В. И. Арнольд, Топология и статистика формул арифметики, *УМН*, 2003, том 58, выпуск 4(352), 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: 54.70.40.11
2 января 2019 г., 03:38:59
ТОПОЛОГИЯ И СТАТИСТИКА ФОРМУЛ АРИФМЕТИКИ

В. И. Арнольд

В статье дан обзор заложенных и классических исследований геометрических прогрессий, общдающих ходу теории Ферма и связанных с этими исследованиями. С теорией динамических систем и оценивающих степень хаосичности образующих геометрические прогрессии, общдающих связанных с этими исследованиями.

В качестве вспомогательного средства изучается группа операций наложения в квадрат элементов конечных групп и моделей. Для космических групп связанные компьютеры этих графов описываются в циклами-атракторы, одинаково оценивающими проявлениям библиотеки корневых деревьев, алгоритма которых также описан в статье. Основные деревья описываются однородными и для графов симметрических групп перестановок, а также для групп чётных перестановок.

Библиография: 6 названий

СОДЕРЖАНИЕ

§1. Динамическая система Ферма—Эйлера ........................................ 4
§2. Случайны ли числа элементов геометрической прогрессии? .. 7
§3. Топология операции всевозможных в квадрат .............................. 10
§4. Алгебра корневых деревьев ..................................................... 11
§5. Графы всевозможных в квадрате с перестановок ...................... 13
§6. Однородность монад всех конечных групп ................................ 16
§7. Модульная 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 теоремы.

Завершая последнее время арифметической квадратичных форм (и ее связанным с редуктивным миром теории, 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 явлении во многих случаях остаются не теоремами, а экспериментальными фактами (подтвержденными всеми...
лишь несколькими миллионами наблюдений), я решаюсь рассказать здесь о некотором из них, тем более что небольшую долю этих фактов уже удалось формулировать 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 теоремо-числовые свойства геометрических прогрессий, приведенных по модулю n, а более периодической последовательности остатков от деления на 13 степеней двойки,

\[ \{1, 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1, 2, \ldots\} \]

(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 распространял Эйлер, у которого основание \( a \) и модуль \( n \) лишь взаимно просты).

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

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

<table>
<thead>
<tr>
<th>( n )</th>
<th>5</th>
<th>7</th>
<th>9</th>
<th>13</th>
<th>15</th>
<th>19</th>
<th>29</th>
<th>31</th>
<th>51</th>
<th>71</th>
<th>509</th>
<th>511</th>
</tr>
</thead>
<tbody>
<tr>
<td>( T )</td>
<td>4</td>
<td>3</td>
<td>6</td>
<td>12</td>
<td>4</td>
<td>18</td>
<td>28</td>
<td>5</td>
<td>8</td>
<td>35</td>
<td>508</td>
<td>9</td>
</tr>
</tbody>
</table>

Более регулярно ведут себя средние (хотя бы во необозримом отрезке 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 периода \( T \) такие:

<table>
<thead>
<tr>
<th>( \sum n )</th>
<th>100</th>
<th>300</th>
<th>500</th>
<th>700</th>
<th>900</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \sum T )</td>
<td>68</td>
<td>158</td>
<td>246</td>
<td>299</td>
<td>329</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>( n )</th>
<th>9</th>
<th>109</th>
<th>509</th>
<th>1009</th>
<th>1509</th>
<th>2009</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \sum T )</td>
<td>15</td>
<td>1409</td>
<td>23607</td>
<td>82761</td>
<td>176016</td>
<td>302277</td>
</tr>
</tbody>
</table>

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

\[ T \approx 1.4n^{4/5} \]
Топология и статистика формул арифметики

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

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

Рассмотрим мультипликативную группу вычетов по модулю $n$, взаимно простых с н (и называем ее группой Эйлера и обозначаем 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 н довольно сложным образом:

<table>
<thead>
<tr>
<th>$n$</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\varphi(n)$</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>2</td>
<td>6</td>
<td>4</td>
<td>6</td>
<td>10</td>
<td>10</td>
<td>4</td>
</tr>
</tbody>
</table>

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

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

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 формулируемое 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,

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

tак что и период $T$, 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):

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>4</th>
<th>8</th>
<th>16</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>6</td>
<td>12</td>
<td>24</td>
<td>17</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>10</td>
<td>20</td>
<td>9</td>
<td>18</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>14</td>
<td>28</td>
<td>25</td>
<td>19</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>22</td>
<td>13</td>
<td>26</td>
<td>21</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>30</td>
<td>29</td>
<td>27</td>
<td>23</td>
<td></td>
</tr>
</tbody>
</table>

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

$N(31) = 6.$

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

<table>
<thead>
<tr>
<th>$n$</th>
<th>37</th>
<th>65</th>
<th>129</th>
<th>229</th>
<th>381</th>
<th>509</th>
<th>511</th>
</tr>
</thead>
<tbody>
<tr>
<td>$T$</td>
<td>36</td>
<td>12</td>
<td>14</td>
<td>76</td>
<td>14</td>
<td>508</td>
<td>9</td>
</tr>
<tr>
<td>$N$</td>
<td>1</td>
<td>4</td>
<td>6</td>
<td>3</td>
<td>18</td>
<td>1</td>
<td>48</td>
</tr>
</tbody>
</table>

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

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

Коэффициент $c$ появляется здесь как вероятность неократимости дроби $p/q$ (точно так же, $1/\zeta(m)$ – вероятность отсутствия целых точек на отрезке $0 \leq x$ в периодическом векторе $m$-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 открыт тоже Эйлер, следует из теоремы рядов Фурье (можно разложить в ряд Фурье $2\pi$-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]).
Так что факт, что сумма \( 2/5 + 4/5 \) показателей эмпирических средних асимптотик для \( N \) и для \( T \) больше показателя 1 средней асимптотики для функции Эйлера \( \varphi \), 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 (вкладное явление перемежаемости в теории турбулентности и в гидродинамике).

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

Эмпирические формулы для средних частот \( p_n \) встречаются 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 сдайбов асимптотик

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

Однако никаких оснований для радиомодальности этих показателей степени (подобной радиоаномальности показателей Кольмогорова в теории турбулентности и предшествующим им аналогичных гидродинамических показателям Леонардо да Винчи) не видно.

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

Прямая Аикари указывает на эмпирические сдайбы (усредненные) асимптотики

\[
T(n) \sim 0.94n^{0.834}, \quad N(n) \sim 0.60n^{0.36}, \quad \varphi(n) \sim cn^{\alpha},
\]

где для \( n = 1 \) до \( 10^9 \) константы приближенно равны \( a = 0.9994, c = 0.612 \), тогда как \( 6/\pi^2 \approx 0.6079 \).

В действительности для сближения с усредненного случая использовались графики в билогарифмическом масштабе значения \( \langle ST \rangle(n) = \sum_{k=1}^{n} T(k) \) и \( \langle SN \rangle(n) = \sum_{k=1}^{n} N(k) \), где \( k \) нечетны. Прямоугольные билогарифмические графики соответствуют степенным функциям

\[
\langle ST \rangle(n) \sim 0.255n^{1.834}, \quad \langle SN \rangle \sim 0.223n^{1.36}.
\]

§ 2. Случаи ли вычеты элементов геометрической прогрессии?

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

Показатель Липунова операции умножения вычетов на 2 указывает на довольно быстрый рост возмущений в диадической системе Ферма-Эйлера. Это позволяет окладить хаотического распределения этих вычетов (среди всех n вычетов из \( Z_n \)) 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.
Дедо в том, что все \( T(n) \) вычетов элементов \( \{2^t \mid t = 1, 2, \ldots, T\} \) по модулю \( n \) в пределах одного периода различны, так как первое же повторение какого-либо вычета приводило бы к повторению и всех следующих за ним.

Если бы вычёты членов изучаемой орбиты из \( T \) элементов были бы неявночными случайными элементами множества из \( m \) элементов \( (m = n \) в случае распределения вычетов в \( Z_n \)), \( n = \varphi(n) \) в случае изучения распределения вычетов в группе Эйлера \( \Gamma(n) \), то задача о диах рождения" из теории вероятностей подсказывала бы для \( T(n) \) гораздо меньше, чем \( n \), значение (порядок \( \sqrt{n} \)).

А именно, вероятность отсутствия совпадений в выборе из \( T \) элементов \( m \)-элементного множества малая, пока \( T \) "невелико", и близка к 1, когда \( T \) "велико", причем переход совершается вблизи специального критического значения, \( T_\ast \sim \sqrt{2m} \).

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 \( n \) неизвестен даже в смысле слаженных средних и слабых асимптотик, эмпирические данные статьи [1–3] подсказывают, что этот показатель если и не равен 1, то, во всяком случае, близко 1, чем к показателю 1/2, который должен был быть наблюдаем, если бы элементы орбиты были неявночными случайными вычетами.

Таким образом, наиболее интересный период геометрической прогрессии больше периода, соответствующего случайному выбору элементов орбиты. То есть вычёты членов прогрессии изображаю ближайшими сближения и в этом смысле растягиваются.

Для измерения этого расстояния я сосчитал среднее расстояние между соседями 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 делают окружность, равны \( x_i \), \( i = 1, \ldots, T \) (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" множество из \( T \) элементов нормализованную сумму квадратов расстояний между соседями,

\[
r = \frac{R}{L^2}
\]

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

Наименьшее значение "меры стохастичности" \( r \), равное \( 1/T \), достигается на каверномом строе арифметической прогрессии равноудаленных точек (делявших окружность на \( T \) дуг длиной \( 1/T \) каждая).

Найболее большое значение \( r = 1 \) достигается на кластерном распределении подвижной случайности (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 $0 \leqslant z_i \leqslant 1$, $\sum z_i = 1$ 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 точек $z$ в симплексе (равномерно по мере Лебега распределенной в нем).

Значение "меры стохастичности" $r$ для такого свободного распределения точек на окружности легко вычислить явно: оно промежуточно между минимальным минимальным значением (для сильно растрацкующихся частий) и кластерным максимальным значением (достигающимся для скучившихся в одно место частий).

Чтобы сравнивать множества с разными числами точек, $T$, я разделил значение показателя $r$ на его минимальное при данном числе точек значение $s_{	ext{max}}$ (по $L$ и по $T$) нормализованной параметра стохастичности

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

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

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

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

$$s_\ast = 2T/(T + 1).$$

Меньшие свободные значения параметра стохастичности $(1 \leqslant s < s_\ast)$ указывают на растрацкующие частии множества (тем более жёсткое, чем меньше $s$), а большие значения $(s_\ast < s \leqslant 1/T)$ — на их взаимное срастание.

Для вычетов теоретически прогрессий явные вычисления [1], [3] значений параметра стохастичности $s$ (предложенные Ф. Айкади с помощью компьютера) дали в большинстве случаев значения дважды нормализованного параметра стохастичности $s$ порядка 1.5 (прочим изредка встречаются и близкие к 1 значения, и сильно большие 2). Однако никаких теорем здесь нет — это всего лишь результаты тысячи экспериментов.

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

В обоих случаях также обнаружилось растрацивание (значения параметра $s$, меньше свободного). 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 подходящих дробей величины $a/n$, можно предполагать возможность получить (в различие в этих двух случаях) асимптотики параметра стохастичности последовательности $(at + b \mod n)$, $1 \leqslant t \leqslant T$, в терминах целой дроби для $a/n$ (случайные утверждения по теореме Гаусса—Курана об эргодических характеристиках элементов целых дробей). Речь идет здесь, разумеется, прежде всего о слабых асимптотиках.

Растрацивание вычетов членов геометрической прогрессии сказывается и на распределении длина дуг недоцикловой окружности $Z_n$ (или группы Эйлера $\Gamma(n)$) между
этими вычетами. Частоты встречаемости дуг различных длин $d$ (от максимальной длины $m - (T - 1)$ до минимальной длины 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 $T - 2$: 

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

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 $\{2^t \mod 15\}$ как четырехточечное подмножество $\{1, 2, 4, 8\}$ восьмиместной окружности вычетов, $\Gamma(15) = \{1, 2, 4, 7, 8, 11, 13, 14\}$ (с расстоянием 1 между последовательными вычисленными числами и между 14 и 1). “Расстояния” между соседними точками прогрессии вложат группы Эйлера $\Gamma(15)$ составляют $\{1, 2, 4\}$, т.е. дуги длины единица встречаются в $2^1 \frac{1}{2}$ раза реже, чем для случайных точек, что еще раз подтверждает растягивание вычетов членов геометрической прогрессии.

При этом дважды нормализованный показатель стихастичности 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 растягивание 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 монаады называется ориентированный граф, вершинами которого являются точки этого конечного множества, а ребра соединяют каждую точку графа с ее образом при отображении.

Иными словами, граф монада — это произвольный конечный граф, из каждой вершины которого выходит ровно одно ребро.

Геометрические прогрессии вычетов $\{2^t \mod n\}$, 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 коде вычетов $\mathbb{Z}_7$ имеет три компоненты связности:

```
0 1 6
\circ \circ \circ
```

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

\footnote{Расстоянием между двумя элементами цикла группы $\Gamma$ называется здесь число свободных от элементов группы дуг между двумя заданными вычетами.}
Теорема 1. Связные компоненты каждой монады представляют собой циклические аттракторы, оснащенные корневыми деревьями, присоединенными своими корнями к каждой вершине циклического аттрактора.

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

Рассмотрим теперь в качестве монады операцию возведения в квадрат элементов конечной коммутативной группы (при датогермированном к которой подключается монада \( x \rightarrow 2x \), порождающую геометрическую прогрессию \( \{2^t, t = 0, 1, 2, \ldots \}\)).

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

Это оснащающее дерево имеет (считая корень, принадлежащий циклу-аттрактору) \( 2^h \) вершин и представляет собой произведение бинарных деревьев в смысле определения произведения, данное 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 \( i = 1, 2, \ldots, n - 1 \).

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 умножений, \( x \rightarrow 2x \), в группе \( Z_4 \) 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, \( X \cdot Y \), действует на точку \((x, y)\) прямого произведения множеств вершин графа \( X \) и множества вершин графа \( Y \) по правилу

\[
(X \cdot Y)(x, y) = (Xx, Yy).
\]

Пример. Умножим п-вершинный цикл \( O_n \) на прямой п-вершинный граф \( T_2 = A_1 \) (в этом, например, нарисовано выше компонента \( \{1, 6\} \) графа возведения в квадрат в кольце \( Z_7 \)). Произведение \( A_n = O_n \cdot A_1 \) представляет собой 2\( n \)-вершинный граф сцилом-аттрактором \( O_n \) вольно оснащенным однородными корневыми деревьями в каждой своей вершине, подобно третьей компоненте \( A_2 = O_2 \cdot A_1 = \{2, 3, 4, 5\} \) нарисованному выше графа возведения в квадрат в кольце вычетов \( Z_7 \).

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

Граф произведения двух монад сам является корневым деревом. Граф дерева произведения монад мы будем называть произведением графов (деревьев) произведением монад.

Пример. Граф \( A_1 \cdot A_1 = D_1 \) — это четырехвершинное корневое дерево, в корень которого входят ровно три ребра (из оставшихся трех вершин). Это граф группы \( Z_2 \times Z_2 \).
Граф $D_n = O_n*D_1$ имеет $4n$ вершин и один цикл-аттрактор, в каждую вершину которого со стороны приходит три ребра (образующие вместе осящающее эту вершину дерево $D_1$).

При исследовании произведений корневых деревьев поделю составить дереву следующий набор "правил": через $r_i$ будем обозначать число вершин, путь от которых до корня состоит из $i$ ребер и имеет длину $i$ (в частности, $r_0 = 1$, $r_1(D_1) = 3$, $r_1(T_i) = 1$, $r_2(T_i) = 2$).

При перенесении графов ранги ведут себя так:

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

где $\max(i, j) = k$. Иными словами, сумма $s_k = r_0 + r_1 + \cdots + r_k$ удовлетворяет тождеству $s_k(X \ast Y) = s_k(X)s_k(Y)$.

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

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

\[
\begin{pmatrix}
2 & 2 & 4 & 8 \\
1 & 1 & 2 & 4 \\
1 & 1 & 2 & 4
\end{pmatrix},
\]

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 $T_2n + T_2n$, равны $\{1, 3, 3 \cdot 4, 3 \cdot 16, \ldots, 3 \cdot 4^{n-1}\}$ (при здании второго бинарного дерева большим исследовательность рангов продолжается степенями двойки).

Я так подробно описывал производство бинарных деревьев потому, что только они встречаются в качестве однородно осящающих цикл деревьев при опи- сании 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 несоциальные 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 конечной циклической группы $Z_n$.

Таблица умножения этих циклов такова:

$$O_m * O_n = dO_c,$$

где $d$ — наибольший общий делитель, a $c$ — наименьшее общее кратное чисел $m$ и $n$ (имеется в виду веерересекающееся объединение $d$ циклов одинаковой длины $c$).
Топология и статистика формул арифметики

Например, имеют место тождества в алгебре графов

\[ O_3 \times O_5 = O_{30}, \quad O_6 \times O_{19} = 2O_{30}. \]

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

![Diagram of graph]

\[ 7 + 7 \equiv 6 \text{ (mod 8)} \]

\{r_k\} = \{1, 1, 2, 4\}

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

Стрелки этого графа ведут к квадратичным вычетам по модулю 125 (например, \(13^2 \equiv 44 \text{ (mod 125)}\), а стоящие вдоль от цикла вершины оснащающих его деревьев \((22, 37, \ldots)\) – квадратичные невычеты (сравнение \(x^2 \equiv 2 \text{ (mod 125)}\) верно решено).

Именно топология подобных графов объясняет такие факты теории квадратичных форм, как, например, строение подгрупп значений "совершенных" квадратичных форм статьи [5] (вроде форм \(x^2 + 2y^2\)). В этом последние примере нечетные значения формы образуют подгруппу чисел вида произведения

\[ \prod p_i^{a_i}q_j^{b_j}r_k^2s_l^{2d_l}, \]

где \(p, q, r, s\) – 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, 123 и 343 все непредставимы, а числа 3, 17, 25 и 49 – представимы в виде \(x^2 + 2y^2\) с неподведенным \(x\) и \(y\) (как \(17 = 3^2 + 2 \times 2^2\)).

§ 5. Графы возведения в квадрат в группах перестановок

При попытке перевести теорему об однородности оснащения цикла монады дерева с коммутативными на произвольные конечные группы я обнаружил следующий факт.

Теорема 3. Любая связная компонента графа операции возведения в квадрат в симметрической группе перестановок и 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 цикл которых имеют нечетные длины.
Но циклическая перестановка нечетной длины сопряжена с его квадрату. Это сопряжение не только переводит в соседнюю одну из вершин цикла-атрактора, но действует и на осноывающие этот цикл деревья, также переставляя их, поэтому все осноывающие одну компоненту деревья 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 сопряжающая перестановка (2, 3) нечетна.

По подобное “сопряжение” нечетной перестановки в группе четных перестановок трех элементов, так как сопряжающая перестановка (2, 3) нечетна.

Однородность оснащения сохраняется и для всех конечных групп.

Я не знаю, насколько алгебраическая перекомпоновка коого произведения группы $1 \to H \to E \to G \to 1$ сказывается на топологической перекомпоновки графа группы-“произведения” $E$ по сравнению с произведением графов группы-“сомножителей” $G$ и $H$ (даже для случая двулистных накрытий, когда $H = \mathbb{Z}_2$, или подгруппы $H$ ин-
Топология и статистика формул арифметики

дека 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:
\[
[\text{граф } (SL(2, \mathbb{Z}_6))] = T + (O_2 \cdot R) + 4(O_2 \cdot E_5) + 8A_2,
\]
где дерево \( T \) имеет суммы рангов \( s = (1, 8, 32) \), а дерево \( R \) - суммы рангов \( s = (1, 2, 8) \).

Явно 16 матриц, составляющих граф \( O_2 \cdot R \), таковы:

\[
\begin{array}{cccc}
15 & 51 & 55 & 21 \\
52 & 14 & 54 & 11 \\
23 & 13 & 43 & 53 \\
35 & 34 & 31 & 52 \\
11 & 12 & 31 & 05 \\
12 & 50 & 35 & 13 \\
31 & 10 & 55 & 01 \\
13 & 53 & 45 & 55 \\
\end{array}
\]

В этой компоненте спиральность оснановника цикла деревьев объясняется (внешним) автоморфизмом, сохраняющим 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 значениями \( a + d \) в каждой компоненте таковы:

<table>
<thead>
<tr>
<th>( a + d )</th>
<th>( T )</th>
<th>( O_2 \cdot R )</th>
<th>( 4(O_2 \cdot E_5) )</th>
<th>( 8A_2 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>24</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>8 \cdot 2</td>
</tr>
<tr>
<td>2</td>
<td>3 + 1</td>
<td>0</td>
<td>3 \cdot (6 + 2) + 6</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>12</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>3 + 1</td>
<td>0</td>
<td>3 \cdot 8 + (8 + 2)</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>8 \cdot 2</td>
</tr>
</tbody>
</table>

Обозначения в роли \( 3 + 1 \) в графе \( (2, T) \) обозначает, что 4 точки графа \( T \), в которых \( a + d \equiv 2 \), подразделяются на два класса, один из 3 элеметов, а другой из 1 элемета, которые занимают в дереве \( T \) неизоморфные места (в рассматриваемом примере эти матрицы
\[
\left\{ \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix}, \begin{pmatrix} 4 & 3 \\ 3 & 4 \end{pmatrix} \right\}
\]
удачны от корня на расстояния 1 и 0).

Было бы интересно связать эти структуры графов монад груп с действиями на эти группы обычных и внутренних автоморфизмов, а также включающих их монадоморфизмов: образуют ли автоморфизм или внутренние автоморфизмы перекрестные дивити в групах монадоморфизмов (и каковы фактор-группы в случае положительного ответа?)
§ 6. Однородность монад всех конечных групп

Монадоморфизмам и образуемыми групами и категориями 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 притягивающее циклом в вершине $a$ дерево в дерево, притягивающее циклом в его следующей вершине, $a^2$.

Определение. Вершина имеет ранге $r$, если она отделена от притягивающего цикла $r$ ребрами.

Пример. Вершины притягивающего цикла имеют ранг нуль.
Рассмотрим притягивающий цикл периода $T$ образованный вершинами $\{a, a^2, a^4, \ldots, a^{2^{T-1}}\}$ (следующая вершина цикла — опять $a$). В этом случае выполняется условие периодичности

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

Определение. Назовем связностью компоненты, притягивающей циклом периода $T$, отображение $P$, переводящее каждую вершину $b$ ранга $t$ в вершину $Pb = b^r$, где $r = (2^T - 1)S + 2$.

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

Из условия периодичности $a^S = 1$ вытекает соотношение

$$b_1^{S+2} = 1, \quad b_2^{S+2} = 1, \quad \ldots, \quad b_r^{S+2} = 1$$

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:

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

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 вершину $c = b^2$ и $c' = (b')^2$ также различим.

Доказательство. Если $r > 0$, то число $x = 2k + 1$ нечетно. В этом случае имеют место тождества
$$c = b(b^2)^k, \quad c' = b'(b^2)^k,$$
поскольку 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 вершин $c$ равен 1).

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

Различных таких степеней $T$, но соотношения
$$(Pb)^2 = P(b^2) = P(a) = a^2$$
приведи бы к выводу $Pb = a$, т.е. $b^{s+2} = b^2$. Последнее равенство означало бы, что $b^{s+2} = b^2$, что и означало бы место соотношения
$$b = b^{T-1} = a^{T-1}$$
и ранг вершины $b$ был бы равен нулю, а не 1.

Полученное противоречие доказывает лемму 3.

Лемма 4. Связность изоморфно отображает дерево, притягивающее вершину $a$ цикла, на дерево, притягивающее следующей вершиной $a^2$ (связность, в частности, ранге вершин).

Доказательство. Обозначим через $n_i$ число вершин деревьев, притягивающих вершиной $a_i$ притягивающего цикла
$$\{a_0 = a, a_1 = a^2, \ldots, a_i = a^{2i}, \ldots\} \quad (i = 0, 1, \ldots, T - 1).$$

Изоморфизм в последующие деревья, обсуждавшиеся в леммах 1–3, доказывают непрерывность вершин от $n_0 \leq n_1 \leq \cdots \leq n_T$.

Из $T$-периодичности цикла следует, что $n_T = n_0$, так что все числа периодической последовательности $n_i$ равны, а все притягивающие вершины цикла $a_i$ изоморфны, что и доказывает лемму 4 (а следуя и теоремой 4).

Замечание. Наряду с определённой выше специальной связностью можно рассматривать и другие связи, определяя их как моноидеризоморфизмы компоненты, сводящие их к единице.

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

Определение. Моноидеризоморфизм $M$ называется моноидером (композитом периода $T$).

Монодромия действует тривиально на нижних этажах деревьев (где $T \leq 1$), но на высших этажах может быть нетривиальной (и, возможно, позволяет определить интересные инварианты группы).
§ 7. Медулярная топология кубов Кеплера

В своей книге "Гармония Мира" Кеплер описал радиусы панцирных орбит в терминах пирамидальных дуг вдруг правильных многогранников, а для этого вписал в куб однопятигранный куб. Ребра этих кубов — это диагональ двери, первой граневой докеаэдра (по одному ребру на каждую грань).

Эти кубы Кеплера автоматически возникают при описании геометрии монады возможного квадрата группы $G = SL(2, Z_5)$, состоящей из 120 компонент. Этот граф имеет 17 компонент:

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

Сейчас мы построим по нему риманову поверхность.

Корневое дерево $T$ имеет 32 вершины; вершину $(0, 0, -4)$ на первом этаже и 30 вершин с периодом 4 (так что $c^4 = 1$) на втором этаже, так что набор рангов имеет вид $r(T) = (1, 1, 30)$ (учитывая корневую вершину 1 на нулевом этаже).

Периоды точек компонент $A_4$ равны 5 (для вершин на протирагивающих циклах) и 10 (для вершин единственного первого этажа описывающих дверь). Типичные примеры — элементы $\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$ 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 протирагивающих циклах) и 6 (для вершин единственного первого этажа описывающих дверь). Типичные примеры — элементы $\begin{pmatrix} 1 & 1 \\ 4 & 0 \end{pmatrix}$ периода 6 и его квадрат $\begin{pmatrix} 0 & 1 \\ 4 & 4 \end{pmatrix}$ периода 3.

**Теорема 5.** Группа $G = SL(2, Z_5)$ действует на конечной проективной прямой $\mathbb{P} = P^1(Z_5)$ как некоторая специальная группа 60 четных перестановок шести точек этой конечной прямой.

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

Соединим каждую грань с противоположной отрезком, соединяющим их центры. Группа симметрии докеаэдра переставляет эти 6 прямих. Чтобы описать подгруппу из 60 специальных четных перестановок (что составляет половину 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 докеаэдра. В конце этой диагонали сходятся с рассматриваемой еще две грани, и на них тоже надо выбрать по одной из всех этих точек диагонали.

Для этого достаточно повернуть докеаэдр вокруг этой конечной 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 выбираем вначале из исходной грани. Так что конструкция Кеплера дает пять кубов, вписанных в додекаэдр.

Нужно найти 60 специальных перестановок шести элементов, реализуемых действием группы $SL(2, Z_5)$ на конечной проективной прямой $\mathbb{P}$, описываются в этих терминах как 60 вариаций додекаэдра, составляющих подчиненную группу его симметрий. Они реализуют все 60 членов перестановок пяти кубов Кеплера. Поэтому проективная группа конечной проективной прямой $\mathbb{P}$ (состоящей из 6 точек) изоморфна группе $S^+(5)$ членов перестановок пяти элементов (а именно, пяти кубов Кеплера):

$$(G = SL(2, Z_5))/\{\pm 1\} \simeq S^+(5).$$

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, матрицы группы $G$ имеют центр $\{\pm 1\}$, состоящий из двух элементов, в то время как центр группы перестановок тривиален.

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

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

Для группы $G$ ранги держав 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, и $15$ не равно $0$.

Аналогичным образом доказывается нетривиальность расслоения $G \to G/K$ для группы $SL(2, Z_p)$, $p > 5$.

В терминах перестановок точек конечной проективной прямой компоненты графа монодромии возврата в квадрат для группы $G = SL(2, Z_5)$ могут быть описаны диаграммами Юнга специальных членов перестановок кубов Кеплера, а именно:

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

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

Геометрически компонента $A_1$ представляет четырех нетривиальных вращениях додекаэдра, сохраняющих 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 тождественными преобразованиями (реализуемыми этажа $T_0$ 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 представляет \( p + 1 \) точку конечной проективной прямой
\[
P = P^1(\mathbb{Z}_p).
\]

**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 образующих 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 вершины точек конечной проективной прямой \( P \).

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

Этот многогранник связан с особенностью \( K_{12} \), голографической 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 подобного изучения.

Сохраняя ими проективная структура на множестве \( p + 1 \) 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 структура 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 (каждая специальная перестановка зависит от структуры).

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

Каждая из этих 120 структур сохраняется специальными четными перестановками \( p + 1 = 8 \) точек конечной проективной прямой, число таких 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 оказывается уже некоторая риманова поверхность, а аналоги кубов Кеплера соответствуют подгруппы Гамильтона.
§ 8. Кеплеровы кубы и подгруппы Гамильтона

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

Кубы Кеплера, вписанные в додекаэдр, и их \( K_{12} \)-объединения, 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 сектетов, каждый из которых образует, вместе с элеметами 1 и \(-1\) нудового 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 сектет, 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 формулированных выше свойств сектетов достаточно проверить их в одном примере, например, для сектета \( \{\pm r, \pm s, \pm t\} \), где

\[
\begin{align*}
    r &= \begin{pmatrix} 0 & 1 \\ 4 & 0 \end{pmatrix}, \\
    s &= \begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix}, \\
    t &= \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix},
\end{align*}
\]

вычислив сопряжения, сохраняющие этот сектет.

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

60 сопряженных к двумюному сектету доставляют 60/12 = 5 разных сектетов (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 сектетов I—IV (выписаны только три элемента каждого сектета, остальные три — это \( -r, -s, -t \)):

<table>
<thead>
<tr>
<th>Сектет</th>
<th>I</th>
<th>II</th>
<th>III</th>
<th>IV</th>
<th>V</th>
</tr>
</thead>
<tbody>
<tr>
<td>( r )</td>
<td>01</td>
<td>11</td>
<td>20</td>
<td>13</td>
<td>14</td>
</tr>
<tr>
<td></td>
<td>40</td>
<td>34</td>
<td>33</td>
<td>14</td>
<td>24</td>
</tr>
<tr>
<td>( s )</td>
<td>02</td>
<td>20</td>
<td>12</td>
<td>20</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>20</td>
<td>13</td>
<td>44</td>
<td>23</td>
<td>43</td>
</tr>
<tr>
<td>( t = rs )</td>
<td>20</td>
<td>33</td>
<td>24</td>
<td>34</td>
<td>32</td>
</tr>
<tr>
<td></td>
<td>02</td>
<td>03</td>
<td>02</td>
<td>02</td>
<td></td>
</tr>
</tbody>
</table>
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 посередине $A$ 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 посередине $A$: $AH A^{-1} = H$.

Определение. Эти 8 элементов третьего порядка являются восьмью вершинами куба Кеплера, связанного с выбранной подгруппой Гамильтона, $H$.

Описанное выше число формирует следующие четверки вершин $(a, b, c, d)$ кубов Кеплера (остальные четыре элементы группы $G$ – это обратные им элементы, т.е. $(a^2, b^2, c^2, d^2)$):

<table>
<thead>
<tr>
<th>секстет</th>
<th>I</th>
<th>II</th>
<th>III</th>
<th>IV</th>
<th>V</th>
</tr>
</thead>
<tbody>
<tr>
<td>$a$</td>
<td>12</td>
<td>04</td>
<td>04</td>
<td>44</td>
<td>44</td>
</tr>
<tr>
<td></td>
<td>13</td>
<td>14</td>
<td>14</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>$b$</td>
<td>32</td>
<td>02</td>
<td>03</td>
<td>02</td>
<td>03</td>
</tr>
<tr>
<td></td>
<td>11</td>
<td>24</td>
<td>34</td>
<td>24</td>
<td>34</td>
</tr>
<tr>
<td>$c$</td>
<td>34</td>
<td>32</td>
<td>34</td>
<td>14</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td>31</td>
<td>11</td>
<td>37</td>
<td>33</td>
<td>13</td>
</tr>
<tr>
<td>$d$</td>
<td>14</td>
<td>24</td>
<td>23</td>
<td>23</td>
<td>24</td>
</tr>
<tr>
<td></td>
<td>33</td>
<td>22</td>
<td>12</td>
<td>12</td>
<td>22</td>
</tr>
</tbody>
</table>

Каждая из десяти вершин кубов Кеплера, указанных в таблице, встречается в ней дважды, и через каждую вершину куба Кеплера проходит ровно два куба, расположенные в разных плоскостях, грань которых содержит вершину, и все 20 вершин куба Кеплера (являющихся разными вершинами), то есть в плоскости каждой гранью третьего порядка в группе $G$.

Вершины кубов Кеплера можно легко вычислить, 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 (упорядоченность в соответствии с этой 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 граней 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.
ТОПОЛОГИЯ И СТАТИСТИКА ФОРМУЛ АРИФМЕТИКИ

Другое описание того же самой соответствия между подгруппами Гамильтона и кубами Кеплера таковы:

четыре вершины куба Кеплера получается из одной из них (см.жем, из $A$), содержащей все элементы подгруппы Гамильтона, $\{A, rAr^{-1}, sAs^{-1}, tAt^{-1}\}$ ($r$ сопряжает такое же, как $t$).

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

Продолжение построение вершина куба Кеплера по элементам подгруппы Гамильтона продолжает отображение

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

принимая вполне определенный смысл матриц $A^*, A^a, A^t$.

Возвращаясь к поверхности додекаэдра, мы можем подумать ее из комбинации группы $G_5$, выбранной в качестве вершины 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 возникает здесь на соотношение между правильным пятиугольником и пятиугольником звездой с теми же вершинами.

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

Сами симметрии определяют такие перестановки, но, кроме того, есть еще и фундаментальная симметрическая перестановка (с точностью до симметрий — только одна).

Эта фундаментальная симметрическая перестановка вершина как раз и преобразует 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, определяющей 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 вершина до графа. Выходящие из одной вершины 3 ребра циклически переставляются сопряжением посредством этой вершины, и с подобными циклическим порядком выходящих из каждой вершины ребер подобный граф оказывается плоским. Он делит плоскость, или сферу $S^2$, в которую вложена, на пятиугольники. Это и составляет основной додекаэдр.

Было бы интересно узнать, насколько эта конструкция распространяется на другие группы $G$ (например, достаточно ли она столь же гладкой и ли даже гладкой, как в случае $G = SL(2, \mathbb{Z}_p)$, поверхности в случаях $SL(2, \mathbb{Z}_m)$ или в случае $GL(2, \mathbb{C}\mathbb{Z}_p)$ 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 переносении додекаэдральных исследований на случай группы \( G = SL(2, \mathbb{Z}) \) получаются следующие выводы.

Теорема 7. В части \( T_0 + T_1 + T_2 \) дерева монады возведения в квадрат в группе \( G \) имеется 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, \( GL(2, \mathbb{Z}) \).

Образующие \((r, s)\) семь из подгрупп Гамильтона и их произведения \( t = rs \) табуны:

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

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 составляют 6 · 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 четрех красок следующей конструющей.

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, разбивающего его на 7 шестиугольников, встречающихся по 3 в 14 вершинах. Каждый шестиугольник имеет обущую сторону с каждой из остальных. Поэтому получающийся на торе карты из 7 стран не может быть правильно раскрашена меньше, чем семью красками. Семь подгрупп, сопряженных с подгруппой \( A \), обозначены ниже окружающими.

Покрытие топой семьей шестиугольниками получается из правильно шестиугольника на евклидовой плоскости \( \mathbb{R}^2 \). Объединение этой шестиугольной области с шестью ее отражениями в сторонах покрывает плоский многогранник, являющийся фундаментальной областью группы \( \mathbb{Z}^2 \) правильных параллелограммов, сохраняющих разбиение плоскости на конгруэнтные шестиугольники. Фактор-тор \( T^2 = \mathbb{R}^2 / \mathbb{Z}^2 \) разбит, как указывало выше, на 7 шестиугольных областей (группа параллелограммных параллелограмм векторами \( AA' \) и \( AA'' \)).
Изоморфность узора пересечений четырехлапчатых сегжетов с этим торическим графом проверяется прямым (хотя и утомительным) вычислением 84 матриц \( \{ \pm r, \pm s, \pm t \} \).

Построение кубов Кеплера из этих 14 подгрупп Гамильтона повторяет проведенную выше \( SL(2, \mathbb{Z}_2) \)-конструкцию и дает 14 кубов Кеплера, из которых 7 соединяют одному из них, а 7 — другому; сопряжения действуют на каждом кубе как его вращение.

Все эти кубы можно было бы нарисовать на обобщенной 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.

Вершины поверхности \( M \) являются элементами третьего порядка в группе \( G \), a грани определяются элементами порядка 14, \( c = ab \), где \( c^2 = -1, a^3 = b^5 = 1 \).

Вместо поверхности \( M \) удобно рисовать ее фактор-поверхность, определенную следующим "складыванием".

Оторажение, сопоставляющее каждой матрице \( A \) трансформированную обратную матрицу \( \bar{A} \), является автоморфизмом группы \( SL(2, \mathbb{Z}) \) (в именуемом, сопряжением посредством матрицы \( \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \)). Этот автоматоморфизм переводит элементы третьего (и четырехлапчатого) порядка в элементы третьего (соответственно, четырехлапчатого) порядка, и поэтому действует на поверхности \( M \).

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

Оторажение \( M \rightarrow M' \) является двудесятным разветвленным нарастанием 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, перечисленных ниже, и 28 их квадратов, \( i = (i) \) (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

<table>
<thead>
<tr>
<th>i</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>40</td>
<td>21</td>
<td>22</td>
<td>23</td>
<td>24</td>
<td>25</td>
<td>26</td>
<td>20</td>
<td>20</td>
<td>20</td>
<td>20</td>
<td>20</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>02</td>
<td>04</td>
<td>04</td>
<td>04</td>
<td>04</td>
<td>04</td>
<td>04</td>
<td>04</td>
<td>04</td>
<td>04</td>
<td>04</td>
<td>04</td>
<td>04</td>
</tr>
<tr>
<td></td>
<td>15</td>
<td>16</td>
<td>17</td>
<td>18</td>
<td>19</td>
<td>20</td>
<td>21</td>
<td>22</td>
<td>23</td>
<td>24</td>
<td>25</td>
<td>26</td>
<td>27</td>
</tr>
<tr>
<td></td>
<td>01</td>
<td>06</td>
<td>04</td>
<td>05</td>
<td>03</td>
<td>02</td>
<td>31</td>
<td>34</td>
<td>32</td>
<td>14</td>
<td>11</td>
<td>13</td>
<td>16</td>
</tr>
<tr>
<td></td>
<td>66</td>
<td>16</td>
<td>56</td>
<td>46</td>
<td>26</td>
<td>36</td>
<td>13</td>
<td>23</td>
<td>43</td>
<td>15</td>
<td>45</td>
<td>65</td>
<td>35</td>
</tr>
<tr>
<td></td>
<td>74</td>
<td>55</td>
<td>55</td>
<td>55</td>
<td>55</td>
<td>55</td>
<td>55</td>
<td>55</td>
<td>55</td>
<td>55</td>
<td>55</td>
<td>55</td>
<td>55</td>
</tr>
</tbody>
</table>

На рисунке показаны 12 сечиугольных граней фундаментальной области поверхности $M'$ на $M$ и их соседи, складывание состоит в склейке $A$ с $A$ вдоль ограничивающей фундаментальную область жирной линии. Точки вставления складывания
Рис. 2. Усредненная зависимость периода от модуля в билогарифическом масштабе

Рис. 3. Билогарифмический график Кольцерова, приведший к открытию закона 5/3 теории турбулентности
$M \rightarrow M'$ — это центральные точки отрезков $(A, A)$, где отрезки суть $(3, 11)$ в области X1, $(23, 22)$ в области I, $(6, 9)$ в области X11 и $(15, 16)$ в области V.

Структуры поверхности $M$ и $M'$ были 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 и наименьшего периода $T(n)$ арифметической прогрессии

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

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

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

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

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

Рис. 2 является теоретико-числовым аналогом приема Кодоморова, с помощью которого он открыл "законы 5/3" теории турбулентности. Оригинальный график Кодоморова воспроизведен на рис. 3.

СПИСОК ЛИТЕРАТУРЫ


Математический институт им. В. А. Стеклова РАН

Поступила в редакцию 05.01.2003