конечной проективной прямой состоит из $(p+1)!$ перестановок, а группа проективных преобразований гораздо меньше.

Лемма. *Группа* $\mathrm{PL}(\mathbb{Z}_p)$ *проективных преобразований* (1) *проективной прямой из* $p+1$ *точки состоит из* $p(p^2-1)$ *перестановок.*

Действительно, если $a \neq 0$, то мы можем, разделив все коэффициенты на a, записать преобразование (1) в виде, для которого $\widetilde{a} = 1$. При этом $\widetilde{b}$ и $\widetilde{c}$ могут иметь каждое (независимо от другого) p значений, а коэффициент $\widetilde{d}$ должен удовлетворять условию $\widetilde{d} \neq \widetilde{b}\widetilde{c}$ (имея $p-1$ возможное значение при фиксированных $\widetilde{b}$ и $\widetilde{c}$). Всего таких проективных преобразований $p^2(p-1)$.

Если же $a = 0$, то из невырожденности преобразования следует, что $bc \neq 0$. Если при этом $d \neq 0$, то, деля на этот коэффициент, мы можем записать преобразование формулой с коэффициентом $\widetilde{d} = 1$; число таких преобразований равно $(p-1)^2$, поскольку $\widetilde{b}\widetilde{c} \neq 0$. Наконец, если $d = 0$, то получается одно из $p-1$ преобразования $\lambda \mapsto b\lambda$.

Итого суммарное число проективных преобразований прямой $P^1(\mathbb{Z}_p)$ всех трёх типов равно сумме $p^2(p-1) + (p-1)^2 + (p-1) = (p-1)(p^2 + {} + (p-1) + 1) = p(p^2-1)$.

Величина $(p+1)!$ гораздо больше $p(p^2-1)$ при больших p (начиная с $p = 5$, когда $(p+1)! = 720$, $p(p^2-1) = 120$).

Дело в том, что *подгруппа проективных перестановок в* $S(p+1)$ *сохраняет ещё некоторую замечательную геометрическую структуру в конечном множестве* $P^1(\mathbb{Z}_p)$, *состоящем из* $p+1$ *точки.*

К сожалению, я не умею красиво описывать эту конечную проективную структуру, но формально она задаётся введением какой-либо аффинной координаты $\lambda \in \mathbb{Z}_p$ на дополнении к одной («бесконечно удалённой») точке «$\lambda = \infty$» рассматриваемого множества M.

Другая подобная координата $\widetilde{\lambda} : (M \setminus .) \to \mathbb{Z}_p$ определяет ту же самую проективную структуру на M, что и λ, если она связана с координатой λ проективным преобразованием (1).

Хотя это алгебраическое описание проективных структур на конечном множестве M и не очень геометрично, мы используем его ниже для исследования соответствующих полям Галуа из p^2 элементов структур на

множествах из $p+1$ элемента и для вычисления действия отображений Фробениуса указанных полей на эти проективные структуры конечных множеств.

А именно, зафиксировав мультипликативную образующую A поля из p^2 элементов, мы отобразим это поле взаимно однозначно на конечную плоскость (или тор) $\mathbb{Z}_p^2$ таблицы поля, как это описано в § 2.

После этого рассмотрим состоящую из $p+1$ точки прямую $P^1(\mathbb{Z}_p)$, точками которой являются проходящие через 0 прямые конечной плоскости $\mathbb{Z}_p^2$.

Лемма. *Множество прямых, проходящих через точку* 0 *на плоскости* $\mathbb{Z}_p^2$, *не зависит от выбора мультипликативной образующей* A *поля из* p^2 *элементов.*

Доказательство. Для двух пропорциональных точек x и cx, где c скаляр $c=1+\ldots+1$, соответствующие им элементы поля тоже скалярно пропорциональны: это A^k и $A^k+\ldots+A^k=cA^k$. Поэтому пропорциональность со скалярным коэффициентом пропорциональности определена инвариантно (не зависит от выбора образующего элемента A), что и доказывает лемму.

В отличие от *множества* прямых, его *проективная структура*, вообще говоря, *зависит* от выбора образующей, и при разных выборах мультипликативных образующих получатся (определяемые разными таблицами одного поля) разные проективные структуры того же множества из $p+1$ прямой.

Мы исследуем эти структуры в следующем параграфе.

Замечание. Проведённый только что анализ легко переносится на поля Галуа из p^n элементов (с любым n).

Прямые такого поля образуют конечное множество M, число точек которого есть

$$|P^m(\mathbb{Z}_p)|=\frac{p^n-1}{p-1}=p^m+p^{m-1}+\ldots+1$$

(где $n=m+1$).

Таблица поля (выбор мультипликативной образующей A) задаёт в этом конечном множестве M структуру конечного проективного пространства $P^m(\mathbb{Z}_p)$, но эта структура, в отличие от теоретико-множественной, *зависит* от выбора образующей, так что *проективная геометрия поля Галуа исследует не одну проективную структуру на* M, *а целый набор таких структур* (их число, как мы вскоре увидим, равно значению функции Эйлера, $\varphi(z-1)$), для поля из $z=p^n$ элементов.

Значение $\varphi(x)$ функции Эйлера φ определяется как число остатков от деления на натуральное число x, которые взаимно просты с x, например,

для простого числа p имеем $\varphi(p) = p - 1$, $\varphi(p^n) = (p-1)\,p^{n-1}$, а для взаимно простых аргументов x и y функция Эйлера мультипликативна, т. е. $\varphi(xy) = \varphi(x)\varphi(y)$.

Таким образом,

$$\varphi(24) = \varphi(3)\varphi(8) = 8, \qquad \varphi(48) = \varphi(3)\varphi(16) = 16,$$
$$\varphi(120) = \varphi(8)\varphi(3)\varphi(3) = 32, \qquad \varphi(168) = \varphi(8)\varphi(3)\varphi(7) = 48.$$

§ 7
ВЫЧИСЛЕНИЕ ПРОЕКТИВНЫХ СТРУКТУР НА КОНЕЧНЫХ ПРОЕКТИВНЫХ ПРЯМЫХ ДЛЯ ПОЛЕЙ ИЗ p^2 ЭЛЕМЕНТОВ

Рассмотрим в качестве простейшего примера поле из 25 элементов (т. е. случай $p=5$). Таблица этого поля вычислена выше (на стр. 14) для мультипликативной образующей, соответствующей матрице $(A)=\begin{pmatrix}0 & 2\\ 1 & 2\end{pmatrix}$.

Соответствующая полю и таблице проективная прямая $P^1(\mathbb{Z}_5)$ состоит из $p+1=6$ точек, определяемых при помощи заданной таблицей аффинной координаты $\lambda=u_k/v_k$ (для элемента A^k нашего поля).

Таким образом, таблица доставляет следующие 6 прямых $\{u_k=\lambda v_k\}$:

λ	показатели k	$k \pmod 6$
0	24, 18, 6, 12	0
1	8, 2, 14, 20	2
2	11, 5, 17, 23	5
3	10, 4, 16, 22	4
4	15, 9, 21, 3	3
∞	1, 19, 7, 13	1

Наблюдение последнего столбца этой таблицы чрезвычайно упрощает дальнейшие вычисления, и мы докажем соответствующее утверждение в более общей форме.

Лемма. *Проходящие через точку* 0 *плоскости* $\mathbb{Z}_p^2$ *прямые* $\{A^k\}$ *выделяются* (*при любом выборе мультипликативной образующей* A, *определяющей таблицу* $\mathbb{Z}_p^2$ *для поля из* p^2 *элементов*) *числовым сравнением* $k\equiv \text{const} \pmod{(p+1)}$ *для показателей* k, *входящих в прямую ненулевых элементов поля*.

Доказательство. Условие $A^k=cA^l$ (где c скаляр) принадлежности точек A^k и A^l одной прямой можно записать в виде скалярности элемента $A^{k-l}=c$. Поэтому мы исследуем *подгруппу скаляров* в циклической мультипликативной группе $\{A^k\}$, состоящей из p^2-1 элемента. Ненулевые скаляры образуют в ней подгруппу из $p-1$ элемента, $\{c=1, c=2, \ldots, c=(p-1)\}$.

Соответствующие элементам этой подгруппы $\{c=A^s\}$ показатели s образуют арифметическую прогрессию из $p-1$ члена в аддитивной группе $\mathbb{Z}_{p^2-1}$. Поэтому шаг упомянутой прогрессии составляет $(p^2-1)/(p-1)=$ $=p+1$, а значит, она имеет вид $\{s=(p+1)r$, где $r\in\{1,2,\ldots,p-1\}\}$ (ибо элемент $A^{p^2-1}=1$) принадлежит подгруппе скаляров $\{c\}$ и потому точка $s=p^2-1$ принадлежит арифметической прогрессии $\{s\}$).

Итак, необходимое и достаточное условие принадлежности ненулевых элементов A^k и A^l поля из p^2 элементов одной прямой состоит в соотношении $k-l=(p+1)r$, $r\in\mathbb{Z}$, что и доказывает лемму.

Отличные от A мультипликативные образующие поля из 25 элементов (в числе $\varphi(25-1)=\varphi(3)\cdot\varphi(8)=2\cdot 4=8$) доставляются элементами A^s поля со взаимно простыми с числом $24=p^2-1$ показателями $s\in\{1,5,7,11,13,17,19,23\}$.

Чтобы увидеть, как переставляет 6 точек проективной прямой переход к мультипликативной образующей $A_s=A^s$, достаточно взять одну из точек k, для которой λ имеет данное значение, и выразить A^k через A_s. Поскольку $A=A_s^r$, где $sr=1$ в Γ, мы получим $A^k=A_s^{rk}$. Из этого видно, что новый выбор образующей переводит каждую прямую *на то же место, что и преобразование Фробениуса* $\Phi_r=\Phi_s^{-1}$.

Поэтому мы рассмотрим теперь *действие отображений Фробениуса* Φ_s на наши прямые. С этой целью вычислим аффинную координату образа прямой с аффинной координатой λ прообраза и обозначим её через

$$\lambda_s(\lambda_1)=\lambda(\Phi_s(x)),\quad \text{где } \lambda(x)=\lambda_1.$$

Вычисляя таким образом функцию λ_s от λ_1, мы можем воспользоваться тем, что если $x=A^k$, то $\Phi_s(x)=A^{ks}$, так что для вычисления $\lambda_s(\lambda_1)$ достаточно выбрать по λ_1 любое k в предыдущей таблице, умножить его на s и найти значение функции λ по этому значению ks (по той же таблице, применяя её в обратную сторону).

Но, поскольку значение $\lambda(A^k)$ определяется остатком $k \pmod 6$ от деления k на 6, то нужно просто умножать на s этот остаток. В результате мы приходим к следующей таблице значений всех восьми функций λ_s. Например, $(\lambda_1=1)\Rightarrow(k\equiv 2)\Rightarrow(5k\equiv 10)\Rightarrow(\lambda_5=3)$, и так далее.

λ_1	0	1	2	3	4	∞
λ_5	0	3	∞	1	4	2
λ_7	0	1	2	3	4	∞
λ_{11}	0	3	∞	1	4	2
λ_{13}	0	1	2	3	4	∞
λ_{17}	0	3	∞	1	4	2
λ_{19}	0	1	2	3	4	∞
λ_{23}	0	3	∞	1	4	2

Эти вычисления можно ещё сильно сократить, учитывая сравнения $1\equiv 7\equiv 13\equiv 19 \pmod 6$, из-за них совпадают четыре функции $\lambda_1=\lambda_7=\lambda_{13}=\lambda_{19}$ (так что $P\Phi_7=P\Phi_{13}=P\Phi_{19}=P\Phi_1=$ (тождественное преобразование прямой $P^1\mathbb{Z}_5$), оставляющее все её точки на месте).

Точно так же, имеют место сравнения $5 \equiv 11 \equiv 17 \equiv 23 \pmod 6$, откуда вытекает совпадение между собой функций λ_5, λ_{11}, λ_{17}, λ_{23} и преобразований Фробениуса $P\Phi_5$, $P\Phi_{11}$, $P\Phi_{17}$ и $P\Phi_{23}$.

Тем самым мы вычислили гомоморфизм группы Эйлера Γ (преобразований Φ_s или остатков от деления s на $p^2-1=24$, взаимно простых с числом p^2-1) на её проективную версию, $\psi : \{\Phi_s\} \to \{P\Phi_s\}$ (где $P\Phi_s \in S(p+1)$ есть перестановка $p+1$ прямой преобразованием Фробениуса Φ_s поля из p^2 элементов).

При $p=5$ мы получаем:

1) $\Gamma \approx \mathbb{Z}_2^3$ (с образующими $a=5$, $b=7$, $c=13$, причём $11=ab$, $17=ac$, $19=bc$, $23=abc$),

2) $\psi(\Gamma) \approx \mathbb{Z}_2$ (с нетривиальным элементом $P\Phi_5$, действующим на точки оси λ как отражение диаграммы $\begin{matrix} 1 & 2 \\ \updownarrow & \updownarrow \\ 3 & \infty \end{matrix}$ $\quad 0 \qquad 4$ в горизонтальной оси).

3) Чтобы выяснить, проективна ли перестановка $P\Phi_5$ шести точек, заметим, что из равенства λ_5 нулю при $\lambda_1=0$ вытекало бы в случае проективности этой перестановки тождество

$$\lambda_5 = \frac{a\lambda_1}{(c\lambda_1+d)},$$

причём из равенства $\lambda_5=\infty$ при $\lambda_1=2$ следовало бы, что $2c+d=0$, тогда как равенство $\lambda_5=2$ при $\lambda_1=\infty$ означает, что $a=2c$. Мы получаем, таким образом, что $d=-2c$, $a=2c$, т. е. что для проективности преобразования Φ_5 должно выполняться тождество $\lambda_5 = 2\lambda_1/(\lambda_1-2)$.

Это тождество, действительно, выполняется для всех шести значений λ_1. Итак, выводы такие:

1) *проективная структура на прямой $P^1(\mathbb{Z}_5)$ не зависит от выбора мультипликативной образующей*, которые все 8 приводят к одной и той же структуре, какой бы из восьми разных таблиц поля мы ни пользовались для определения этой структуры;

2) *ядро гомоморфизма ψ* состоит из четырёх (не сдвигающих ни одну прямую) преобразований Фробениуса $\{\Phi_1, \Phi_7, \Phi_{13}, \Phi_{19}\}$, образующих группу, изоморфную $\mathbb{Z}_2^2$;

3) *образ гомоморфизма ψ* изоморфен $\mathbb{Z}_2$ и его единственная нетривиальная перестановка шести точек прямой $P^1(\mathbb{Z}_5)$ проективна, оставляет на месте точки $\lambda_1=0$ и $\lambda_1=4$ и переставляет между собой точки пар ($\lambda_1=1$ с $\lambda_1=3$), ($\lambda_1=2$ с $\lambda_1=\infty$). Эта перестановка задаётся формулой $\lambda_5 = \dfrac{2\lambda_1}{\lambda_1-2}$; она порождена автоморфизмом Φ_5 поля из 25 элементов (для которого, в отличие от преобразования Φ_7, выполнено тождество $\Phi_5(x+y)=\Phi_5(x)+\Phi_5(y)$).

Вычисления проективных структур и преобразований Фробениуса для полей из p^2 элементов с другими простыми числами p следуют такой же схеме, но ответы получаются удивительно разнообразными для разных p, и я не располагаю ни теоремами, ни даже гипотезами об этих ответах при бóльших значениях p, чем в описанных ниже примерах.

Случай $p = 7$.

Группа Эйлера Γ состоит из $\varphi(p^2-1) = \varphi(48) = \varphi(3)\varphi(16) = 16$ взаимно простых с числом 48 остатков,

$$\{1,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 25,\ 29,\ 31,\ 35,\ 37,\ 41,\ 43,\ 47\}.$$

Эта группа изоморфна произведению $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ (с образующими 5 для $\mathbb{Z}_4$ и 7, 17 для сомножителей $\mathbb{Z}_2$).

Восемь точек проективной прямой $P^1(\mathbb{Z}_7)$, соответствующие элементам A^k поля, где $(A) = \begin{pmatrix} 0 & 2 \\ 1 & 2 \end{pmatrix}$, определяются остатками от деления показателя k на 8 так:

$\lambda_1(A^k)$	0	1	2	3	4	5	6	∞
$k \pmod 8$	0	2	6	7	5	3	4	1

(по таблице поля на стр. 16).

Действие образующих группы Эйлера преобразованиями Фробениуса Φ_5, Φ_7 и Φ_{17} доставляет значения функций λ_5, λ_7, λ_{11} (по подробно описанному выше в случае $p = 5$ алгоритму умножения k на s).

λ_1	0	1	2	3	4	5	6	∞
λ_5	0	1	2	5	∞	3	6	4
λ_7	0	2	1	∞	5	4	6	3
λ_{17}	0	1	2	3	4	5	6	∞

(для $P\Phi_{17}$ вычислять ничего не нужно, поскольку $17 \equiv 1 \pmod 8$, так что перестановка прямых $P\Phi_{17} = P\Phi_1$ — тождественное преобразование проективной прямой $P^1(\mathbb{Z}_7)$ и $\lambda_{17} \equiv \lambda_1$).

Перестановки $P\Phi_5$ и $P\Phi_7$ переставляют точки с разными значениями λ как отражения в горизонтальной прямой следующих диаграмм

$$P\Phi_5: \begin{matrix} 3 & 4 & & & & \\ \updownarrow & \updownarrow & 0 & 1 & 2 & 6. \\ 5 & \infty & & & & \end{matrix}$$

$$P\Phi_7: \begin{matrix} 1 & 3 & 4 & & \\ \updownarrow & \updownarrow & \updownarrow & 0 & 6. \\ 2 & \infty & 5 & & \end{matrix}$$

Первая перестановка, $P\Phi_5$, не проективна, так как она имеет четыре неподвижных точки, а такое преобразование проективной прямой оставляет неподвижными все её точки.

Для предположительно проективной перестановки $P\Phi_7$ мы выводим из $0 \mapsto 0$ вид $\lambda_7 = \dfrac{a\lambda_1}{c\lambda_1 + d}$, из $3 \mapsto \infty$ следует тогда, что $3c + d = 0$, а из $\infty \mapsto 3$ — что $a = 3c$. Итак, значение функции λ_5 должно всюду равняться $3\lambda_1/(\lambda_1 - 3)$, что и выполняется.

Перемножая вычисленные перестановки, мы находим весь гомоморфизм проективизации $\psi : (\Gamma = \{\Phi_s\}) \to \{P\Phi_s\}$.

Окончательные выводы таковы.

1) На множестве 8 точек конченой проективной прямой $P^1(\mathbb{Z}_7)$ *при различных выборах мультипликативной образующей поля из* 49 *элементов получаются* 2 *разных проективных структуры, переходящие друг в друга при перестановке* $P\Phi_5$, *определённой выше.*

2) Перестановка $P\Phi_7$ сохраняет обе проективные структуры множества точек прямой $P^1(\mathbb{Z}_7)$.

3) Перестановка $P\Phi_{17} = P\Phi_1$ оставляет неподвижной все точки прямой $P^1(\mathbb{Z}_7)$, то есть Φ_{17} входит в *ядро гомоморфизма проективизации* ψ. *Ядро*, $\operatorname{Ker}\psi$, *состоит из четырёх преобразований Фробениуса* Φ_s,

$$\operatorname{Ker}\psi = \{\Phi_1, \Phi_{17}, \Phi_{25}, \Phi_{41}\},$$

для которых s сравнимо с 1 по модулю 8. Эта группа изоморфна $\mathbb{Z}_2^2$ (например, $\Phi_{17} = \Phi_{25} = \Phi_{41}$).

4) *Образ гомоморфизма проективизации* тоже изоморфен $\mathbb{Z}_2^2$. Он состоит из четырёх перестановок $(P\Phi_1, P\Phi_5, P\Phi_7, P\Phi_{11})$, из которых $P\Phi_1 = 1$ и $P\Phi_7$ являются проективными (сохраняют обе проективные структуры), а $P\Phi_5$ и $P\Phi_{11}$ переставляют их.

Преобразование Фробениуса Φ_7 являются автоморфизмом поля из 49 элементов $(\Phi_7(x + y) = \Phi_7(x) + \Phi_7(y))$, в отличие от преобразований Φ_5 и Φ_{11}.

Из всего этого следует, что на множестве (двух) проективных структур прямой $P^1(\mathbb{Z}_7)$, определённых разными мультипликативными образующими поля из 49 элементов, группа $\{P\Phi_s\} \approx \mathbb{Z}_2^3$ действует как $\mathbb{Z}_2$ (с ядром $\{P\Phi_1, P\Phi_7\}$, порождённым автоморфизмами Фробениуса поля).

Одна и другая проективные структуры получаются из таблицы поля при таких выборах мультипликативной образующей A^s:

P_1	1	7	17	23	25	31	41	47	$s = 8r \pm 1$
P_5	5	11	13	19	29	35	37	43	$s = 8r \pm 3$

При этом *преобразования Фробениуса* Φ_s *первой строки* (*где* $s = 8r \pm 1$) *сохраняют обе структуры* P_1 *и* P_5, *а второй* (*где* $s = 8r \pm 3$) *переставляют их*.

Случай $p = 11$.

Группа Эйлера Γ состоит из $\varphi(p^2-1) = \varphi(120) = \varphi(3)\varphi(5)\varphi(8) = 32$ взаимно простых с числом 120 остатков,

$$\{1,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31,\ 35,\ 37,\ 41,\ 43,\ 47,\ 49,\ 53,\ 59,\ 61,\ \ldots\}$$

(включая $120 - s$ вместе с s).

Эта группа изоморфна произведению $\mathbb{Z}_4 \times \mathbb{Z}_2^3$ (с образующими 7 для $\mathbb{Z}_4$ и 11, 19, 61 для сомножителей $\mathbb{Z}_2$).

12 точек проективной прямой $P^1(\mathbb{Z}_{11})$, соответствующие элементам A^k поля, где $(A) = \begin{pmatrix} 0 & 3 \\ 1 & 1 \end{pmatrix}$, определяются остатками от деления показателя k на 12 так:

$\lambda_1(A^k)$	0	1	2	3	4	5	6	7	8	9	10	∞
$k \pmod{12}$	0	9	7	5	2	3	8	4	10	6	11	1

(по таблице поля на стр. 16).

Действие образующих группы Эйлера преобразованиями Фробениуса Φ_7, Φ_{11}, Φ_{19} и Φ_{61} доставляет следующую таблицу значений функций λ_7, λ_{11}, λ_{19}, λ_{61} на $P^1(\mathbb{Z}_{11})$, задающих перестановки $P\Phi_7, \ldots, P\Phi_{61} \in S(12)$ двенадцати точек проективной прямой $P^1(\mathbb{Z}_{11})$:

$$\lambda_s(\lambda_1(x)) = \lambda_1(\Phi_s(x)).$$

Как объяснено выше (при $p = 5$), вычисление $\lambda_s(\lambda_1)$ по предыдущей таблице производится так:

$$(\lambda_1 \mapsto k), \quad (k \mapsto sk), \quad (sk \mapsto \lambda_1(A^{sk})),$$

с использованием таблицы сперва сверху вниз, а потом снизу вверх.

Эти вычисления достаточно проводить только для одного представителя каждого из классов сравнимых по модулю 12 показателей $s \in \Gamma$:

$$\begin{array}{r} \Gamma_1: \ 1 \sim 13 \sim 37 \sim 49 \sim 61 \sim 73 \sim \ 97 \sim 109 \\ \Gamma_7: \ 7 \sim 19 \sim 31 \sim 43 \sim 67 \sim 79 \sim \ 91 \sim 103 \\ \Gamma_{11}: 11 \sim 23 \sim 47 \sim 59 \sim 71 \sim 83 \sim 107 \sim 119 \\ \Gamma_{17}: 17 \sim 29 \sim 41 \sim 53 \sim 77 \sim 89 \sim 101 \sim 113 \end{array}$$

В случае Γ_1 преобразование $P\Phi_s$ тождественно, $\lambda_1 = \lambda_{13} = \lambda_{37} = \ldots$ $\ldots = \lambda_{109}$.

Вычисление перестановки $P\Phi_{17}$ (и функций $\lambda_{17}=\lambda_{29}=\ldots=\lambda_{113}$) сводится к перемножению перестановок $P\Phi_7$ и $P\Phi_{11}$ (поскольку $7\cdot 11=77\in$ $\in\Gamma_{17}$). Остаётся вычислить лишь функции λ_7 и λ_{11}, для которых предыдущая таблица значений $\lambda_1(A^k)$ быстро доставляет ответы $\lambda_1\mapsto k\mapsto sk\mapsto$ $\mapsto\lambda_1(A^k)$:

λ_1	0	1	2	3	4	5	6	7	8	9	10	∞
λ_7	0	5	∞	10	4	1	6	7	8	9	3	2
λ_{11}	0	5	3	2	8	1	7	6	4	9	∞	10
λ_{17}	0	1	10	∞	8	5	7	6	4	9	2	3

Перестановки $P\Phi_7$, $P\Phi_{11}$ и $P\Phi_{17}$ переставляют точки проективной прямой $P^1(\mathbb{Z}_{11})$ с различными значениями аффинной координаты $\lambda=\lambda_1$, как отражения следующих диаграмм в горизонтальной прямой

$$P\Phi_7:\ \begin{matrix}1\\ \updownarrow\\ 5\end{matrix}\ \begin{matrix}2\\ \updownarrow\\ \infty\end{matrix}\ \begin{matrix}3\\ \updownarrow\\ 10\end{matrix}\ 0\ \ 1\ \ 4\ \ 6\ \ 7\ \ 8\ \ 9,$$

$$P\Phi_{11}:\ \begin{matrix}1\\ \updownarrow\\ 5\end{matrix}\ \begin{matrix}2\\ \updownarrow\\ 3\end{matrix}\ \begin{matrix}4\\ \updownarrow\\ 8\end{matrix}\ \begin{matrix}6\\ \updownarrow\\ 7\end{matrix}\ \begin{matrix}10\\ \updownarrow\\ \infty\end{matrix}\ 0\ \ 9,$$

$$P\Phi_{17}:\ \begin{matrix}2\\ \updownarrow\\ 10\end{matrix}\ \begin{matrix}3\\ \updownarrow\\ \infty\end{matrix}\ \begin{matrix}4\\ \updownarrow\\ 8\end{matrix}\ \begin{matrix}6\\ \updownarrow\\ 7\end{matrix}\ 0\ \ 1\ \ 5\ \ 9.$$

Из этих диаграмм следует, что инволюции $P\Phi_7$ и $P\Phi_{17}$ не сохраняют проективной структуры P_1 прямой $P^1(\mathbb{Z}_{11})$, заданной координатой λ_1, а инволюция $P\Phi_{11}$ сохраняет её, поскольку $\lambda_{11}=-\dfrac{\lambda_1}{\lambda_1+1}$ дробно-линейно зависит от λ_1.

Образы проективной структуры P_1 под действием перестановок $P\Phi_7$ и $P\Phi_{17}$ одинаковы:

$$P_7:=P\Phi_7(P_1)=P_{17}:=P\Phi_{17}(P_1),$$

поскольку функции λ_7 и λ_{17} связаны дробно-линейно:

$$\lambda_{17}=-\frac{\lambda_7}{\lambda_7+1}.$$

Перестановка $P\Phi_{11}$ (порождённая автоморфизмом Фробениуса Φ_{11} поля из 121 элементов) сохраняет обе проективные структуры P_1 и P_7 $(=P_{11})$ на проективной прямой $P^1(\mathbb{Z}_{11})$ из 12 точек, а перестановки $P\Phi_7$ и $P\Phi_{17}$ переставляют эти две проективные структуры, P_1 и P_7.

Ядро гомоморфизма проективизации $\psi : (\Gamma \sim \{\Phi_s\}) \mapsto \{P\Phi_s\}$ состоит из восьми образующих Γ_1 преобразований Фробениуса Φ_s, где $s = 12r + 1$, т. е. $s \in \{1,\ 13,\ 37,\ 49,\ 61,\ 73,\ 97,\ 109\}$,

$$\operatorname{Ker}\psi \approx \mathbb{Z}_4 \times \mathbb{Z}_2,$$

образующие: $s = 13$ для $\mathbb{Z}_4$, $s = 61$ для $\mathbb{Z}_2$.

Образ гомоморфизма проективизации ψ состоит из четырёх перестановок $\{P\Phi_1, P\Phi_7, P\Phi_{11}, P\Phi_{17}\}$, образующих группу, изоморфную $\mathbb{Z}_2^2$. Её действие на точки проективной прямой $P^1(\mathbb{Z}_{11})$ и на её две проективные структуры, P_1 и P_7, доставляемые полем из 121 элемента, описано выше (в частности, $P\Phi_{17} = P\Phi_{11}(P\Phi_7)$, $\quad P\Phi_{11}(P\Phi_{11}) = P\Phi_7(P\Phi_7) = 1$).

Из всего этого вытекает, что группа Γ из 32 преобразований Фробениуса действует на множестве из двух связанных с полем из 121 элемента проективных структур P_1 и P_7, как группа $\mathbb{Z}_2$ их перестановок (причём на месте обе эти структуры остаются при 16 преобразованиях $P\Phi_s$, для которых $s = 12r \pm 1$ $(r \in \mathbb{Z})$, т. е. когда s принадлежит спискам Γ_1 и Γ_{11} выше, в то время как 16 преобразований $P\Phi_s$, для которых $s = 12r \pm 5$ $(\in \mathbb{Z})$, то есть когда s принадлежит спискам Γ_7 и Γ_{17} выше, переставляют между собой структуры P_1 и P_7).

Итак, ядро гомоморфизма $\varphi : \Gamma \to \mathbb{Z}_2$, определённого действием преобразований Фробениуса на проективные структуры, есть $\operatorname{Ker}\varphi = \Gamma_1 \cup \Gamma_{11} \approx$ $\approx \mathbb{Z}_4 \times \mathbb{Z}_2^2$ (образующие Φ_{13} для $\mathbb{Z}_4$, Φ_{61} и Φ_{11} для групп $\mathbb{Z}_2$).

Случай $p = 13$.

Группа Эйлера Γ состоит из $\varphi(p^2 - 1) = \varphi(168) = \varphi(3)\varphi(7)\varphi(8) = 48$ взаимно простых с числом 168 остатков,

$$\{1,\ 5,\ 11,\ 13,\ 17,\ 19,\ 23,\ 25,\ 29,\ 31,\ 37,\ 41,\ 43,\ 47,\ 53,\ 59,\ 61,\ 65,\ 67,\ 71,\ 73,\ 79,\ 83,\ 85, \ldots\}$$

(вместе с s в Γ включается и $168 - s$).

Эта группа изоморфна произведению четырёх циклических групп $\mathbb{Z}_6 \times \mathbb{Z}_2^3$ (образующие: 5 для $\mathbb{Z}_6$, 29, 43, 85 для сомножителей второго порядка).

14 точек проективной прямой $P^1(\mathbb{Z}_{13})$, соответствующие элементам A^k поля из 169 элементов, где выбрана образующая $(A) = \begin{pmatrix} 0 & 2 \\ 1 & 4 \end{pmatrix}$, определяются остатками от деления показателя k на $p + 1 = 14$ так:

$\lambda_1(A^k)$	0	1	2	3	4	5	6	7	8	9	10	11	12	∞
$k \pmod{14}$	0	8	2	13	11	6	7	12	4	9	10	5	3	1

(по таблице поля на стр. 21).

Действие образующих группы Эйлера преобразованиями Фробениуса (Φ_5, Φ_{29}, Φ_{43}, Φ_{85}) доставляет значения функций λ_5, λ_{29}, λ_{43} и λ_{85} по обычному алгоритму

$$(\lambda_1 \mapsto k), \quad (k \mapsto sk), \quad (\lambda_s = \lambda_1(A^{sk})).$$

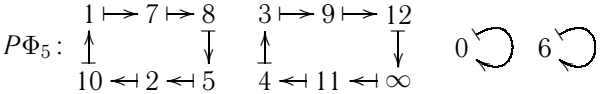
Из этого следует, что перестановка $P\Phi_s$ зависит лишь от остатка от деления показателя s на 14, так что вся группа Эйлера Γ разбивается на 6 классов смежности чисел s по модулю 14:

$$\begin{array}{rll}
\Gamma_1: & \{1,29,43,71,85,113,127,155\}, & s = 14r+1;\\
\Gamma_5: & \{5,19,47,61,89,103,131,145\}, & s = 14r+5;\\
\Gamma_{11}: & \{11,25,53,67,95,109,137,151\}, & s = 14r-3;\\
\Gamma_{13}: & \{13,41,55,83,97,125,139,167\}, & s = 14r-1;\\
\Gamma_{17}: & \{17,31,59,73,101,115,143,157\}, & s = 14r+3;\\
\Gamma_{23}: & \{23,37,65,79,107,121,149,163\}, & s = 14r-5;
\end{array}$$

Таблица соответствий k и $\lambda_1(A^k)$, приведённая выше, доставляет следующие значения функций λ_s:

λ_1	0	1	2	3	4	5	6	7	8	9	10	11	12	∞
λ_5	0	7	10	9	3	2	6	8	5	12	1	4	∞	11
λ_{11}	0	8	1	12	9	10	6	5	2	∞	7	3	11	4
λ_{13}	0	5	7	∞	12	1	6	2	10	11	8	9	4	3
λ_{17}	0	10	5	4	11	8	6	1	7	3	2	∞	9	12
λ_{23}	0	2	8	11	∞	7	6	10	1	4	5	12	3	9

Перестановка $P\Phi_5$ действует, следовательно, на 14 точек проективной прямой $P^1(\mathbb{Z}_{13})$ так:

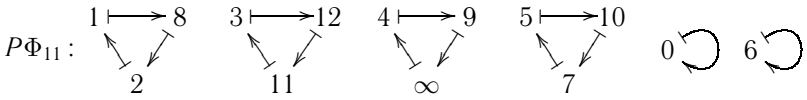


(точки проективной прямой изображены своими аффинными координатами, $\lambda_1(A^k)$): две орбиты перестановки состоят из 6 точек и 2 точки неподвижны. Полезно отметить, что $(P\Phi_7)^6 = 1$.

Перестановка $P\Phi_5$ не проективна, так как в противном случае мы имели бы тождество $\lambda_5 = a\lambda_1/(c\lambda_1 + d)$, ввиду того, что $\lambda_5 = 0$ при $\lambda_1 = 0$. Тогда условие ($\lambda_5 = \infty$ при $\lambda_1 = 12$) дало бы $12c + d = 0$, а условие ($\lambda_5 = 11$ при $\lambda_1 = \infty$) дало бы соотношение $a = 11c$. Стало быть, проективная перестановка должна бы была описываться функцией $\lambda_5 = 11/(-11) = 12$, тогда как на самом деле в таблице $\lambda_5(1) = 2$.

Итак, перестановка $P\Phi_5$ переводит обычную проективную структуру P_1 (соответствующую координате λ_1) в новую проективную структуру P_5 (соответствующую координате λ_5).

Перестановка $P\Phi_{11}$ переставляет 14 точек прямой $P^1(\mathbb{Z}_{13})$ так:



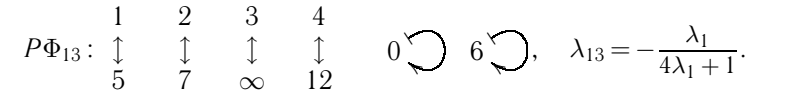
(две неподвижных точки и четыре трёхточечных орбиты). Полезно заметить, что $P\Phi_{11} = (P\Phi_5)^2$ и что $(P\Phi_{11})^3 = 1$. Если бы эта перестановка $P\Phi_{11}$ была проективна, то было бы $\lambda_{11} = a\lambda_1/(c\lambda_1 + d)$, причём из $(9 \mapsto \infty)$ следовало бы $(9c + d = 0)$, а из $(\infty \mapsto 4)$ следовало бы $(a = 4c)$, так что получилось бы проективное преобразование

$$\lambda_{11} = 4\frac{\lambda_1}{\lambda_1 - 9}.$$

Стало быть, тогда было бы λ_{11} $(\lambda_1 = 1)$ $= 4/(-8) = -20 = 6 \pmod{13}$, вопреки табличному значению $\lambda_{11}(1) = 8$.

Итак, перестановка $P\Phi_{11}$ не проективна, и она переводит стандартную проективную структуру P_1, заданную аффинной координатой λ_1, в новую проективную структуру P_{11} (заданную аффинной координатой λ_{11}).

Перестановка $P\Phi_{13}$ проективна, так как она порождается автоморфизмом Φ_{13} поля из 169 элементов. Это видно и из таблицы функции λ_{13}:



$$\lambda_{13} = -\frac{\lambda_1}{4\lambda_1 + 1}.$$

Остальные перестановки $P\Phi_s$ (при $s = 17$ и 23) получаются теперь простым умножением:

$$13 \cdot 5 = 65 \in \Gamma_{23}, \quad 13 \cdot 11 = 143 \in \Gamma_{17},$$

поэтому

$$P\Phi_{23} = P\Phi_5(P\Phi_{13}), \quad P\Phi_{17} = P\Phi_{11}(P\Phi_{13}).$$

Стало быть, перестановка $P\Phi_{23}$ переводит структуру P_1 в структуру P_5 (сначала перестановка $P\Phi_{13}$ переводит P_1 в себя, а потом перестановка $P\Phi_5$ превращает её в P_5).

Точно так же перестановка $P\Phi_{17}$ переводит структуру P_1 в структуру P_{11}.

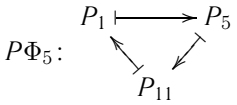
Кроме того, перестановка $P\Phi_{13}$ сохраняет также каждую из структур P_5 и P_{11}, поэтому перестановка $P\Phi_{23}$ сохраняет структуру P_5, а перестановка $P\Phi_{17}$ сохраняет структуру P_{11}.

Действие перестановки $P\Phi_5$ на структуру P_{11} можно исследовать при помощи аффинной координаты λ_{11}, вычислив значение функции λ_{11} в точке x^5, при данном $\lambda_{11}(x)$.

Поскольку $P\Phi_{11}(P\Phi_5) = P\Phi_{13}$ (ибо $55 \in \Gamma_{13}$), $\lambda_{11}(x^5) := \lambda_1(x^{55}) = \lambda_1(x^{13}) = \lambda_{13}(x)$, так что речь идёт о зависимости $\lambda_{13}(x)$ от $\lambda_{11}(x)$, сразу доставляемой нашей таблицей функций λ_1:

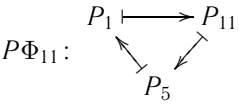
$\lambda_{11}(x)$	0	1	2	3	4	5	6	7	8	9	10	11	12	∞
$\lambda_{13}(x)$	0	7	10	9	3	2	6	8	5	12	1	4	∞	11

Итак, преобразование Φ_5 действует на структуру P_{11} так же, как на структуру P_1: оно не сохраняет её, а переводит её в новую проективную структуру P_{13} (заданную аффинной координатой λ_{13}). Но структура P_{13} совпадает со структурой P_1, так как преобразование Фробениуса Φ_{13} является автоморфизмом поля из 169 элементов. Итак, *преобразование* Φ_5 *действует на проективные структуры так*:



(она переводит структуру P_5 в структуру P_{11} потому, что $5 \cdot 5 = 25 \in \Gamma_{11}$).

Совершенно таким же образом исследуется действие на эти 3 структуры преобразования $P\Phi_{11}$, связанного, впрочем, с перестановкой $P\Phi_5$ тождеством $P\Phi_{11} = (P\Phi_5)^2$ и, следовательно, *действующего на структуры как обратная к* $P\Phi_5$ *перестановка трёх структур*:



Описание ядра и образа гомоморфизма проективизации

$$\psi\colon (\Gamma \sim \{\Phi_s\}) \mapsto (\{P\Phi_s\})$$

также содержится в наших явных формулах для этих перестановок. *Ответы такие*:

$$\Gamma \sim (\mathbb{Z}_6 \times \mathbb{Z}_2^3),$$
$$\operatorname{Ker}\psi \sim \mathbb{Z}_2^3, \quad \operatorname{Im}\psi \sim \mathbb{Z}_6.$$

Ядро состоит из 8 *преобразований Фробениуса* Φ_s *класса* Γ_1 ($s = 14r + 1$). В качестве *образующих ядра* можно взять, например, преобразования Φ_{29}, Φ_{43}, Φ_{85} (ведь $\Phi_{71} = \Phi_{29}(\Phi_{43})$, $\Phi_{113} = \Phi_{29}(\Phi_{85})$, $\Phi_{127} = \Phi_{43}(\Phi_{85})$, $\Phi_{155} = \Phi_{29}(\Phi_{43}(\Phi_{85}))$).

В качестве образующей образа можно взять перестановку шестого порядка $g = P\Phi_5$. Образ состоит из её степеней, $g^2 = P\Phi_{11}$, $g^3 = P\Phi_{13}$, $g^4 = P\Phi_{37}$, $g^5 = P\Phi_{17}$, $g^6 = 1$ (поскольку $5^2 \in \Gamma_{11}$, $5^3 \in \Gamma_{13}$, $5^4 \in \Gamma_{37}$, $5^5 \in \Gamma_{17}$).

На три связанные с полем из 169 элементов проективные структуры P_1, P_5, P_{11} перестановка g действует, переставляя их циклически (так что g^3 оставляет все три структуры на месте, будучи автоморфизмом Фробениуса нашего поля).

К сожалению, я не располагаю ни теоремами, ни даже гипотезами о том, как вся эта проективная теория переносится на поля из бóльшего числа элементов (даже в случаях p^2 элементов с бóльшими простыми значениями p). По-видимому, для обнаружения этих обобщающих изложенную выше теорию ответов необходимо прежде всего явно вычислить проективные структуры и действия преобразований Фробениуса на них (хотя бы для полей из p^2 элементов) в бóльшем числе примеров, так как разнообразие ответов в разобранных случаях $p = 5,\ 7,\ 11$ и 13 мешает угадать, как будет обстоять дело при бóльших значениях p.

Автор благодарен слушателям за многочисленные полезные замечания и надеется на плодотворное сотрудничество с будущими читателями этих лекций, которым многое предстоит ещё сделать.

ПРИЛОЖЕНИЕ.
КУБИЧЕСКИЕ ТАБЛИЦЫ ПОЛЕЙ

Ниже приведены таблицы полей из 8, 27, 125, 16 и 81 элементов.

Для поля из p^3 элементов мы выбираем в качестве аддитивного базиса элементы 1, A и A^2, выбрав сперва мультипликативную образующую A. Таблица поля заполняет точки (u, v, w) конечного куба (тора) $\mathbb{Z}_p^3$ показателями $k \pmod{(p^3-1)}$ степеней A^k мультипликативной образующей,

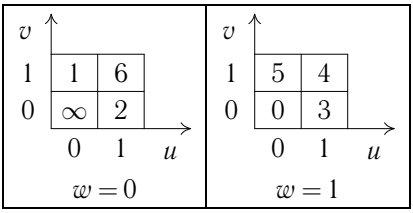
$$A^k = u_k A^2 + v_k A + w_k 1.$$

Чтобы изобразить этот куб, ниже приведены заполнения его плоских сечений $w = \text{const}$ соответствующими показателями k. Появление числа k в клеточке (u, v) квадрата номер w в таблице поля означает тождество

$$A^k = uA^2 + vA + w1.$$

Эти таблицы квадратных сечений куба (тора) приведены ниже для $p = 2, 3$ и 5.

Таблица поля из 2^3 элементов.

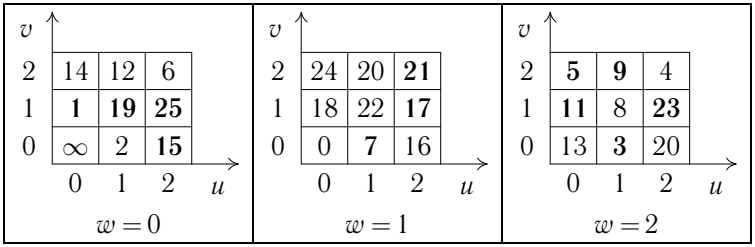


Эта таблица составлена для мультипликативной образующей, заданной (в матричном представлении поля) матрицей

$$(A) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix}.$$

Таблица является краткой геометрической записью 6 тождеств, $A^0 = 1$, $A^3 = A^2 + 1$, $A^4 = A^2 + A + 1$, $A^5 = A + 1$, $A^6 = A^2 + A$, $A^7 = 1$. Эти тождества рекуррентно вытекают из второго из них. Число производящих элементов A^k, где $1 \leqslant k \leqslant 6$, равно $\varphi(2^3 - 1) = 6$.

Таблица поля из 3^3 элементов.



v	$u=0$	$u=1$	$u=2$
2	14	12	6
1	**1**	**19**	**25**
0	∞	2	**15**

$w=0$

v	$u=0$	$u=1$	$u=2$
2	24	20	**21**
1	18	22	**17**
0	0	**7**	16

$w=1$

v	$u=0$	$u=1$	$u=2$
2	**5**	**9**	4
1	**11**	8	**23**
0	13	**3**	20

$w=2$

В качестве мультипликативной образующей выбран элемент поля, представленный матрицей

$$(A)=\begin{pmatrix}0&1&0\\0&0&1\\2&0&1\end{pmatrix}.$$

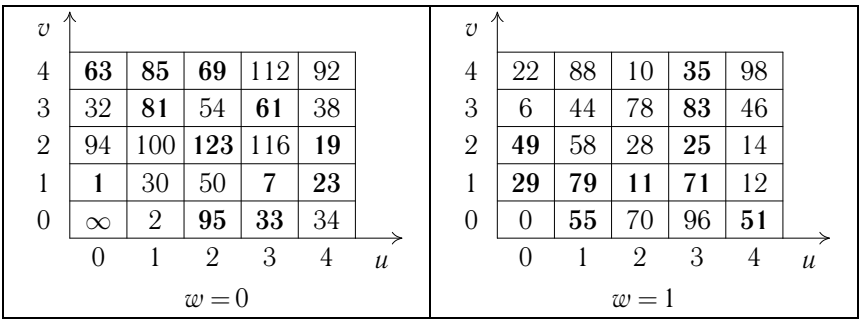
Таблица означает $3^3-2=25$ тождеств, включающих, например, тождества

$$A^0=1,\quad A^3=A^2+2,\quad A^4=A^2+2A+2,$$
$$A^5=2A+2,\quad A^6=2A^2+2A,\quad A^7=A^2+1,$$
$$A^8=A^2+A+2,\quad A^9=2A^2+2A+2,\quad \ldots$$
$$\ldots,\quad A^{24}=2A+1,\quad A^{25}=2A^2+A,\quad A^{26}=1.$$

Все эти тождества рекуррентно вытекают из второго из них.

Число производящих элементов A^k (где $1\leqslant k\leqslant 25$), есть $\varphi(3^3-1)=12$. Эти 12 значений показателя k выделены в таблице полужирным шрифтом.

Таблица поля из 5^3 элементов.



v	$u=0$	$u=1$	$u=2$	$u=3$	$u=4$
4	**63**	**85**	**69**	112	92
3	32	**81**	54	**61**	38
2	94	100	**123**	116	**19**
1	**1**	30	50	**7**	**23**
0	∞	2	**95**	**33**	34

$w=0$

v	$u=0$	$u=1$	$u=2$	$u=3$	$u=4$
4	22	88	10	**35**	98
3	6	44	78	**83**	46
2	**49**	58	28	**25**	14
1	**29**	**79**	**11**	**71**	12
0	0	**55**	70	96	**51**

$w=1$

Таблица поля из 5^3 элементов (продолжение).

$w=2$

v \ u	0	1	2	3	4
4	18	118	**27**	**107**	**121**
3	**115**	4	**57**	**67**	**103**
2	122	40	48	**105**	104
1	**99**	52	**13**	**15**	**47**
0	93	**65**	24	20	**39**

$w=3$

v \ u	0	1	2	3	4
4	**37**	**109**	**77**	**75**	114
3	60	42	**43**	110	102
2	**53**	**41**	**5**	**119**	66
1	80	**59**	**45**	**89**	56
0	31	**101**	82	86	**3**

$w=4$

v \ u	0	1	2	3	4
4	**91**	74	**9**	**73**	**17**
3	**111**	76	**87**	90	120
2	68	108	**21**	16	106
1	84	36	**97**	72	26
0	62	**113**	34	8	**117**

$$(A)=\begin{pmatrix}0&1&0\\0&0&1\\3&0&4\end{pmatrix}.$$

Например, эта таблица является краткой геометрической записью $5^3-2=$ $=123$ тождеств:

$$A^0=1,\quad A^3=4A^2+3,\quad A^4=A^2+3A+2,\quad A^5=2A^2+2A+3,$$
$$A^6=3A+1,\quad \ldots,\quad A^{63}=4A,\quad \ldots,\quad A^{114}=4A^2+4A+3,\quad \ldots$$
$$\ldots,\quad A^{123}=2A^2+2A,\quad A^{124}=1.$$

Все эти тождества рекуррентно вытекают из второго из них (определяемого последней строкой матрицы (A)).

Число производящих элементов A^k (где $1\leqslant k\leqslant 123$), равно $\varphi(5^3-1)=$ $=\varphi(31)\cdot\varphi(4)=60$. Эти 60 значений показателя k набраны полужирным шрифтом в таблице поля.

Для составления таблиц полей из p^4 элементов мы выберем в качестве базиса аддитивных образующих элементы $1, A, A^2, A^3$, где A — мультипликативная образующая.

Таблица поля заполняет показателями k $(\mathrm{mod}\,(p^4-1))$ степеней A^k мультипликативной образующей точки (u,v,w,t) конечного четырёхмерного куба (тора), $\mathbb{Z}_p^4$,

$$A^k=u_kA^3+v_kA^2+w_kA+t_k1.$$

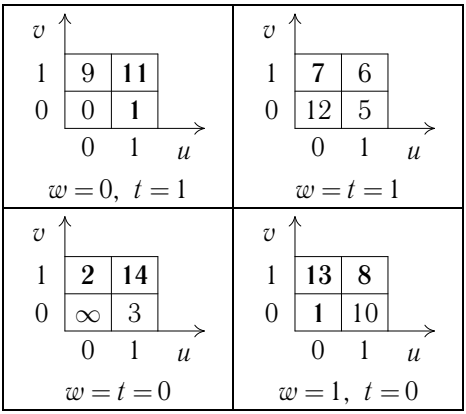
Чтобы изобразить четырёхмерный куб, ниже приведены заполнения его плоских сечений ($w = \text{const}$, $t = \text{const}$) соответствующими показателями k, (где $0 \leqslant k \leqslant p^4 - 2$).

Появление числа k в клеточке (u, v) квадрата с номером (w, t) в таблице поля означает тождество

$$A^k = uA^3 + vA^2 + wA + t1.$$

Эти таблицы квадратных плоских сечений конечного четырёхмерного куба (тора) приведены ниже для $p = 2$ и для $p = 3$.

Таблица поля из 2^4 элементов.



Эта таблица составлена для мультипликативной образующей, заданной матрицей представления

$$(A) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}.$$

Таблица является краткой геометрической записью $2^4 - 3 = 13$ тождеств,

$$A^0 = 1, \quad A^4 = A^3 + 1, \quad A^5 = A^3 + A + 1,$$
$$A^6 = A^3 + A^2 + A + 1, \quad \ldots, \quad A^{14} = A^3 + A^2, \quad A^{15} = 1.$$

Все эти тождества рекуррентно вытекают из второго из них (определяемого последней строкой матрицы (A)).

Число производящих элементов A^k (где $1 \leqslant k \leqslant 14$) равно $\varphi(2^4 - 1) = \varphi(3)\varphi(5) = 8$. Эти 12 значений показателя k выделены в таблице полужирным шрифтом.

Таблица поля из 3^4 элементов.

$w=0,\ t=2$

v \ u	0	1	2
2	18	20	36
1	65	**27**	50
0	40	44	**31**

$w=1,\ t=2$

v \ u	0	1	2
2	34	46	**7**
1	**23**	**73**	**13**
0	68	5	**61**

$w=2,\ t=2$

v \ u	0	1	2
2	16	52	15
1	8	62	14
0	**37**	32	**51**

$w=0,\ t=1$

v \ u	0	1	2
2	25	10	**67**
1	58	76	60
0	0	**71**	4

$w=1,\ t=1$

v \ u	0	1	2
2	48	54	22
1	56	55	12
0	**77**	**11**	72

$w=2,\ t=1$

v \ u	0	1	2
2	**63**	**53**	**33**
1	74	**47**	6
0	28	**21**	45

$w=0,\ t=1$

v \ u	0	1	2
2	42	70	**39**
1	2	**79**	30
0	∞	**3**	**43**

$w=1,\ t=1$

v \ u	0	1	2
2	**29**	75	64
1	78	**57**	**49**
0	**1**	**59**	26

$w=2,\ t=1$

v \ u	0	1	2
2	38	**9**	**17**
1	**69**	24	35
0	**41**	66	**19**

Эта таблица составлена при помощи мультипликативной образующей, заданной в матричном представлении поля матрицей

$$(A)=\begin{pmatrix}0&1&0&0\\0&0&1&0\\0&0&0&1\\1&0&0&2\end{pmatrix}.$$

Таблица поля из 81 элемента есть краткая геометрическая запись $78=3^4-3$ тождеств:

$$A^0=1,\quad A^4=2A^3+1,\quad A^5=A^3+A+2,\quad A^6=2A^3+A^2+2A+1,$$
$$A^7=2A^3+2A^2+A+2,\quad \ldots,\quad A^{79}=A^3+A^2,\quad A^{80}=1.$$

Все эти тождества рекуррентно вытекают из второго из них (определяемого последней строкой матрицы (A)): например,

$$A^5=AA^4=2A^4+A=2(2A^3+1)+A=A^3+2+A$$

(поскольку $2\cdot 2=1$ в $\mathbb{Z}_3$), и т. д.

Число производящих элементов A^k (где $1 \leqslant k \leqslant 79$), есть $\varphi(3^4-1) = \varphi(5)\cdot\varphi(16) = 32$. Эти 32 значения показателя k выделены в таблице полужирным шрифтом.

Таблицы полей из 2^5, 2^6 и 2^7 элементов приведены в книге

Лидл Р., *Нидеррайтер Г.* Конечные поля. В 2-х т. — М: Мир, 1998 (*Lidl R.*, *Niederreiter H.* Finite Fields. — Addison-Wesley, 1983). См. особенно с. 673–676 в т. 2.

Эта книга содержит также обширную (хотя и не полную) библиографию по теории конечных полей (и доказательства пропущенных в начале наших лекций теорем о существовании и единственности поля из p^n элементов и о цикличности его мультипликативной группы, т. е. об отсутствии других конечных полей).

Таблицы полей из 32, 64 и 128 элементов приведены в этой книге для мультипликативных образующих, заданных, в матричном представлении поля, следующими матрицами (соответственно):

$$(A) = \begin{pmatrix} 0&1&0&0&0\\ 0&0&1&0&0\\ 0&0&0&1&0\\ 0&0&0&0&1\\ 1&0&0&1&0 \end{pmatrix}, \quad \begin{pmatrix} 0&1&0&0&0&0\\ 0&0&1&0&0&0\\ 0&0&0&1&0&0\\ 0&0&0&0&1&0\\ 0&0&0&0&0&1\\ 1&0&0&0&0&1 \end{pmatrix}, \quad \begin{pmatrix} 0&1&0&0&0&0&0\\ 0&0&1&0&0&0&0\\ 0&0&0&1&0&0&0\\ 0&0&0&0&1&0&0\\ 0&0&0&0&0&1&0\\ 0&0&0&0&0&0&1\\ 1&1&0&0&0&0&0 \end{pmatrix},$$

так что, соответственно, выполняются тождества, выраженные последними строками этих матриц:

$$A^5 = A^3 + 1, \quad A^6 = A^5 + 1, \quad A^7 = A + 1.$$

К сожалению, явного вида столь удобных мультипликативных образующих (A) для поля из p^n элементов я не знаю, даже при $p = 2$ (вероятно, вследствие запутанности приведённой в цитированной книге библиографии). В книге указывается, впрочем, что самые полезные таблицы впервые появились в сочинении

Jacobi G. G. J. Canon Arithmeticus. — Berlin, 1839 (переиздание: Berlin: Akademic-Verlag, 1956).

В этой полезной библиографии, например, важный результат теории симметрических функций А. Жирара (опубликованный им в Амстердаме в книге 1629 года) приписан (без ссылок на их цитируемые в книге работы) Ньютону (1707) и Варингу.

Забытая теорема Жерара выражает моменты (т. е. суммы степеней $s_k = x_1^k + \ldots + x_n^k$) корней многочлена

$$\prod (x - x_j) = x^n - \sigma_1 x^{n-1} + \sigma_2 x^{n-2} - \ldots \pm \sigma_n$$

через коэффициенты (предвосхищая знаменитую теорему Шевалле).

Эти выражения являются, конечно, многочленами с целыми коэффициентами от переменных σ_j. Эти коэффициенты обладают рядом удивительных свойств, связывающих их и с естественными науками, и с теорией чисел (включая обобщение «малой теоремы» Ферма на следы матриц).

Асимптотическое поведение этих коэффициентов доставляет комбинаторное описание энтропии $\sum p_j \log p_j$ (описывающей статистику длинных слов в конечном алфавите в терминах частот p_j их букв).

Эти коэффициенты доставляют также удивительные обобщения странного модулярного или псевдодвоякопериодического p-адического поведения степеней $d(a,b)$ простого числа p в сравнениях

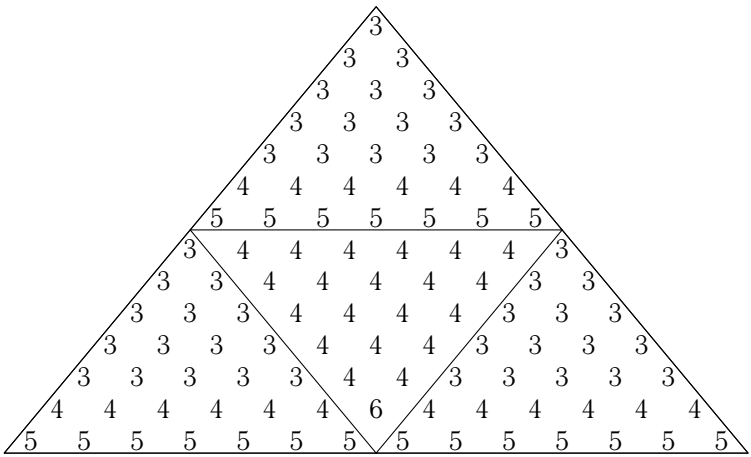
$$C_{pa}^{pb} - C_a^b = p^d q$$

(где q взаимно просто с p) для биномиальных коэффициентов и для их мультиномиальных обобщений.

Более подробное описание этих сравнений и странных периодичностей можно найти в книге: *Арнольд В. И.* Задачи семинара 2003–2004 г. М.: МЦНМО, 2005. — С. 12–17.

Например, $d(mp+1,b)$ не зависит от b, пока m не слишком велико, и величина $d(a,b)$ обладает своеобразной p-адической двоякой периодичностью по обоим аргументам a и b.

Чтобы уяснить себе природу этой функции d переменных a и b, полезно рассмотреть следующую таблицу её значений при $p=7$ (ниже приведено 14 строк расположенного как треугольник Паскаля набора значений, соответствующих значениям аргументов $2 \leqslant a \leqslant 15$ для этих четырнадцати строк, причем аргумент b меняется в каждой строке в пределах $0 < b < a$).



«Двойная периодичность» этой таблицы заключается лишь в *конечном* повторении «фундаментальной области» размера p, а именно, она повторяется p раз в каждом направлении, а затем слегка искажается. Образованный таким образом блок размера p^2 опять повторяется (по p раз в обоих направлениях), после чего опять искажается, образуя блок размера p^3.

Эта конструкция построения блоков все бóльших размеров продолжается до бесконечности. Но, несмотря на такую p-адическую «псевдопериодичность» и на появление величины p^n, ни точная p-адическая формула для этой «псевдопериодичности», ни её отношение к полям Галуа (из p^n элементов) не известны.

Малая теорема Ферма связана с неравенством $d \geqslant 2$ и с некоторым (нерегулярным) ростом $d(a, b)$ с a.

Матричная версия этой теоремы Ферма и её обобщения, открытого Эйлером:

$$a^m \equiv a^{m-\varphi(m)} \pmod{m},$$

представляет собой сравнение для следов целочисленных матриц,

$$\operatorname{tr}(A^m) \equiv \operatorname{tr}(A^{m-\varphi(m)}) \pmod{m},$$

где $m = p^n$.

Необходимость последнего ограничения для справедливости этого сравнения подсказывает возможность связи предмета с полями Галуа (но эти связи, насколько я знаю, еще не открыты).

К сожалению, все эти замечательные факты не удостоились внимания ни современных математиков, ни компьютерщиков. Численные эксперименты в этой области немедленно приводят к открытию поразительных законов природы.

Например, число делителей большого целого числа n растет в среднем как его натуральный логарифм, $\ln n$. Сумма делителей числа n растет в среднем как линейная функция cn, где постоянная c (найденная Эйлером) есть

$$c = \zeta(2) = \pi^2/6 \approx 3/2.$$

Средний делитель большого числа n в среднем растет, однако, как $c_1 n/(\sqrt{\ln n})$, а не как $cn/(\ln n)$ (последнее склонны были бы предполагать естествоиспытатели, ожидающие среднее значение дроби, равное отношению среднего значения числителя к среднему значению знаменателя).

Средняя асимптотика[1] $c_1 n/\sqrt{\ln n}$ для среднего делителя большого числа n была обнаружена А. Карацубой, причем постоянная c_1, по вычислениям М. Королева, есть $c_1 \approx 0{,}7138067\ldots$,

$$c_1 = \frac{1}{\pi}\prod_p \Big(\frac{p^{3/2}}{\sqrt{p-1}}\ln\Big(1+\frac{1}{p}\Big)\Big).$$

Этот результат был получен ими в связи с моим предшествующим докладом о чезаровских средних, вычисленных Дирихле.

Однако до сих пор не выяснены средние ни для числа делителей τ, ни для суммы делителей σ, ни для среднего делителя σ/τ чисел вида значений $\varphi(n)$ функции Эйлера. Между тем, минимальный период $T(n)$ геометрической прогрессии $(t = 1, 2, \ldots, T)$ остатков от деления на n является делителем числа $\varphi(n)$ по теореме Эйлера. Поэтому естественно было бы сравнить среднюю асимптотику периода $T(n)$ со средней асимптотикой чисел $\sigma(\varphi(n))/\tau(\varphi(n))$.

Эмпирически наблюдаемый средний рост периода $T(n)$ порядка $c(a)n/(\ln n)$ был обнаружен Ф. Айкарди (C. R. Ac.-SCI. Paris. Ser. I. Vol. 339 (2004). P. 15–20, "Empirical estimates of the average order of orbits period lengths in Euler groups"), где рассматривались большие значения $n < 10^9$.

Различие между средним поведением среднего от периода $T(n)$ и среднего поведения среднего делителя $\sigma(n)/\tau(n)$ может объясняться рядом причин, каждая из которых заслуживает и эмпирического, и теоретического исследования.

а) Поведение дробей $\sigma(\varphi(n))/\tau(\varphi(n))$ при случайном выборе числа n может сильно отличаться от поведения дробей $\sigma(m)/\tau(m)$ при случайном выборе числа $m = \varphi(n)$.

---

[1] Насколько я понимаю, здесь асимптотическая чезаровская средняя последовательности $a(n)$ определяется как обычная асимптотика для величины

$$\hat{a}(x) = \frac{1}{x}\sum_{n\leqslant x} a(n).$$

Это определение приводит к странному «среднему» $\hat{a}(n) = n/2$ для величины $a(n) = n$.

Я предпочитаю определять чезаровскую асимптотику величины a соотношением

$$\lim_{x\to\infty} \frac{\sum\limits_{n\leqslant x} a(n)}{\sum\limits_{n\leqslant x} b(n)} = 1.$$

При этом (физически более естественном) определении, которым я пользовался выше при описании поведения функций τ и σ, постоянная c_1 в асимптотике для σ/τ будет другой, чем указали Карацуба и Королев.

Уже Эйлер установил, что в среднем $\varphi(n) \sim (6/\pi^2)n$.

b) Делитель $T(n)$ числа $\varphi(n)$ (при случайном выборе числа n) может вести себя не так, как средний делитель $\sigma(\varphi(n))/\tau(\varphi(n))$ этого числа: период $T(n)$ является одним из делителей числа $\varphi(n)$, но делителей много, и природа может предпочесть не средний, а экзотический выбор.

c) Среднее значение дроби $\sigma(m)/\tau(m)$ может сильно отличаться от отношения средних значений числителя и знаменателя, прежде всего вследствие малоизученных корреляций между отклонениями величин σ и τ от своих средних (что аналогично известным в теории турбулентности явлениям перемежаемости).

Имеет ли место такая теоретико-числовая перемежаемость — вопрос, интересный и сам по себе, вне связи с поведением периода $T(n)$.

Ни имя Жерара, ни его теорема не упомянуты даже в знаменитой книге «Concrete Mathematics», авторы которой хотели объединить *непрерывную* математику (откуда часть «con» слова «concrete») с *дискретной* («discrete», откуда часть слова «crete») и с железобетонной («concrete»).

Рассматривая единство математики как её главное сокровище, я надеюсь способствовать (при помощи геометрического изложения теории полей Галуа и её взаимоотношений с эргодической теорией динамических систем, со статистикой хаотических процессов и с проективной геометрией) возвращению всех этих забытых классических теорий к реальному ($\mathbb{R}$) миру естественных наук.