Math-Net.Ru

Общероссийский математический портал

В. И. Арнольд, Топология и статистика формул арифметики, *УМН*, 2003, том 58, выпуск 4, 3–28

DOI: <https://doi.org/10.4213/rm641>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением

<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 107.22.136.117

26 апреля 2023 г., 16:27:24

УДК 51

ТОПОЛОГИЯ И СТАТИСТИКА ФОРМУЛ АРИФМЕТИКИ

В. И. Арнольд

В статье дан обзор недавних и классических исследований геометрических прогрессий вычетов, обобщающих малую теорему Ферма и связывающих эту область с теорией динамических систем и оценивающих степень хаотичности образующих геометрическую прогрессию систем вычетов, обнаруживающих своеобразное расталкивание.

В качестве вспомогательного средства изучаются графы операций возведения в квадрат элементов конечных групп и колец. Для коммутативных групп связанные компоненты этих графов оказываются циклами-аттракторами, однородно оснащенными произведениями бинарных корневых деревьев, алгебра которых также описана в статье. Оснащение деревьями оказывается однородным и для графов симметрических групп перестановок, а также для групп четных перестановок.

Библиография: 6 названий.

СОДЕРЖАНИЕ

§ 1. Динамическая система Ферма—Эйлера	4
§ 2. Случайны ли вычеты элементов геометрической прогрессии?	7
§ 3. Топология операции возведения в квадрат	10
§ 4. Алгебра корневых деревьев	11
§ 5. Графы возведения в квадрат в группах перестановок	13
§ 6. Однородность монад всех конечных групп	16
§ 7. Модулярная топология кубов Кеплера	18
§ 8. Кеплеровы кубы и подгруппы Гамильтона	21
§ 9. Риманова поверхность семиугольников и ее кубы Кеплера	24
§ 10. Статистика периодов Ферма—Эйлера	28
Список литературы	28

Объектами топологии могут быть не только кривые и поверхности, но также формулы и теории.

Занимаясь последнее время арифметикой квадратичных форм (и ее связями с релятивистским миром де Ситтера), я обнаружил топологическую природу большого ряда явлений теории чисел с одной стороны и странные статистические свойства ее простейших объектов с другой.

Хотя и эти статистические свойства, и топологические явления во многих случаях остаются не теоремами, а экспериментальными фактами (подтвержденными всего

лишь несколькими миллионами наблюдений), я решаюсь рассказать здесь о некоторых из них, тем более что небольшую долю этих фактов уже удалось сформулировать и доказать в виде математических теорем (см. [1]–[5]).

§ 1. Динамическая система Ферма–Эйлера

Простейшим топологическим по существу примером геометрии формул является “малая теорема Ферма”, обобщенная Эйлером и описывающая теоретико-числовые свойства геометрических прогрессий, приведенных по модулю n , вроде периодической последовательности остатков от деления на 13 степеней двойки,

$$\{1, 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1, 2, \dots\}$$

(для $n = 13$). Наблюдение Ферма состоит в том, что такая последовательность $\{a^t \pmod n\}$ всегда периодична (он рассматривал случай простого числа n , а на общий случай его теорему распространил Эйлер, у которого основание a и модуль n лишь взаимно просты).

Примером нерешенной статистической задачи эргодической теории чисел, возникающей уже в этом простом примере, является вопрос об асимптотическом поведении при больших n странно нерегулярной величины периода $T(n)$ геометрической прогрессии вычетов по модулю n (например, последовательности $\{2^t \pmod n$, $t = 0, 1, 2, \dots\}$, если n – нечетное число), хотя бы в смысле слабой асимптотики, введенной в [6].

Наблюдения показывают *в среднем линейный* рост периода (хотя отклонения в обе стороны довольно велики, встречаются они относительно редко):

n	5	7	9	13	15	19	29	31	51	71	509	511
T	4	3	6	12	4	18	28	5	8	35	508	9

Более регулярно ведут себя средние (хотя бы по небольшому отрезку изменения модуля n) значения. Например, суммы последовательных десятков нечетных чисел $1 \leq n \leq 19$, $21 \leq n \leq 39$ и т. д. и соответствующих им десятков значений периодов T таковы:

$\sum n$	100	300	500	700	900
$\sum T$	68	158	246	299	329

Суммы всех периодов для нечетных модулей $1 \leq k \leq n$, по вычислениям Ф. Аикарди, ведут себя так:

n	9	109	509	1009	1509	2009
$\sum T$	15	1409	23607	82761	176016	302277

Эти числа, исследованные при помощи двойной логарифмической шкалы (подобной использованной А. Н. Колмогоровым для открытия показателей своих законов турбулентности), в среднем соответствуют скорее эмпирической формуле вида

$$T \approx 1.4n^{4/5}$$

(приводящей к росту сумм как $n^{9/5}$). Но никаких теорем об асимптотике здесь пока не доказано, и не исключены даже возможности $T \approx Cn$ или $T \approx Cn/\log n$.

“Топологическим” аспектом малой теоремы Ферма является следующая ее переформулировка, принадлежащая в основном Эйлеру (обсуждение см. в [1]).

Рассмотрим мультипликативную группу вычетов по модулю n , взаимно простых с n (я называю ее *группой Эйлера* и обозначаю ее через $\Gamma(n)$).

Если $n = p$ – простое число, то в группу Эйлера входят все $p - 1$ ненулевых вычетов. В общем случае число $\varphi(n)$ элементов группы Эйлера меняется с n довольно сложным образом:

n	1	2	3	4	5	6	7	8	9	10	11	12
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4	10	4

Функцию φ Гаусс назвал *функцией Эйлера*. Если (разные) простые множители модуля n равны p_k , а их кратности равны a_k , то значение функции Эйлера $\varphi(n)$ есть

$$\varphi\left(\prod p_k^{a_k}\right) = \prod [(p_k - 1)p_k^{a_k - 1}].$$

Умножение всех вычетов из $\Gamma(n)$ на один из них (например на 2, если n нечетно) задает перестановку $(2*)$ конечного множества $\Gamma(n)$, состоящего из $\varphi(n)$ элементов (из всех взаимно простых с n вычетов).

Наблюдение Эйлера (эквивалентное теореме Эйлера–Ферма, обычно формулируемой иначе) таково:

ТЕОРЕМА ЭЙЛЕРА. *Диаграмма Юнга перестановки “умножение на фиксированный элемент a из группы $\Gamma(n)$ ” является прямоугольником, т.е. все циклы этой перестановки имеют одинаковую длину $T(n)$.*

Обозначим через $N(n)$ число этих циклов, т.е. число орбит динамической системы “умножение на a ”

$$(a*): \Gamma(n) \rightarrow \Gamma(n)$$

(для определенности ниже выбрано $a = 2$ и n нечетно).

Тогда площадь всей диаграммы Юнга перестановки $(a*)$ есть значение функции Эйлера,

$$\varphi(n) = T(n)N(n),$$

так что T и число орбит N являются делителями значения функции Эйлера.

ПРИМЕР. При $n = 31, a = 2$ имеем

$$\varphi(n) = 30, \quad T(n) = 5, \quad N(n) = 6.$$

Диаграмма Юнга (заполненная элементами циклов перестановки “умножение на 2”) имеет следующий вид (mod 31):

1	2	4	8	16
3	6	12	24	17
5	10	20	9	18
7	14	28	25	19
11	22	13	26	21
15	30	29	27	23

$$16 \cdot 2 \equiv 1 \pmod{31}, \quad T(31) = 5$$

$$N(31) = 6.$$

Вот несколько примеров значений периода T и числа орбит N операции умножения вычетов на 2 для разных значений модуля n (ср. [2]):

n	37	65	129	229	381	509	511
T	36	12	14	76	14	508	9
N	1	4	6	3	18	1	48

Произведение $\varphi(n) = T(n)N(n)$ растет в среднем как cn , где $c = 6/\pi^2$, а именно, доказано (Б. А. Венковым), что

$$\lim_{n \rightarrow \infty} \frac{\sum_{k=1}^n \varphi(k)}{\sum_{k=1}^n k} = c = \frac{1}{\zeta(2)}.$$

Коэффициент c появляется здесь как вероятность несократимости дроби p/q (точно так же, $1/\zeta(m)$ – вероятность отсутствия целых точек на отрезке от 0 до целочисленного вектора m -мерного пространства).

Что эта вероятность (в случае плоскости) есть $1/\zeta(2)$, следует из формулы Эйлера,

$$\prod_p \frac{1}{1 - 1/p^m} = \sum_{n=1}^{\infty} \frac{1}{n^m}$$

(произведение по всем простым), для того Эйлером и придуманной (см. подробности в [1]).

Что $\zeta(2) = \pi^2/6 (\approx 3/2)$, как открыл тоже Эйлер, следует из теории рядов Фурье (нужно разложить в ряд Фурье 2π -периодическую функцию, совпадающую с $|x|$ на отрезке $|x| \leq \pi$).

Интересно отметить, что, согласно [1], эмпирический средний рост числа орбит $N(n)$ примерно такой же, как если бы число орбит N росло как

$$N \approx 0.67n^{2/5}$$

(это – “слабая асимптотика” в смысле статьи [6]).

Тот факт, что сумма $2/5 + 4/5$ показателей эмпирических средних асимптотик для N и для T больше показателя 1 средней асимптотики для функции Эйлера φ , не противоречит формуле Эйлера $\varphi = NT$, так как произведение средних – вовсе не то же, что среднее значение произведения. Напротив того, это расхождение является своеобразным указанием на частое чередование больших отклонений сомножителей от средних в ту и другую сторону (подобное явлению перемежаемости в теории турбулентности и в гидродинамике).

Хотя имеющиеся наблюдения дают даже некоторые эмпирические средние “асимптотики” для этой теоретико-числовой перемежаемости, никакие теоремы на этот счет еще не доказаны.

Эмпирические формулы для средних частот p_N встречаемости значений $N = 1, 2, 4, 8$ и $N \geq 10$ в окрестности фиксированного значения n (между 1 и 2000) имеют, согласно статье [1], вид степенных слабых асимптотик

$$p_1 \sim an^{-7/18}, \quad p_2 \sim bn^{-1/9}, \quad p_4 \sim cn^{1/3}, \quad p_8 \sim dn^{1/9}, \quad p_{\geq 10} \sim en.$$

Однако никаких оснований для рациональности этих показателей степени (подобной рациональности показателей Колмогорова в теории турбулентности и предшествовавших им аналогичных гидродинамических показателей Леонардо да Винчи) не видно.

Значения $T(n)$ и $N(n)$ для нечетных $n = 2k + 1$, $k = 1, \dots, 1000$, были вычислены Ф. Аикарди. Ее результаты показаны в билогарифмической шкале ниже в разделе 10; аналогичным методом А. Н. Колмогоров нашел свой закон $5/3$ в теории турбулентности (его график тоже показан ниже в разделе 10).

Прямая Аикарди указывает на эмпирические слабые (усредненные) асимптотики

$$T(n) \sim 0.94 n^{0.834}, \quad N(n) \sim 0.60 n^{0.36}, \quad \varphi(n) \sim cn^a,$$

где для n от 1 до 10^5 константы приближенно равны $a = 0.9994$, $c = 0.612$, тогда как $6/\pi^2 \approx 0.6079$.

В действительности для сглаживающего усреднения использовались графики в билогарифмическом масштабе величин $(\Sigma T)(n) = \sum_{k=1}^n T(k)$ и $(\Sigma N)(n) = \sum_{k=1}^n N(k)$, где k нечетны. Почти прямолинейные билогарифмические графики соответствуют степенным функциям

$$(\Sigma T)(n) \sim 0.255 n^{1.834}, \quad (\Sigma N) \sim 0.223 n^{1.36}.$$

§ 2. Случайны ли вычеты элементов геометрической прогрессии?

Здесь описаны “критерии стохастичности”, разработанные для того, чтобы распознавать степень случайности последовательности.

Показатель Ляпунова операции умножения вычетов на 2 указывает на довольно быстрый рост возмущений в динамической системе Ферма–Эйлера. Это позволяет ожидать хаотического распределения этих вычетов (среди всех n вычетов из $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ или хотя бы среди $\varphi(n)$ взаимно простых с n вычетов из группы Эйлера $\Gamma(n)$).

Однако наблюдаемая статистика периодов $T(n)$ указывает на *неполную хаотичность* элементов орбиты из $T(n)$ вычетов, а именно, наблюдается некоторое *взаимное отталкивание* вычетов элементов геометрической прогрессии.

Дело в том, что все $T(n)$ вычетов элементов $\{2^t \ (t = 1, 2, \dots, T)\}$ по модулю n в пределах одного периода различны, так как первое же повторение какого-либо вычета привело бы к повторению и всех следующих за ним.

Если бы вычеты членов изучаемой орбиты из T элементов были бы независимыми случайными элементами множества из m элементов ($m = n$ в случае распределения вычетов в $\mathbb{Z}_n$, $m = \varphi(n)$ в случае изучения распределения вычетов в группе Эйлера $\Gamma(n)$), то знаменитая “задача о днях рождения” из теории вероятностей подсказывала бы для $T(n)$ гораздо меньшее, чем n , значение (порядка $\sqrt{n}$).

А именно, вероятность отсутствия совпадений в выборке из T элементов m -элементного множества мала, пока T “невелико”, и близка к 1, когда T “велико”, причем переход совершается вблизи специального критического значения, $T_* \sim \sqrt{2m}$.

Ибо число T -элементных последовательных выборок из m элементов есть $m(m-1) \cdots (m-T+1)$, а число всех таких выборок (возможно, с повторениями) есть m^T , так что вероятность отсутствия повторений есть

$$p(T, m) = \prod_{k=0}^{T-1} \frac{m-k}{m} \sim e^{\sum \ln(1-k/m)} \sim e^{-\sum k/m} \sim e^{-T^2/2m}.$$

Хотя показатель степенной асимптотики зависимости периода T от модуля n не известен даже в смысле сглаженных средних и слабых асимптотик, эмпирические данные статей [1]–[3] подсказывают, что этот показатель если и не равен 1, то, во всяком случае, ближе к 1, чем к показателю $1/2$, который должен бы был наблюдаться, если бы элементы орбиты были независимыми случайными вычетами.

Таким образом, наблюдаемый период геометрической прогрессии больше периода, соответствующего случайному выбору элементов орбиты. То есть вычеты членов прогрессии избегают близких сближений и в этом смысле расталкиваются.

Для измерения этого расталкивания я сосчитал среднее расстояние между соседними точками на окружности длины L из заданного T -точечного множества, определяя это среднее следующим образом (введенным в статье [1]).

Если длины дуг, на которые точки множества делят окружность, равны x_i , $i = 1, \dots, T$ (так что $\sum x_i = L$), то составим прежде всего сумму квадратов этих длин,

$$R = \sum x_i^2.$$

Чтобы избавиться от (размерной) длины окружности L , рассмотрим в качестве “меры стохастичности” множества из T элементов нормализованную сумму квадратов расстояний между соседями,

$$r = R/L^2$$

(это деление на L^2 эквивалентно нормализующему сжатию окружности длины L до окружности длины 1).

Наименьшее значение “меры стохастичности” r , равное $1/T$, достигается на казарменном строе арифметической прогрессии равноудаленных точек (делящих окружность на T дуг длиной $1/T$ каждая).

Наибольшее значение $r = 1$ достигается на кластерном распределении полной скупченности (все дуги, кроме одной, длины 0).

Все это удобно представлять себе, интерпретируя r как квадрат расстояния от нуля до точки $z = x/L$ $(T - 1)$ -мерного симплекса $0 \leq z_i \leq 1$, $\sum z_i = 1$ в T -мерном евклидовом пространстве.

Минимум расстояния до нуля достигается в центре симплекса, а максимум – в вершинах.

Случайному выбору точек множества на окружности соответствует случайное распределение точки z в симплексе (равномерно по мере Лебега распределенной в нем). Значение “меры стохастичности” r для такого свободолюбивого распределения точек на окружности легко вычислить явно: оно промежуточно между казарменным минимальным значением (для сильно расталкивающихся частиц) и кластерным максимальным значением (достигающимся для скучившихся в одно место частиц).

Чтобы сравнивать множества с разными числами точек, T , я разделил значение показателя r на его минимальное при данном числе точек значение и определил *дважды (по L и по T) нормализованный параметр стохастичности*

$$s = r/r_{\min} = Tr.$$

Казарменное (минимальное) и кластерное (максимальное) значения этого нового параметра суть

$$(s_{\min} = 1) \leq s \leq (s_{\max} = T).$$

Вычисления показывают, что свободолюбивое значение этого параметра стохастичности близко к двойке: оно равно (см. [1])

$$s_* = 2T/(T + 1).$$

Меньшие свободолюбивого значения параметра стохастичности ($1 \leq s < s_*$) указывают на расталкивание частиц множества (тем более сильное, чем меньше s), а большие значения ($s_* < s \leq 1/T$) – на их взаимное притяжение.

Для вычетов геометрических прогрессий явные вычисления [1], [3] значений параметра стохастичности s (проведенные Ф. Аикарди с помощью компьютера) дали в большинстве случаев значения дважды нормализованного параметра стохастичности s порядка 1.5 (причем изредка встречаются и близкие к 1 значения, и сильно большие 2). Однако никаких теорем здесь нет – это всего лишь результаты тысяч экспериментов.

Я проделал аналогичные вычисления и для других множеств, например, для распределения вычетов первых сотен простых чисел и для арифметических прогрессий вычетов (см. [1]).

В обоих случаях также обнаружилось расталкивание (значения параметра s , меньшие свободолюбивого). При этом для арифметической прогрессии результат сильно зависит от того, какой длины T отрезок прогрессии рассматривается. И для средних значений по параметру T , и для оптимальных выборов T , зависящих от подводящих дробей величины a/n , можно предполагать возможность получить (различные в этих двух случаях) асимптотики параметра стохастичности последовательности $\{at + b \bmod n\}$, $1 \leq t \leq T$, в терминах цепной дроби для a/n (с возможным усреднением по теореме Гаусса–Кузьмина об эргодических характеристиках элементов цепных дробей). Речь идет здесь, разумеется, прежде всего о слабых асимптотиках.

Расталкивание вычетов членов геометрической прогрессии сказывается и на распределении длин дуг целочисленной окружности $\mathbb{Z}_n$ (или группы Эйлера $\Gamma(n)$) между

этим вычетами. Частоты встречаемости дуг различных длин дуг k (от максимальной длины $m - (T - 1)$ до минимальной длины дуги 1 на целочисленной окружности длины m , разделенной на T целочисленных дуг случайно независимо выбранными T различными точками) относятся друг к другу как числа треугольника Паскаля, лежащие на прямой, параллельной его стороне и отстоящей от нее на расстояние $T - 2$:

$$p_k = C_{m-1-k}^{T-2} / C_{m-1}^{T-1}.$$

Например, для выбора четырех точек ($T = 4$) из восьми ($m = 8$) частоты дуг длин 1, 2, 3, 4 и 5 относятся как $15 : 10 : 6 : 3 : 1$ (т.е. дуги длины 4 встречаются в пять раз реже, чем дуги длины 1).

Рассмотрим геометрическую прогрессию $\{2^t \bmod 15\}$ как четырехточечное подмножество $\{1, 2, 4, 8\}$ восьмиточечной окружности вычетов, $\Gamma(15) = \{1, 2, 4, 7, 8, 11, 13, 14\}$ (с расстоянием 1 между последовательными выписанными числами и между 14 и 1). “Расстояния” между соседними точками прогрессии вдоль¹ группы Эйлера $\Gamma(15)$ составляют $\{1, 1, 2, 4\}$, т.е. дуга длины единица встречается в $2\frac{1}{2}$ раза реже, чем для случайных точек, что еще раз подтверждает расталкивание вычетов членов геометрической прогрессии.

При этом дважды нормализованный показатель стохастичности равен

$$s = \frac{1 + 1 + 4 + 16}{8^2} \cdot 4 = \frac{22}{16} = 1.375,$$

что существенно меньше, чем его свободолюбивое значение $2T/(T+1) = 1.6$, и также указывает на расталкивание вычетов членов прогрессии друг другом.

§3. Топология операции возведения в квадрат

Начнем с совершенно абстрактного и скорее логического объекта.

ОПРЕДЕЛЕНИЕ. *Монадой* называется отображение конечного множества в себя. *Графом монады* называется ориентированный граф, вершинами которого являются точки этого конечного множества, а ребра соединяют каждую точку графа с ее образом при отображении.

Иными словами, граф монады – это *произвольный конечный граф*, из каждой вершины которого выходит ровно одно ребро.

Геометрические прогрессии вычетов $\{2^t \bmod n\}$, рассматривавшиеся выше, связаны с такими “Фробениусовыми монадами”: каждый элемент конечной группы (или кольца) переводится в свой квадрат, $x \mapsto x^2$. Показатели степени получаемых при итерациях этой монады степеней элемента x образуют геометрическую прогрессию.

ПРИМЕР. Граф возведения в квадрат в кольце вычетов $\mathbb{Z}_7$ имеет три компоненты связности:

Например, $4^2 \equiv 2 \pmod{7}$, $5^2 \equiv 4 \pmod{7}$.

¹Расстоянием между двумя элементами вдоль группы Γ называется здесь число свободных от элементов группы дуг между двумя заданными вычетами.

ТЕОРЕМА 1. *Связные компоненты любой монады представляют собой циклы-аттракторы, оснащенные корневыми деревьями, присоединенными своими корнями к каждой вершине цикла-аттрактора.*

Длина цикла может быть и единицей, как для компонент $\{1, 6\}$ и $\{0\}$ в примере выше.

Рассмотрим теперь в качестве монады операцию возведения в квадрат элементов конечной коммутативной группы (при логарифмировании которой получается монада $x \mapsto 2x$, порождающая геометрическую прогрессию $\{2^t, t = 0, 1, 2, \dots\}$).

ТЕОРЕМА 2. *Каждая компонента связности графа операции возведения в квадрат элементов конечной коммутативной группы представляет собой цикл, оснащенный однородно (в каждой своей вершине одинаковым деревом).*

Это оснащающее дерево имеет (считая корень, принадлежащий циклу-аттрактору) 2^k вершин и представляет собой произведение бинарных деревьев в смысле определения произведения, данного ниже.

Бинарное дерево T_{2^n} из 2^n вершин состоит из корня и n этажей, причем в каждую вершину i -го этажа ведут ровно два ребра (из двух вершин $(i + 1)$ -го этажа) при $i = 1, 2, \dots, n - 1$.

В корень дерева T_{2^n} , который можно считать вершиной нулевого этажа, тоже ведут 2 ребра: из него самого и из (единственной) вершины первого этажа.

ПРИМЕР. Монада удвоений, $x \mapsto 2x$, в группе $\mathbb{Z}_4$ имеет своим графом бинарное дерево T_4 .

§ 4. Алгебра корневых деревьев

Умножение монад определяется как покомпонентное действие обеих операций на прямом произведении множеств вершин графов этих монад: монада-произведение, $X * Y$, действует на точку x, y прямого произведения множества вершин графа X и множества вершин графа Y по правилу

$$(X * Y)(x, y) = (Xx, Yy).$$

ПРИМЕР. Умножим n -вершинный цикл O_n на простейший бинарный граф $T_2 = A_1$ (A_1 — это, например, нарисованная выше компонента $\{1, 6\}$ графа возведения в квадрат в кольце $\mathbb{Z}_7$). Произведение $A_n = O_n * A_1$ представляет собой $2n$ -вершинный граф с циклом-аттрактором O_n , однородно оснащенный однореберными корневыми деревьями в каждой своей вершине, подобно третьей компоненте $A_2 = O_2 * A_1 = \{2, 3, 4, 5\}$ нарисованного выше графа возведения в квадрат в кольце вычетов $\mathbb{Z}_7$.

Корневые деревья являются связными графами монад (с единственным циклом длины один).

Граф произведения таких монад сам является корневым деревом. Граф (дерево) произведения монад мы будем называть *произведением графов* (деревьев) перемножаемых монад.

ПРИМЕР. Граф $A_1 * A_1 = D_1$ — это четырехвершинное корневое дерево, в корень которого входят ровно три ребра (из остальных трех вершин). Это граф группы $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Граф $D_n = O_n * D_1$ имеет $4n$ вершин и один цикл-аттрактор, в каждую вершину которого со стороны приходят три ребра (образующие вместе оснащающее эту вершину дерево D_1).

При исследовании произведений корневых деревьев полезно сопоставлять дереву следующий набор “*рангов*”: через r_i будем обозначать число вершин, путь от которых до корня состоит из i ребер и имеет длину i (в частности, $r_0 = 1$, $r_1(D_1) = 3$, $r_1(T_4) = 1$, $r_2(T_4) = 2$).

При перемножении графов ранги ведут себя так:

$$r_k(X * Y) = \sum r_i(X)r_j(Y),$$

где $\max(i, j) = k$. Иными словами, суммы $s_k = r_0 + r_1 + \dots + r_k$ удовлетворяют тождеству $s_k(X * Y) = s_k(X)s_k(Y)$.

Это означает, что для вычисления рангов дерева-произведения нужно составить матрицу произведений рангов деревьев-сомножителей и сосчитать суммы ее элементов в окаймляющих вершину $i = j = 0$ углах.

Например, для произведения бинарных деревьев T_4 и T_8 матрица произведений рангов имеет вид (уголки отмечены)

$$\left(\begin{array}{c|c|c|c} 2 & 2 & 4 & 8 \\ \hline 1 & 1 & 2 & 4 \\ \hline 1 & 1 & 2 & 4 \end{array} \right),$$

поэтому ранги произведения равны

$$r_0 = 1, \quad r_1 = 3, \quad r_2 = 12, \quad r_3 = 16.$$

Точно так же, ранги произведения бинарного дерева на себя, $T_{2^n} * T_{2^n}$, равны $\{1, 3, 3 \cdot 4, 3 \cdot 16, \dots, 3 \cdot 4^{n-1}\}$ (при замене второго бинарного дерева бóльшим последовательность рангов продолжается степенями двойки).

Я так подробно описываю произведения бинарных деревьев потому, что *только они встречаются (в качестве однородно оснащающих циклы деревьев) при описании графов конечных коммутативных групп*.

Это вытекает из того, что такая группа является прямым произведением циклических групп, а *граф операции умножения на 2, т.е. сложения элемента с самим собой, в (аддитивно записанной) циклической группе нечетного порядка разбивается на неоснащенные циклы*.

Действительно, из теоремы Эйлера следует, что $2^{\varphi(n)} \equiv 1 \pmod{n}$ для любого нечетного числа n . Поэтому $2^{\varphi(n)}a \equiv a \pmod{n}$, и следовательно каждый элемент a принадлежит циклу монады циклической группы $\mathbb{Z}_n$.

Таблица умножения этих циклов такова:

$$O_m * O_n = dO_c,$$

где d – наибольший общий делитель, а c – наименьшее общее кратное чисел m и n (имеется в виду непересекающееся объединение d циклов одинаковой длины c).

Например, имеют место тождества в алгебре графов

$$O_3 * O_5 = O_{30}, \quad O_6 * O_{10} = 2O_{30}.$$

Граф операции сложения элементов с собой в аддитивной циклической группе порядка 2^n оказывается бинарным деревом T_{2^n} :

Описанная выше алгебра графов позволяет быстро исследовать и более сложные случаи. Например, в содержащей 100 элементов группе Эйлера $\Gamma(125) \approx \mathbb{Z}_{100}$ самая большая компонента связности графа операции возведения в квадрат (очень полезная для анализа квадратичных вычетов по модулю 125) имеет вид $O_{20} * T_4$ и 80 вершин (см. рисунок на следующей странице).

Стрелки этого графа ведут к квадратичным вычетам по модулю 125 (например, $13^2 \equiv 44 \pmod{125}$), а стоящие вдали от цикла вершины оснащающих его деревьев $(22, 37, \dots)$ – квадратичные невычеты (сравнение $x^2 \equiv 2 \pmod{125}$ неразрешимо).

Именно топология подобных графов объясняет такие факты теории квадратичных форм, как, например, строение полугрупп значений “совершенных” квадратичных форм статьи [5] (вроде формы $x^2 + 2y^2$). В этом последнем примере нечетные значения формы образуют полугруппу чисел вида произведения

$$\prod p_i^{a_i} q_j^{b_j} r_k^{2c_k} s_l^{2d_l},$$

где p_i, q_j, r_k и s_l – различные нечетные простые множители, дающие при делении на 8 в остатке 1, 3, 5 и 7 соответственно. Множители r и s (равные 5 и 7 mod 8) должны входить в четных степенях.

Например, числа 5, 7, 125 и 343 все непредставимы, а числа 3, 17, 25 и 49 – представимы в виде $x^2 + 2y^2$ с целыми x и y (как $17 = 3^2 + 2 \cdot 2^2$).

§ 5. Графы возведения в квадрат в группах перестановок

При попытке перенести теорему об однородности оснащения цикла монады деревьев с коммутативных на произвольные конечные группы я обнаружил следующий факт.

ТЕОРЕМА 3. *Любая связная компонента графа операции возведения в квадрат в симметрической группе перестановок n элементов (или же в ее подгруппе четных перестановок) оснащена однородно (т.е. оснащающие деревья всех вершин цикла компоненты изоморфны друг другу).*

Этот результат об однородности оснащения выводится из такого описания элементов цикла-аттрактора для графа группы перестановок: аттрактор состоит из перестановок, все циклы которых имеют нечетные длины.

Но *циклическая перестановка нечетной длины сопряжена своему квадрату*. Это сопряжение не только переводит в соседнюю одну из вершин цикла-аттрактора, но действует и на оснащающие этот цикл деревья, также переставляя их, поэтому все оснащающие одну компоненту дерева и изоморфны.

В группе четных перестановок квадрат перестановки с циклом $(1, 2, 3)$ уже не сопряжен исходной перестановке в группе четных перестановок трех элементов, так как сопрягающая перестановка $(2, 3)$ нечетна.

Но подобное “сопряжение” нечетной перестановкой все же определяет (внешний) автоморфизм, сдвигающий вершину цикла-аттрактора на соседнее место и переводящий оснащающее ее дерево в соседнее оснащающее дерево, так что оснащение цикла компоненты оказывается однородным и для графа операции возведения в квадрат элементов группы четных перестановок.

Однородность оснащения сохраняется и для всех конечных групп.

Я не знаю, насколько алгебраическая перекошенность косога произведения групп $1 \rightarrow H \rightarrow E \rightarrow G \rightarrow 1$ сказывается на топологической перекошенности графа группы-“произведения” E по сравнению с произведением графов групп-“сомножителей” G и H (даже для случая двулистных накрытий, когда $H = \mathbb{Z}_2$, или подгрупп H ин-

декса 2, когда $G = \mathbb{Z}_2$).

Группа $SL(2, \mathbb{Z}_6)$ состоит из 144 матриц $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, элементы которых – вычеты по модулю 6, для которых $ad - bc \equiv 1 \pmod{6}$.

Граф возведения в квадрат состоит из 14 компонент:

$$[\text{граф}(SL(2, \mathbb{Z}_6))] = T + (O_2 * R) + 4(O_2 * E_8) + 8A_2,$$

где дерево T имеет суммы рангов $s = (1, 8, 32)$, а дерево R – суммы рангов $s = (1, 2, 8)$.

Явно 16 матриц, составляющих граф $O_2 * R$, таковы:

В этой компоненте однородность оснащения цикла деревьями объясняется (внешним) автоморфизмом, сопрягающим каждую матрицу при помощи меняющего ориентацию отображения плоскости, переставляющего оси координат и преобразующего матрицу $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ в $\begin{pmatrix} d & c \\ b & a \end{pmatrix}$.

Числа матриц с различными следами $a + d$ в каждой компоненте таковы:

$a + d$	T	$O_2 * R$	$4(O_2 * E_8)$	$8A_2$
0	24	0	0	0
1	0	2	0	$8 \cdot 2$
2	$3 + 1$	0	$3 \cdot (6 + 2) + 6$	0
3	0	12	0	0
4	$3 + 1$	0	$3 \cdot 8 + (8 + 2)$	0
5	0	2	0	$8 \cdot 2$

Обозначения в роде $3 + 1$ в графе $(2, T)$ обозначает, что 4 точки графа T , в которых $a + d \equiv 2$, подразделяются на два класса, один из 3 элементов, а другой из 1 элемента, которые занимают в дереве T неизоморфные места (в рассматриваемом примере эти матрицы

$$\left\{ \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix}, \begin{pmatrix} 4 & 3 \\ 3 & 4 \end{pmatrix} \right\} \text{ и } \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

удалены от корня на расстояния 1 и 0).

Было бы интересно связать эти структуры графов монадгрупп с действиями на эти группы обычных и внутренних автоморфизмов, а также включающих их монадоморфизмов: образуют ли автоморфизмы или внутренние автоморфизмы нормальные делители в группах монадоморфизмов (и каковы фактор-группы в случае положительного ответа?)

§6. Однородность монад всех конечных групп

Монадоморфизмы и образуемые ими группы и категории заслуживают специального изучения.

ТЕОРЕМА 4. *Для любой конечной группы оснащение притягивающего цикла каждой компоненты связности графа монады возведения в квадрат однородно (корневые деревья, присоединенные к циклу во всех его точках, одинаковы для каждой компоненты связности).*

ДОКАЗАТЕЛЬСТВО. Мы построим отображение, отображающее притягиваемое циклом в вершине a дерево в дерево, притягиваемое циклом в его следующей вершине, a^2 .

ОПРЕДЕЛЕНИЕ. Вершина имеет *ранг* r , если она отделена от притягивающего цикла r ребрами.

ПРИМЕР. Вершины притягивающего цикла имеют ранг нуль.

Рассмотрим притягивающий цикл периода T образованный вершинами $\{a, a^2, a^4, \dots, a^{2^{T-1}}\}$ (следующая вершина цикла – опять a). В этом случае выполняется условие периодичности

$$a^S = 1, \quad \text{где } S = 2^T - 1.$$

ОПРЕДЕЛЕНИЕ. Назовем *связностью* компоненты, притягиваемой циклом периода T , отображение P , переводящее каждую вершину b ранга r в вершину

$$Pb = c = b^x, \quad \text{где } x = (2^r - 1)S + 2.$$

ПРИМЕР. Вершины $(a, b_1, b_2, \dots)$ рангов $(0, 1, 2, \dots)$ переходят в $Pa = a^2$, $Pb_1 = b_1^{S+2}$, $Pb_2 = b_2^{3S+2}, \dots$

Из условия периодичности $a^S = 1$ вытекают соотношения

$$b_1^{2^S} = 1, \quad b_2^{4^S} = 1, \quad \dots, \quad b_r^{2^r S} = 1$$

для вершин b_r ранга r (поскольку вершина $b_r^{2^r} = a$ принадлежит притягивающему циклу).

Выбор значения $x(r)$ в определении связности объясняется следующим фактом.

ЛЕММА 1. *Связность является монадоморфизмом:*

$$P(b^2) = (P(b))^2.$$

ДОКАЗАТЕЛЬСТВО. Для вершины b ранга r ранг вершины b^2 равен $r - 1$. Поэтому имеют место следующие тождества:

$$\begin{aligned} P(b^2) &= (b^2)^y = b^{2y}, \quad \text{где } y = (2^{r-1} - 1)S + 2; \\ (P(b))^2 &= (b^x)^2 = b^{2x}, \quad \text{где } y = (2^r - 1)S + 2. \end{aligned}$$

Отношение этих двух степеней вершины b равно $b^{2(x-y)}$. Но $2(x-y) = 2^r S$, поэтому отношение равно 1, согласно условию периодичности, и лемма 1 доказана.

ЛЕММА 2. Если разные вершины b и b' имеют общий квадрат $b^2 = (b')^2$, то вершины $c = b^x$ и $c' = (b')^x$ также различны.

ДОКАЗАТЕЛЬСТВО. Если $r > 0$, то число $x = 2k + 1$ нечетно. В этом случае имеют место тождества

$$c = b(b^2)^k, \quad c' = b'(b^2)^k,$$

поэтому из равенства $c = c'$ вытекает равенство $b = b'$, доказывающее лемму 2.

ЛЕММА 3. Если вершина b имеет ранг 1, то вершина $c = Pb$ не принадлежит притягивающему циклу (так что ранг вершины c равен 1).

ДОКАЗАТЕЛЬСТВО. Если бы вершина $c = b^{S+2}$ принадлежала притягивающему циклу, то эта вершина была бы степенью a^{2^i} принадлежащей циклу вершины $a = b^2$.

Различных таких степеней T , но соотношения

$$(Pb)^2 = P(b^2) = P(a) = a^2$$

привели бы к выводу $Pb = a$, т.е. $b^{S+2} = b^2$. Последнее равенство означало бы, что $b^{2^T+1} = b^2$, так что имели бы место соотношения

$$b = b^{2^T} = a^{2^{T-1}}$$

и ранг вершины b был бы равен нулю, а не 1.

Полученное противоречие доказывает лемму 3.

ЛЕММА 4. Связность изоморфно отображает дерево, притягиваемое вершиной a цикла, на дерево, притягиваемое следующей вершиной a^2 (сохраняя, в частности, ранги вершин).

ДОКАЗАТЕЛЬСТВО. Обозначим через n_i число вершин дерева, притягиваемое вершиной a_i притягивающего цикла

$$\{a_0 = a, a_1 = a^2, \dots, a_i \equiv a^{2^i}, \dots\} \quad (i = 0, 1, \dots, T-1).$$

Изоморфизмы в последующие деревья, обсуждавшиеся в леммах 1–3, доказывают цепочку неравенств $n_0 \leq n_1 \leq \dots \leq n_T$.

Из T -периодичности цикла следует, что $n_T = n_0$, так что все числа периодической последовательности n_i равны, а все притягиваемые вершинами цикла деревья изоморфны, что и доказывает лемму 4 (а с ней и теорему 4).

ЗАМЕЧАНИЕ. Наряду с определенной выше специальной связностью можно рассматривать и другие связности, определяя их как монадоизоморфизмы компоненты, сдвигающие цикл на единицу.

Итерированная связность $M = P^T$ отображает каждое из оснащающих цикл деревьев на себя самого.

ОПРЕДЕЛЕНИЕ. Монадоморфизм M называется *монодромией* (компоненты периода T).

Монодромия действует тривиально на нижних этажах деревьев (где $r \leq 1$), но на высших этажах может быть нетривиальной (и, возможно, позволяет определить интересные инварианты группы).

ПРИМЕР. Для цикла периода $T = 5$ и вершины b ранга $r = 2$ вершина $b^4 = a$ принадлежит притягивающему циклу, так что $a^{3^2} = a$, $a^{3^1} = 1$, $b^{12^4} = 1$.

В этом случае $S = 31$, $x = 3S + 2 = 95$, $Mb = b^z$, $z = 95^5 \equiv 63 \pmod{124}$. Вершина $Mb = b^{63}$ может не совпадать с b , тогда как их проекции на первый этаж дерева (т.е. b^2 и $(Mb)^2$) совпадают: $b^2 = b^{126}$.

§ 7. Модулярная топология кубов Кеплера

В своей книге “Гармония Мира” Кеплер описал радиусы планетных орбит в терминах вписанных друг в друга правильных многогранников, а для этого вписал в додекаэдр пять кубов. Ребра этих кубов – это диагональ двенадцати граней додекаэдра (по одному ребру на каждую грань).

Эти кубы Кеплера автоматически возникают при описании геометрии монады возведения в квадрат группы $G = SL(2, \mathbb{Z}_5)$, состоящей из 120 элементов. Этот граф имеет 17 компонент:

$$[\text{граф } G] = T + 10A_2 + 6A_4.$$

Сейчас мы построим по нему риманову поверхность.

Коренное дерево T имеет 32 вершины: вершину $\begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}$ на первом этаже и 30 вершин c периода 4 (так что $c^4 = 1$) на втором этаже, так что набор рангов имеет вид $r(T) = (1, 1, 30)$ (учитывая коренную вершину 1 на нулевом этаже).

Периоды точек компонент A_4 равны 5 (для вершин на притягивающих циклах) и 10 (для вершин единственного первого этажа оснащающих деревьев). Типичные примеры – элемент $\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$ периода 10 и его квадрат $\begin{pmatrix} 2 & 3 \\ 3 & 0 \end{pmatrix}$ периода 5.

Периоды точек компонент A_2 равны 3 (для вершин на притягивающих циклах) и 6 (для вершин единственного первого этажа оснащающих деревьев). Типичные примеры – элемент $\begin{pmatrix} 1 & 1 \\ 4 & 0 \end{pmatrix}$ периода 6 и его квадрат $\begin{pmatrix} 0 & 1 \\ 4 & 4 \end{pmatrix}$ периода 3.

ТЕОРЕМА 5. *Группа $G = SL(2, \mathbb{Z}_5)$ действует на конечной проективной прямой $\mathbb{P} = P^1(\mathbb{Z}_5)$ как некоторая специальная группа 60 четных перестановок шести точек этой конечной прямой.*

Чтобы описать эти перестановки, начнем с додекаэдра с его двенадцатью пятиугольными гранями.

Соединим каждую грань с противоположной отрезком, соединяющим их центры.

Группа симметрий додекаэдра переставляет эти 6 прямых. Чтобы описать подгруппу из 60 специальных четных перестановок (что составляет малую долю из общего числа $360 = 6!/2$ четных перестановок шести элементов), обратимся к кубам Кеплера.

Построение такого куба начинается с выбора одной из диагоналей на одной из граней додекаэдра. В конце этой диагонали сходятся с рассматриваемой еще две грани, и на них тоже надо выбрать по проходящей через эту концевую точку диагонали.

Для этого достаточно повернуть додекаэдр вокруг этой концевой точки на угол 120° , переставляя циклически три сходящиеся в ней грани. Исходная диагональ грани перейдет при этом в ортогональную ей диагональ соседней грани.

Продолжая этот процесс, переходя от одного конца диагонали к другому, мы быстро построим 12 диагоналей граней (по одной на каждой грани), они образуют куб Кеплера (будучи его ребрами).

Этот куб зависит от того, какую из пяти диагоналей мы выбрали вначале на исходной грани. Так что конструкция Кеплера дает пять кубов, вписанных в додекаэдр.

Нужные нам 60 специальных перестановок шести элементов, реализуемых действием группы $SL(2, \mathbb{Z}_5)$ на конечной проективной прямой $\mathbb{P}$, описываются в этих терминах как 60 *вращений* додекаэдра, составляющих половину группы его симметрий. Они реализуют все 60 четных перестановок пяти кубов Кеплера. Поэтому *проективная группа конечной проективной прямой $\mathbb{P}$ (состоящей из 6 точек) изоморфна группе $S^+(5)$ четных перестановок пяти элементов (а именно, пяти кубов Кеплера)*:

$$(G = SL(2, \mathbb{Z}_5))/\{\pm 1\} \simeq S^+(5).$$

ЗАМЕЧАНИЕ 1. Группа G состоит из 120 элементов, как и группа $S(5)$ всех перестановок пяти элементов. Эти две группы из 120 элементов не изоморфны. Действительно, матричная группа G имеет центр $\{\pm 1\}$, состоящий из двух элементов, в то время как центр группы перестановок тривиален.

ЗАМЕЧАНИЕ 2. Группа G не представляется в виде прямого произведения $K \times H$, где $K = \{\pm 1\}$ – группа из двух элементов.

Действительно, обозначим через $(R_0 = 1, R_1, R_2, \dots)$ ранги дерева T компоненты единицы графа группы H . Ранги произведения $A_1 * T$ будут тогда равны $(1, 2R_1 + 1, 2R_2, \dots)$ (по формуле рангов произведения), поскольку граф A_1 группы K имеет набор рангов $(1, 1)$.

Для группы G ранги дерева компоненты единицы равны $(1, 1, 30)$. Поэтому, если бы группа G была изоморфна произведению $K \times H$, то мы должны бы были иметь $2R_1 + 1 = 1, 2R_2 = 30$, т.е. $R_1 = 0, R_2 = 15$, что невозможно, так как второй этаж пуст, когда пуст первый, а 15 не равно 0.

Аналогичным образом доказывается нетривиальность расслоения $G \rightarrow G/K$ для групп $SL(2, \mathbb{Z}_p), p > 5$.

В терминах перестановок точек конечной проективной прямой компоненты графа монады возведения в квадрат для группы $G = SL(2, \mathbb{Z}_5)$ могут быть описаны диаграммами Юнга специальных четных перестановок кубов Кеплера, а именно:

$$A_1 \sim (5), \quad A_2 \sim (3 + 1 + 1), \quad T_r \sim (1 + 1 + 1 + 1 + 1)$$

на этажах $r = 0$ и $r = 1, T_2 \sim (2 + 2 + 1)$.

Геометрически компонента A_4 представляется четырьмя нетривиальными вращениями додекаэдра, сохраняющими одну из его граней (и, следовательно, противоположную грань). Таких пар граней 6, компонент 6, а всего таких нетривиальных вращений додекаэдра 24.

Вращения, реализуемые компонентой типа A_2 , сохраняют вершину додекаэдра (и, следовательно, противоположную вершину). Таких пар вершин 10, компонент 10, и всего таких нетривиальных вращений додекаэдра 20.

Вращения, реализуемые элементом второго этажа T_2 , сохраняют ребро (и, следовательно, противоположное ребро). Таких пар ребер 15, элементов 15, и вместе с тождественным преобразованием (реализуемым этажами T_0 и T_1) получаются все $24 + 20 + 15 + 1 = 60$ вращений додекаэдра.

Рассмотрим с такой же точки зрения группу $G = SL(2, \mathbb{Z}_p)$, где p нечетно. Она переставляет $p + 1$ точку конечной проективной прямой

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

ТЕОРЕМА 6. *Все эти перестановки четны.*

Действительно, образующие $g = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ и $h = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ группы G имеют нечетный порядок p в группе G (т.е. $g^p = h^p = 1$). Из этого следует четность соответствующих образующим перестановок, потому что для нечетной перестановки f ее нечетная итерация f^p была бы нечетной перестановкой и не могла бы быть тождественным преобразованием.

Итак, группа $G/\{\pm 1\}$ специальных (проективных) перестановок $p + 1$ элементов (состоящая из некоторых $p(p^2 - 1)/2$ четных перестановок) гораздо меньше, чем вся группа $(p + 1)!/2$ четных перестановок $p + 1$ элемента.

Простейший пример здесь – случай $p = 7$, когда проективная группа $G/\{\pm 1\}$ состоит из 168 специальных четных перестановок восьми точек конечной проективной прямой $\mathbb{P}$.

Додекаэдр в этом примере заменяется “правильным многогранником рода $g = 3$ ”, имеющим 24 семиугольных граней, встречающихся по 3 в 56 вершинах и ограниченных 84 ребрами.

Этот многогранник связан с особенностью K_{12} голоморфной функции $x^2 + y^3 + z^7$ в $\mathbb{C}^3$ и с группой отражений треугольника плоскости Лобачевского с углами $(\pi/2, \pi/3, \pi/7)$.

Забавная комбинаторика этих специальных четных перестановок заслуживает подробного изучения.

Сохраняемая ими проективная структура на множестве из $p + 1$ точки фиксируется выбором циклического порядка на подмножестве из $p - 1$ точки. Выбор этого подмножества несуществен, но его нужно зафиксировать для того, чтобы получить взаимнооднозначное соответствие между проективными структурами и циклическими порядками.

Если $p = 5$, то структур 6, поскольку множество из $p - 1 = 4$ элементов имеет 6 циклических порядков (число циклических порядков на множестве из $m = p - 1$ элементов равно $(m - 1)! = (p - 2)!$).

Каждая из этих шести структур сохраняется $360/6 = 60$ специальными перестановками шести точек (класс специальных перестановок зависит от структуры).

Если $p = 7$, то число циклических порядков на фиксированном подмножестве из $p - 1 = 6$ из $p + 1 = 8$ точек прямой $\mathbb{P}$ равно $(p - 2)! = 5! = 120$.

Каждая из этих 120 структур сохраняется специальными четными перестановками $p + 1 = 8$ точек конечной проективной прямой, число каковых специальных перестановок равно

$$\frac{(p + 1)!/2}{(p - 2)!} = \frac{p(p^2 - 1)}{2} = 168.$$

Чтобы обобщить имеющуюся при $p = 5$ интерпретацию этой проективной группы $G/\{\pm 1\}$ при помощи кубов Кеплера, мы должны построить при $p > 5$ аналог поверхности додекаэдра и аналог конструкции кубов Кеплера.

Обобщением додекаэдра окажется ниже некоторая риманова поверхность, а аналоги кубов Кеплера доставляют подгруппы Гамильтона.

§8. Кеплеровы кубы и подгруппы Гамильтона

Классическая группа Гамильтона состоит из 8 кватернионных единиц, $\{\pm 1, \pm i, \pm j, \pm k\}$. Она изоморфна связной компоненте единицы для монады возведения в квадрат группы $SL(2, \mathbb{Z}_3)$ (которая является единственной из групп $SL(2, \mathbb{Z}_n)$, для которой компонента единицы монады возведения в квадрат составляет подгруппу).

Кубы Кеплера, вписанные в додекаэдр, и их K_{12} -обобщения, описанные ниже, связаны с подгруппами компоненты единицы монады возведения в квадрат в группе $G = SL(2, \mathbb{Z}_p)$, изоморфными классической группе Гамильтона.

Из 30 элементов порядка 4, составляющих второй этаж T_2 компоненты единицы монады возведения в квадрат группы $G = SL(2, \mathbb{Z}_5)$, можно выделить пять непересекающихся секстетов, каждый из которых образует, вместе с элементами 1 и -1 нулевого и первого этажей группы G подгруппу, изоморфную классической группе Гамильтона.

Все пять определенных таким образом подгрупп Гамильтона группы G сопряжены в группе G .

Чтобы опознать секстет, можно воспользоваться соотношениями $\{r^2 = -1, s^2 = -1, t^2 = -1\}$ для его антикоммутирующих образующих r, s и их произведения $t = rs$.

Для доказательства сформулированных выше свойств секстетов достаточно проверить их в одном примере, например, для секстета $\{\pm r, \pm s, \pm t\}$, где

$$r = \begin{pmatrix} 0 & 1 \\ 4 & 0 \end{pmatrix}, \quad s = \begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix}, \quad t = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix},$$

вычислив сопряжения, сохраняющие этот секстет.

Эти сопряжения порождают 12 автоморфизмов соответствующей подгруппы Гамильтона. Все 120 элементов группы G действуют как 60 операций сопряжения, поскольку $axa^{-1} = (-a)x(-a)^{-1}$.

60 сопряженных к данному сексету доставляют $60/12 = 5$ разных секстетов (так что мы получаем 5 подгрупп Гамильтона в G), которые все друг другу сопряжены.

Произведение двух элементов порядка 4 в G само имеет порядок 4 (удовлетворяя соотношению $(rs)^2 = -1$) в точности для тех пар (r, s) , которые порождают подгруппу Гамильтона. В частности, оба элемента такой пары антикоммутируют (что помогает легко распознать их, так это – единственные антикоммутирующие пары элементов порядка 4).

Описанные вычисления доставляют следующие 5 секстетов I–IV (выписаны только три элемента каждого секстета, остальные три – это $(-r, -s, -t)$):

секстет	I	II	III	IV	V
r	01 40	11 34	20 33	13 14	14 24
s	02 20	20 13	12 44	20 23	20 43
$t = rs$	20 03	33 02	24 03	34 02	32 02

Пять кубов Кеплера порождаются этими пятью подгруппами Гамильтона H следующим образом (который имитирует вычисление матрицы A^h для матрицы $h \in H$).

Выберем в группе G элемент A порядка 3. Сопряжение посредством A переводит каждую подгруппу Гамильтона группы G в подгруппу Гамильтона. Для данной подгруппы Гамильтона H в G имеется 8 элементов A порядка 3, сохраняющих H при сопряжении посредством A : $ANA^{-1} = H$.

ОПРЕДЕЛЕНИЕ. Эти 8 элементов третьего порядка являются восемью вершинами куба Кеплера, связанного с выбранной подгруппой Гамильтона, H .

Описанные вычисления доставляют следующие четверки вершин (a, b, c, d) кубов Кеплера (остальные четыре элемента группы G – это обратные им элементы, т.е. (a^2, b^2, c^2, d^2)):

секстет	I	II	III	IV	V
a	12 13	04 14	04 14	44 10	44 10
b	32 11	02 24	03 34	02 24	03 34
c	34 31	32 11	34 37	14 33	12 13
d	14 33	24 22	23 12	23 12	24 22

Каждая из десяти вершин кубов Кеплера, указанных в таблице, встречается в ней дважды, и через каждую вершину куба Кеплера проходит ровно два куба, доставляя, вместе с обратными элементами, все 20 вершин додекаэдра (являющихся как раз всеми двадцатью элементами третьего порядка в группе G).

Вершины кубов Кеплера можно легко вычислять, используя следующие свойства этих элементов группы G .

Выберем ориентацию куба и соответствующую ориентацию каждой его грани. Пусть P, Q, R, S – последовательность вершин одной грани (упорядоченная в соответствии с ориентацией). Тогда

$$PQ = QR = RS = SP$$

будет соответствующим элементом подгруппы Гамильтона (все 4 ребра одной грани дают одно и то же произведение).

Полученное соответствие шести элементов секстета шести граням куба обладает следующим свойством (которое можно было бы принять за определение либо куба Кеплера, если секстеты определены, либо секстета, если определены кубы):

произведение трех элементов группы G , соответствующих трем сходящимся в вершине куба граням (с правильными ориентациями) равно всегда 1.

Таких раскрашиваний граней куба элементами секстета 12, и все они переводятся друг в друга вращениями куба.

Другое описание того же самого соответствия между подгруппами Гамильтона и кубами Кеплера таково:

четыре вершины куба Кеплера получаются из одной из них (скажем, из A), сопрягая ее восемью элементами подгруппы Гамильтона, $\{A, rAr^{-1}, sAs^{-1}, tAt^{-1}\}$ ($-r$ сопрягает так же, как и r).

Остальные четыре вершины куба Кеплера обратны описанным, т.е. это $\{A^2, rA^2r^{-1}, \dots\}$. Вершины куба Кеплера соединены ребрами так, как соединены друг с другом расставленные в вершинах куба элементы группы Гамильтона: вершины (s, t, r) – соседи вершины 1, вершина $(-u)$ противоположна вершине u .

Предыдущее построение вершин куба Кеплера по элементам подгруппы Гамильтона продолжает отображение

$$1 \mapsto A, \quad (-1) \mapsto A^{-1},$$

приписывая вполне определенный смысл матрицам A^r, A^s, A^t .

Возвращаясь к поверхности додекаэдра, мы можем получить ее из комбинаторики группы G , выбирая в качестве вершин элементы порядка 3. Вслед за этим следует выбрать один из двух классов сопряженных элементов порядка 5 в группе $PSL(2, \mathbb{Z}_5)$ (или же порядка 10 в группе $SL(2, \mathbb{Z}_5)$).

В зависимости от этого выбора класса сопряженных элементов мы получим из группы $G = SL(2, \mathbb{Z}_5)$ ту или иную додекаэдрическую поверхность. Ситуация похожа здесь на соотношение между правильным пятиугольником и пятиугольной звездой с теми же вершинами.

Перестановку вершин додекаэдра назовем симметрической, если она переводит каждую симметрию додекаэдра в его (вообще говоря, другую) симметрию.

Сами симметрии определяют такие перестановки, но, кроме них, есть еще и нетривиальная симметрическая перестановка (с точностью до симметрий – только одна).

Эта нетривиальная симметрическая перестановка вершин как раз и превращает додекаэдр, полученный при одном из выборов класса сопряженных элементов, в додекаэдр, соответствующий другому выбору.

В терминах группы $G = SL(2, \mathbb{Z}_5)$ переход от одной додекаэдрической поверхности к другой можно еще описать как $GL(2, \mathbb{Z}_5)$ -сопряжение (посредством матрицы, определитель которой не является квадратичным вычетом, например, матрицы $\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$).

Когда класс сопряженных элементов выбран, две вершины A и B (третьего порядка в G) соединяются ребром, если произведение принадлежит выбранному классу. Это дополняет набор вершин до графа. Выходящие из одной вершины 3 ребра циклически переставляются сопряжением посредством этой вершины, и с получаемым циклическим порядком выходящих из каждой вершины ребер полученный граф оказывается плоским. Он делит плоскость, или сферу S^2 , в которую вложен, на пятиугольники. Это и доставляет искомым додекаэдр.

Было бы интересно узнать, насколько эта конструкция распространяется на другие группы G (например, доставляет ли она столь же гладкие или даже голоморфные, как в случае $G = SL(2, \mathbb{Z}_5)$, поверхности в случаях $SL(2, \mathbb{Z}_n)$ или в случае $GL(2, \mathbb{CZ}_p)$ матриц, элементы которых являются комплексными числами $x + iy$, где x и y – вычеты по модулю p).

§9. Риманова поверхность семиугольников и ее кубы Кеплера

При перенесении додекаэдрических исследований на случай группы $G = SL(2, \mathbb{Z}_7)$ получаются следующие выводы.

ТЕОРЕМА 7. *В части $T_0 + T_1 + T_2$ дерева монады возведения в квадрат в группе G имеются 14 подгрупп Гамильтона. Семь из них сопряжены одной из них, а семь другой, эти же две не сопряжены в G , хотя и сопряжены в большей группе, $GL(2, \mathbb{Z}_7)$.*

Образующие (r, s) семи из подгрупп Гамильтона и их произведения $t = rs$ таковы:

подгруппа	I	II	III	IV	V	VI	VII
r	01 60	24 45	32 24	02 30	03 20	16 26	13 46
s	23 35	15 16	34 14	26 55	25 65	14 36	12 66
t	35 54	66 21	46 33	33 64	41 43	55 62	56 52

Остальные 7 подгрупп Гамильтона получаются из этих при помощи группового автоморфизма

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} a & -b \\ -c & d \end{pmatrix}$$

(подгруппа $\tilde{I}$, двойственная подгруппе I , содержит матрицы $\begin{pmatrix} 0 & 6 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 4 \\ 4 & 5 \end{pmatrix}, \begin{pmatrix} 3 & 2 \\ 2 & 4 \end{pmatrix}$ и т.д.)

14 секстетов этих 14 подгрупп Гамильтона доставляют $6 \cdot 14 = 84$ элемента порядка 4, в то время как второй этаж T_2 монады группы G содержит всего 42 элемента.

Поэтому описанные секстеты пересекаются. Эти пересечения связаны с проблемой четырех красок следующей конструкцией.

Составим граф, 14 вершин которого представляют собой 14 подгрупп Гамильтона группы G , а ребра которого соединяют те вершины, секстеты которых пересекаются. Получающийся граф можно описать как подмножество двумерного тора, разбивающее его на 7 шестиугольников, встречающихся по 3 в 14 вершинах. Каждый шестиугольник имеет общую сторону с каждым из остальных. Поэтому получающаяся на торе карта из 7 стран не может быть правильно раскрашена меньше, чем семью красками. Семь подгрупп, сопряженных с подгруппой A , обозначены ниже окружностями.

Покрытие тора семью шестиугольниками получается из правильно шестиугольника на евклидовой плоскости $\mathbb{R}^2$. Объединение этой шестиугольной области с шестью ее отражениями в сторонах покрывает плоский многоугольник, являющийся фундаментальной областью группы $\mathbb{Z}^2$ параллельных переносов, сохраняющих разбиение плоскости на конгруэнтные шестиугольники. Фактор-тор $T^2 = \mathbb{R}^2/\mathbb{Z}^2$ разбит, как указано выше, на 7 шестиугольных областей (группа параллельных переносов порождена векторами AA' и AA'').

Изоморфность узора пересечений четырнадцати секстетов с этим торическим графом проверяется прямым (хотя и утомительным) вычислением 84 матриц $\{\pm r, \pm s, \pm t\}$.

Построение кубов Коплера из этих 14 подгрупп Гамильтона повторяет проведенную выше $SL(2, \mathbb{Z}_5)$ -конструкцию и доставляет 14 кубов Кеплера, из которых 7 сопряжены одному из них, а 7 – другому; сопряжения действуют на каждом кубе как его вращения.

Все эти кубы можно было бы нарисовать на обобщающей додекаэдр поверхности M , покрытой 24-мя семиугольниками, встречающимися вдоль 84 ребер, образуя поверхность рода 3 с 56 вершинами, в каждой из которых сходятся три грани.

Вершинами поверхности M являются элементы третьего порядка в группе G , а грани определяются элементами порядка 14, $c = ab$, где $c^7 = -1$, $a^3 = b^3 = 1$.

Вместо поверхности M удобно рисовать ее фактор-поверхность, определенную следующим “складыванием”.

Отображение, сопоставляющее каждой матрице A транспонированную обратную матрицу $\tilde{A}$, является автоморфизмом группы $Q = SL(2, \mathbb{Z}_7)$ (а именно, сопряжением посредством матрицы $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$). Этот автоморфизм переводит элементы третьего (и четырнадцатого) порядка в элементы третьего (соответственно, четырнадцатого) порядка, и поэтому действует на поверхности M .

Фактор-поверхность M' получается из M отождествлением каждой матрицы A с $\tilde{A}$, и мы получаем отображение складывания $M \rightarrow M'$. Поверхность M' имеет только 28 вершин и только 12 семиугольных граней, изображенных ниже. Она имеет род 1 (гомеоморфна тору).

Отображение $M \rightarrow M'$ является двулистным разветвленным накрытием с четырьмя точками ветвления, топологически типа комплексной функции $\sqrt{z}$. Точки ветвления – не вершины построенных выше многоугольников, а середины некоторых четырех ребер.

Вершины поверхности M – это 28 матриц $\begin{bmatrix} i \end{bmatrix}$ перечисленных ниже, и 28 их квадратов, $\widehat{\begin{bmatrix} i \end{bmatrix}} = \left(\begin{bmatrix} i \end{bmatrix}\right)^2$ (это – все элементы третьего порядка в группе G): номер матрицы, i ,

Рис. 1. Фундаментальная область фактор-поверхности M'

принимает значения от 1 до 13 и от 15 до 29

i	1	2	3	4	5	6	7	8	9	10	11	12	13
$\boxed{i}$	40 02	21 04	22 04	23 04	24 04	25 04	26 04	20 64	20 54	20 14	20 24	20 34	20 44

i	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
$\boxed{i}$	01 66	06 16	04 56	05 46	03 26	02 36	31 13	34 23	32 43	14 15	11 45	13 65	16 35	12 25	75 55

На рисунке показаны 12 семиугольных граней фундаментальной области поверхности M' на M и их соседи, складывание состоит в склейке A с $\tilde{A}$ вдоль ограничивающей фундаментальную область жирной линии. Точки ветвления складывания

Рис. 2. Усредненная зависимость периода от модуля в билогарифмическом масштабе

Рис. 3. Билогарифмический график Колмогорова, приведший к открытию закона $5/3$ теории турбулентности

$M \rightarrow M'$ – это центральные точки отрезков $(A\tilde{A})$, где отрезки суть $(\hat{3}, 11)$ в области XI, $(\hat{23}, 22)$ в области I, $(6, \hat{9})$ в области XII и $(15, \hat{16})$ в области V.

Комплексные структуры поверхностей M и M' было бы тоже интересно определить в терминах комбинаторики группы G , так как тогда эту комбинаторику можно было бы связать с геометрией и с арифметикой эллиптических функций.

§ 10. Статистика периодов Ферма–Эйлера

Здесь описана зависимость от модуля n наименьшего периода $T(n)$ арифметической прогрессии

$$\{2^t \pmod{n}, t = 1, 2, \dots, T\}$$

для нечетных $n \leq 2001$. Вычисления были проведены Ф. Аикарди на компьютере.

Ради сглаживания хаотических отклонений от усредненного поведения, вместо частоты осциллирующей величины периода $T(n)$ график изображает пропорциональную Чезаровскому среднему величину суммы

$$S(n) = \sum_{k=1}^n T(k),$$

причем в билогарифмическом масштабе (по осям откладываются $\ln n$ и $\ln S$).

Рис. 2 является теоретико-числовым аналогом приема Колмогорова, с помощью которого он открыл “закон 5/3” теории турбулентности. Оригинальный график Колмогорова воспроизведен на рис. 3.

СПИСОК ЛИТЕРАТУРЫ

- [1] В. И. Арнольд. Группы Эйлера и арифметика геометрических прогрессий. М.: МЦНМО, 2003.
- [2] В. И. Арнольд. Динамическая система Ферма–Эйлера и статистика арифметик геометрических прогрессий // Функци. анализ и его прил. 2003. Т. 37. № 1. С. 1–20.
- [3] V. I. Arnold. Ergodic arithmetical properties of geometric progressions dynamics // Mosc. Math. J. 2004 (to appear).
- [4] В. И. Арнольд. Топология алгебры: комбинаторика операции возведения в квадрат // Функци. анализ и его прил. 2003. Т. 37. № 2. С. 3–16.
- [5] V. I. Arnold. Arithmetics of binary quadratic forms, symmetry of their continued fractions and geometry of their de Sitter world. Moscow, Dubna: MCCME, 2002; // Bol. Brasil. Math. Soc. (N.S.). 2003. V. 34. № 1. P. 1–41.
- [6] В. И. Арнольд. Слабые асимптотики чисел решений диофантовых задач // Функци. анализ и его прил. 1999. Т. 33. № 3. С. 65–66.

Математический институт им. В. А. Стеклова РАН

Поступила в редакцию

05.01.2003