12 июня 2007 года выдающемуся математику современности академику
Владимиру Игоревичу Арнольду исполнилось 70 лет.
На протяжении многих лет В.И.Арнольд является членом редакционного совета журнала «Квант».
Он написал для нашего журнала много ярких, интересных статей.
Мы желаем Владимиру Игоревичу крепкого здоровья
и новых достижений во имя науки.

Современная математика, восходящая к Эйлеру

В.АРНОЛЬД

§1. Дзета-функция Эйлера и малая теорема Ферма

Дроби бывают сократимые и несократимые. Сопоставим дроби p/q точку r на плоскости с декартовыми координатами (p,q). Если дробь сократима, то эта целая точка *делима*: на отрезке, соединяющем r с началом координат, есть и другие целые точки.

Нарисуем все неделимые целые точки в круге $p^2+q^2 \le 5^2$ (рис.1; начало координат будем считать делимой точкой, так как ноль делится нацело на что угодно). Неделимых точек в этом круге 48, а всего в нем 81 целая точка. Неделимые точки составляют $48/81 \approx 59\%$ от числа всех целых точек в этом круге.

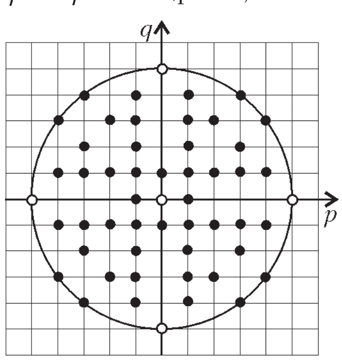


Рис.1. Неделимые целые точки в круге радиуса 5

Эйлер задал себе вопрос: а что будет, если увеличивать радиус круга? Будет ли доля неделимых целых точек стремиться при этом к какому-нибудь пределу, и к какому именно?

Он решил этот вопрос, доказав следующее:

Теорема Эйлера 1. *Доля неделимых целых точек среди всех целых точек круга $p^2+q^2 \le R^2$ стремится при $R \to \infty$ к пределу, который равен*

$$\frac{6}{\pi^2} \approx 0{,}608\ldots \tag{1}$$

Этот предел Эйлер выразил еще одной замечательной формулой:

$$\frac{\pi^2}{6} = 1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \ldots \tag{2}$$

Заметьте, что $\pi^2/6 \approx 1{,}64$, так что сумма первых двух членов (1,25) еще далека от суммы этого не так уж быстро сходящегося ряда.

Определение. Сумма ряда (сходящегося при $s > 1$)

$$\frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \ldots = \zeta(s) \tag{3}$$

называется значением в точке s *дзета-функции* ζ.

Таким образом, теорема Эйлера выражает предельную долю неделимых целых точек плоскости $\mathbb{R}^2$ (называемую также «вероятностью несократимости дроби p/q») формулой

$$(\text{вероятность неделимости вектора } \boldsymbol{r} \in \mathbb{R}^2) = \frac{1}{\zeta(2)}. \tag{4}$$

Его доказательство доставляет также и аналогичный результат о целых точках s-мерного пространства $\mathbb{R}^s$:

$$(\text{вероятность неделимости вектора } \boldsymbol{r} \in \mathbb{R}^s) = \frac{1}{\zeta(s)}. \tag{5}$$

Например, эта вероятность убывает при росте размерности s.

Доказательство приведенный выше теоремы Эйлера (и формул (2), (4), (5)) содержит ряд замечательных идей Эйлера, которые привели к созданию целых областей современной математики – вероятностной теории чисел, теории градуированных алгебр с их рядами Пуанкаре, «геометрии чисел» и т.д.

Но Эйлер начинал с совершенно понятных и элементарных рассуждений, которые я сейчас и опишу.

Лемма 1. *Целочисленный вектор является делимым, если и только если существует простое число p, на которое делится каждая его компонента.*

Доказательство. Делимость на произведение простых множителей вызывает делимость на каждый из них. Поэтому лемма 1 вытекает из разложимости каждого (большего 1) целого числа на простые множители.

Лемма 2. *Вероятность делимости целочисленного вектора $\boldsymbol{r} \in \mathbb{R}^2$ на 2 равна $1/4$.*

Доказательство. Для делимости вектора с компонентами u и v на 2 необходима и достаточна делимость на 2 как целого числа u, так и целого числа v. Каждое из этих событий имеет вероятность $1/2$, и они независимы. Поэтому делящиеся на 2 целочисленные векторы составляют 25% всех целочисленных векторов плоскости.

Лемма 3. *Вероятность делимости целочисленного вектора* $\boldsymbol{r} \in \mathbb{R}^s$ *на* p *равна* $1/p^s$.

Доказательство. Вероятность делимости целого числа u на p равна $1/p$ (так как арифметическая прогрессия с разностью p составляет при большом R почти $(1/p)$-ю часть отрезка $|u| \le R$). Так как s компонент $(u_1,\dots,u_s)$ вектора $\boldsymbol{r}$ независимы, вероятность делимости вектора на p равна произведению вероятностей делимости на p всех s его компонент, т.е. равна $(1/p)^s$.

Лемма 4. *Вероятность неделимости вектора* $\boldsymbol{r} \in \mathbb{R}^s$ *на* p *равна* $1-\dfrac{1}{p^s}$.

Доказательство. Вектор $\boldsymbol{r}$ либо делится на p, либо не делится. Зная вероятность делимости из леммы 3, получаем для неделимости дополняющую до 1 вероятность.

Лемма 5. *Делимости на разные простые числа – события независимые.*

Например, доля делящихся на 3 целых чисел среди всех четных чисел такая же, как и среди всех целых чисел (или среди всех нечетных чисел), – она составляет $1/3$. Это видно из того, что среди p_2 остатков $(1p_1)\dots(p_2p_1)$ от деления на простое число p_2 встречаются по разу все остатки $(1,\dots,p_2)$ (каково бы ни было простое число p_1). Ибо, если бы числа ip_1 и jp_1 (где $1 \le i < j \le p_2$) давали при делении на p_2 одинаковые остатки, то разность $(j-i)p_1$ делилась бы на p_2, что при $0 < j-i < p_2$ невозможно.

Лемма 6. *Вероятность неделимости целочисленного вектора* $\boldsymbol{r} \in \mathbb{R}^s$ *(* $s > 1$*) на простые числа 2, 3, … …, p равна*

$$\left(1-\frac{1}{2^s}\right)\left(1-\frac{1}{3^s}\right)\dots\left(1-\frac{1}{p^s}\right).$$

Доказательство. Вероятность одновременного наступления независимых событий равна произведению вероятностей наступления каждого из них. Поэтому лемма 6 вытекает из лемм 4 и 5.

Лемма 7. *Вероятность неделимости целочисленного вектора* $\boldsymbol{r} \in \mathbb{R}^s$ *(*$s > 1$*) ни на какое целое число равна бесконечному произведению по всем простым числам p*

$$(6)\quad \prod_p\left(1-\frac{1}{p^s}\right) := \lim_{p\to\infty}\left[\left(1-\frac{1}{2^s}\right)\left(1-\frac{1}{3^s}\right)\dots\left(1-\frac{1}{p^s}\right)\right].$$

Это – прямое следствие лемм 1 и 6, нужно только проверить, что указанный в формуле (6) предел существует (при $s > 1$). Эта сходимость легко выводится из сходимости при $n > 1$ ряда

$$\frac{1}{1^s}+\frac{1}{2^s}+\frac{1}{3^s}+\frac{1}{4^s}+\dots$$

(или даже интеграла $\int_1^\infty \frac{dx}{x^s} = \frac{1}{s-1}$).

Детали доказательства леммы 7 я оставляю читателю.

Приведенные леммы Эйлера доставляют для вероятности несократимости выражение (6). Эйлер сумел получить для него и формулы (1), (2), (4), (5). Этот вывод основан на совершенно других идеях Эйлера (которые включены в современную математику под названием «теории рядов Пуанкаре градуированных алгебр»).

Начнем со следующих элементарных замечаний, помещенных Эйлером в его замечательном учебнике «Введение в анализ» (содержащем естественно предшествующие анализу положения, которые, к сожалению, в современных изложениях анализа обычно отсутствуют).

Степенью одночлена $x_1^{m_1}x_2^{m_2}\dots x_s^{m_s}$ от s переменных $(x_1,\dots,x_s)$ называется целое число $m = m_1+\dots+m_s$.

Например, при $s = 2$ имеется 4 одночлена степени 3 (с коэффициентом единица):

$$\{x^3, x^2y, xy^2, y^3\}$$

(если обозначать x_1 через x и x_2 через y).

Эйлер поставил вопрос: *сколько существует одночленов (с коэффициентом единица) степени m от s переменных*?

Эта задача элементарной комбинаторики допускает простое комбинаторное решение, но Эйлер придумал еще и другое рассуждение, доставляющее гораздо больше следствий.

Начнем с одночленов $(1, x, x^2, x^3, \dots)$ от одной переменной x. В этом случае имеется ровно один (считая коэффициент одночлена равным 1) одночлен любой степени $m = 0, 1, 2, \dots$ Чтобы записать ответ: «число (каких-либо объектов, зависящих от натурального числа m) ровно p_m», Эйлер использует «производящую функцию» (сегодня называемую «рядом Пуанкаре», по следовавшему за Эйлером великому французскому математику):

$$(7)\qquad P(t) = p_0 + p_1t + p_2t^2 + \dots$$

В этих терминах предыдущий ответ на вопрос о числе одночленов от одной переменной записывается так:

Предложение 1. *Ряд Пуанкаре градуированной степенью алгебры многочленов от одной переменной есть рациональная функция*

$$(8)\qquad P(t) = 1+t+t^2+\dots = \frac{1}{1-t}.$$

Чтобы вывести отсюда формулу для числа многочленов от двух переменных, Эйлер предложил перемножить два ряда вида (8):

$$(9)\quad P(x)P(y) = \left(1+x+x^2+\dots\right)\left(1+y+y^2+\dots\right) = 1+(x+y)+\left(x^2+xy+y^2\right)+\dots$$

В стоящем в правой части формулы (9) ряду каждый одночлен (с коэффициентом 1) от переменных x и y встречается ровно однажды. Поэтому, если заменить аргументы x и y на t, в правой части получится ряд, в котором коэффициент при t^m будет равен числу P_n одночленов степени m (с равными 1 коэффициентами) от переменных x и y.

Таким образом, мы получаем из формул (8) и (9) для ряда Пуанкаре градуированной степенью алгебры многочленов от двух переменных

$$P_0 + P_1 t + P_2 t^2 + \ldots$$

выражение

$$P(t) = \frac{1}{(1-t)^2}.$$

Совершенно так же Эйлер доказал следующее:

Предложение 2. *Ряд Пуанкаре градуированной степенью алгебры многочленов от s переменных является рациональной функцией*

$$P(t) = \frac{1}{(1-t)^s}.$$

Явное выражение для чисел P_m (в виде чисел сочетаний) получается отсюда по формуле бинома Ньютона (с показателем $-n$).

Вдохновляясь этими результатами абстрактной алгебры, Эйлер преобразовал доказанную им формулу (6) (леммы 7)) следующим образом. Заменим множитель $\left(1 - \frac{1}{p^s}\right)$ на обратный множитель

$$\left(1 - \frac{1}{p^s}\right)^{-1} = 1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \frac{1}{p^{3s}} + \ldots$$

При (формальном) перемножении таких рядов, соответствующих всем простым числам p, мы получим ряд, общий член которого имеет вид

$$\frac{1}{2^{a_2 s}} \cdot \frac{1}{3^{a_3 s}} \cdot \frac{1}{5^{a_5 s}} \cdot \ldots = \frac{1}{n^s}, \text{ где } n = 2^{a_2} \cdot 3^{a_3} \cdot 5^{a_5} \cdot \ldots$$

Тем самым доказана (для формальных рядов, по проверке сходимости при $s > 1$ несложная) замечательная формула Эйлера для ζ-функции:

Теорема Эйлера 2. *Следующее произведение по простым p равно (при s > 1) следующей сумме по натуральным n*

$$\prod_{p \ge 2} \frac{1}{1 - \frac{1}{p^s}} = \sum_{n \ge 1} \frac{1}{n^s} \quad (:= \zeta(s)).$$

Так Эйлер получил формулы (4) и (5).

Вычисление значений ζ-функции при фиксированном значении аргумента s не просто, но значение $\zeta(2) = \pi^2/6$ Эйлер умел получать разными способами.

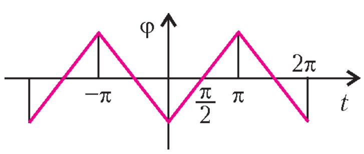


Рис.2. «Пила» f

«Пила» f задается как 2π-периодическая функция аргумента t, равная $|t| - \frac{\pi}{2}$ при $|t| \le \pi$ (рис.2). Ищем разложение в ряд Фурье

$$f(t) = \sum_{k=1}^{\infty} a_k \cos(kt),$$

при четных k получаем $a_k = 0$, а при нечетных – $a_k = \left(-\frac{4}{\pi}\right)\frac{1}{k^2}$. Вычисляя $f(0)$ при помощи (сходящегося) ряда Фурье, мы находим

$$-\frac{\pi}{2} = f(0) = -\frac{4}{\pi} \sum_{m=0}^{\infty} \frac{1}{(2m+1)^2},$$

так что сумма обратных квадратов нечетных чисел есть

$$A = \sum_{m=0}^{\infty} \frac{1}{(2m+1)^2} = \frac{\pi^2}{8}.$$

Вводя обозначение B для

$$\zeta(2) = \sum_{m=0}^{\infty} \frac{1}{(2m+1)^2} + \sum_{m=1}^{\infty} \frac{1}{(2m)^2},$$

мы получаем $B = A + B/4$, откуда $\zeta(2) = B = \frac{4}{3}A = \frac{\pi^2}{6}$, что и доказывает теорему Эйлера 2.

Замечание: о равномерном распределении неделимых точек

Я предполагаю, что распределение неделимых целых точек на плоскости обладает некоторой асимптотической равномерностью (резко отличающей его от, например, набора целых точек полуплоскости, составляющего половину множества всех целых точек плоскости, но распределенную неравномерно).

Чтобы определить эту равномерность распределения, начнем, например, с (любой) гладкой функции $h: \mathbb{R}^2 \to \mathbb{R}$, равной нулю всюду вне некоторого круга. Растягивая функцию h в K раз, определим новую функцию $H: \mathbb{R}^2 \to \mathbb{R}$ соотношением $H(\boldsymbol{r}_0 + \boldsymbol{r}) = h(\boldsymbol{r}/K)$ для всякого $\boldsymbol{r} \in \mathbb{R}^2$ (где $\boldsymbol{r}_0$ – некоторый фиксированный вектор). Сравним теперь сумму значений растянутой функции H во всех целых точках плоскости, обозначим эту сумму через SH, и сумму значений той же растянутой функции H во всех неделимых целых точках плоскости, обозначим эту сумму через ΣH.

Свойство равномерной распределенности состоит в том, что при больших K вторая сумма составляет приблизительно такую долю первой, какую долю составляют изучаемые (неделимые) точки среди всех целых точек, $\lambda = 6/\pi^2 = 1/\zeta(2)$:

$$\lim_{K \to \infty} \frac{\Sigma H}{SH} = \lambda$$

(при любом векторе $\boldsymbol{r}_0$, сдвигавшем функцию H).

Если бы суммирование в Σ происходило не по равномерно распределенным на плоскости неделимым точкам, а, например, по целым точкам полуплоскости, то функции h и H могли бы быть тождественно равными 0 в этой полуплоскости. Тогда $(\Sigma H)/(SH) = 0$, хотя целые точки полуплоскости составляют долю $\lambda = 1/2$ от всех целых точек плоскости, так что целые точки полуплоскости распределены среди всех целых точек плоскости неравномерно.

Традиция приписывает изобретение дзета-функции Риману, жившему на сотню лет позже описанной выше работы Эйлера. Фурье тоже жил много позже Эйлера (но его ряды использовались задолго до него и Эйлером, и Лагранжем, и даже Ньютоном). Ньютон считал изобретение метода «параллелограмма Ньютона» (доставляющего своеобразный вариант теории преобразования Фурье, рядов Лорана и рядов Пюизо) своим самым важным вкладом в математику, позволяющим решать всевозможные уравнения: алгебраические и функциональные, дифференциальные и интегральные, обыкновенные и в частных производных.

В современном университетском образовании все эти важнейшие теории обычно не упоминаются, и даже работа Эйлера о дзета-функции незаслуженно забыта.

Сделанный Эйлером подсчет вероятности несократимости дробей доставляет также асимптотику замечательной *функции Эйлера* φ натурального аргумента n:

n	1	2	3	4	5	6	7	8	9	10	11	12
φ	1	1	2	2	4	2	6	4	6	4	10	4

Определяется значение $\varphi(n)$ так: оно равно числу тех из остатков $\{1, 2, \ldots, n\}$ от деления на n, каждый из которых взаимно прост с n (так что его наибольший общий делитель с n равен 1).

Пример. Четыре взаимно простых с $n = 12$ остатка от деления на 12 – это $\{1, 5, 7, 11\}$. Для простого числа, $n = p$, имеем, очевидно,

$$\varphi(p) = p - 1.$$

Для квадрата простого числа, $n = p^2$, не взаимно простых с n остатков имеется p, поэтому

$$\varphi\left(p^2\right) = p^2 - p = (p-1)p.$$

Точно так же, для $n = p^a$ получаем

$$\varphi\left(p^a\right) = (p-1)p^{a-1}$$

(из-за p^{a-1} делящихся на p остатков).

Если $n = ab$ – произведение двух взаимно простых чисел, то функция Эйлера, очевидно, мультипликативна,

$$\varphi(ab) = \varphi(a)\varphi(b).$$

Все это дает явную формулу для значения $\varphi(n)$, если разложение n на простые множители известно.

Но приведенная выше таблица показывает, что функция φ сильно осциллирует при изменении значения аргумента: то растет, то убывает (до малой доли значения аргумента).

Теорема Эйлера 3. *Среднее арифметическое значений функции Эйлера* φ,

$$\hat{\varphi}(n) = \frac{\varphi(1) + \varphi(2) + \ldots + \varphi(n)}{n},$$

ведет себя при $n \to \infty$ *как* cn, *где постоянная* c *есть*

$$c = \lim_{n\to\infty} \frac{\hat{\varphi}(n)}{n} = \frac{6}{\pi^2} = \frac{1}{\zeta(2)} \approx 0{,}608\ldots$$

Этот результат вытекает из доказанной выше теоремы Эйлера 1, потому что взаимная простота остатка a с числом n эквивалентна неделимости целочисленного вектора (n, a).

Функция Эйлера φ естественно возникла у него при попытке обобщения малой теоремы Ферма. Эта теорема Ферма состоит в сравнении по модулю простого числа p

$$a^{p-1} \equiv 1(p)$$

для любого взаимно простого с p числа a. Она означает периодичность последовательности остатков от деления членов геометрической прогрессии $a, a^2, a^3, \ldots$ на p (с периодом $T = p - 1$).

Рассмотрим, например, остатки от деления членов геометрической прогрессии $\left\{2^t : t = 1, 2, \ldots\right\}$ на $p = 13$:

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

Двенадцатый член прогрессии равен 1, поэтому тринадцатый равен первому и т.д. (период $T = 12$).

Эйлер поставил себе вопрос: а как ведет себя геометрическая прогрессия из остатков от деления на натуральное число n, уже не являющееся простым?

Теорема Эйлера 4. *Последовательность остатков от деления на* n *членов геометрической прогрессии* $\left\{a, a^2, a^3, \ldots\right\}$, *знаменатель которой взаимно прост с* n, *периодична, и ее период* T *является делителем целого числа* $\varphi(n)$:

$$a^{\varphi(n)} \equiv 1(n), \quad \varphi(n) = T(n)N(n).$$

Пример. Остатки от деления членов геометрической прогрессии $\left\{2^t : t = 1, 2, \ldots\right\}$ на $n = 15$

$$\{2, 4, 8, 1\}, \{2, 4, 8, 1\}, \ldots$$

образуют последовательность периода $T = 4$. Значение функции Эйлера $\varphi(15) = \varphi(3)\varphi(5) = 2 \cdot 4 = 8$ делится на 4.

Доказательство теоремы 4. Рассмотрим все $\varphi(n)$ остатков от деления на n, взаимно простых с n. Эти остатки образуют (мультипликативную) группу: если a и b взаимно просты с n, то произведение ab тоже взаимно просто с n. Произведения a на все (взаимно простое с n) остатки b различны (иначе произведение $a\left(b_1 - b_2\right)$ делилось бы на n, а так как a взаимно просто с n, то $b_1 - b_2$ делилось бы на n, будучи меньше n).

Стало быть, одно из $\varphi(n)$ произведений остатков ab равно 1 (так как эти $\varphi(n)$ различных произведений все являются взаимно простыми с n остатками от деления на n и, значит, пробегают все $\varphi(n)$ взаимно простых с n остатков, в том числе и остаток 1). Следовательно, для любого взаимно простого с n остатка a существует такой взаимно простой с n остаток b, что $ab = 1$ (так что остаток b обратен остатку a в нашей мультипликативной группе).

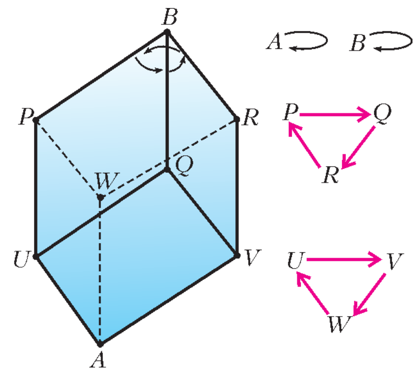


Рис.3. Вращение куба вокруг диагонали AB

Рассмотрим теперь действие операции умножения на a на все элементы описанной группы из $\varphi(n)$ взаимно простых с n остатков. Эта операция переставляет $\varphi(n)$ элементов нашей группы (так как умножение на $b = a^{-1}$ действует в обратную сторону).

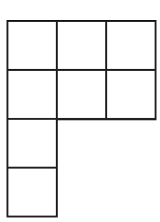
Любая перестановка элементов конечного множества разбивается на циклы. Например, поворот куба на угол 120° вокруг его главной диагонали AB переставляет его 8 вершин. При этом две вершины (концы этой диагонали) остаются на месте, т.е. каждая из них уже является циклом, остальные же 6 вершин разбиваются на 2 цикла (рис.3).

Разбиение перестановки на циклы удобно описывать при помощи специальной картинки, называемой *диаграммой Юнга.* Диаграмма Юнга перестановки N элементов состоит из N единичных квадратиков, стоящих в стольких строках, сколько у перестановки циклов. При этом элементы каждого цикла заполняют соответствующую строку (в порядке прохождения цикла). В первой строке ставится самый длинный цикл, во второй – следующий по длине и т.д., так что длины всех y строк $x_1 \geq x_2 \geq \ldots \geq x_y$ образуют разбиение

$$N = x_1 + x_2 + \ldots + x_y$$

числа переставляемых элементов N.

Пример. Диаграмма Юнга вращения куба (см. рис.3) имеет вид



$x_1 = 3$

$x_2 = 3$

$x_3 = 1$

$x_4 = 1,$

соответствует разбиению 8 вершин куба:

$$8 = 3 + 3 + 1 + 1$$

и заполняется циклами вращения так:

P	Q	R
U	V	W
A		
B		

Доказательство теоремы 4 основано на следующем факте:

Лемма. *Диаграмма Юнга перестановки $\varphi(n)$ взаимно простых с n остатков от деления на n, умножающей каждый такой остаток b на фиксированный такой остаток a, является прямоугольником (т.е. все циклы этой перестановки имеют одинаковую длину).*

Доказательство. Пусть $\{ab, ab^2, \ldots, a^Tb = b\}$ – цикл длины T. Если c – какой-либо остаток, взаимно простой с n, то мы можем представить его в виде произведения $c = bd$, где d – взаимно простой с n остаток (а именно, $d = cb^{-1}$).

Умножая c на a много раз, мы получим

$$ac = (ab)d,\ a^2c = (a^2b)d,\ a^3c = (a^3b)d,\ \ldots$$
$$\ldots,\ a^Tc = (a^Tb)d = bd = c,$$

так что T является одним из периодов и для начинающегося в c цикла.

Стало быть, наименьший период начинающегося в c цикла является делителем наименьшего периода начинающегося в b цикла. Но b и c можно поменять местами – значит, наименьшие периоды начинающихся в b и в c циклов делят друг друга, т.е. совпадают (что и доказывает лемму).

Следствие. *Период T циклов перестановки умножения на a взаимно простых с n остатков от деления на n является делителем числа $\varphi(n)$.*

Доказательство. Площадь прямоугольника равна произведению его основания на высоту, поэтому

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

где T – (наименьший) период операции умножения на a, а N – число циклов этой перестановки (всех $\varphi(n)$ взаимно простых с n остатков от деления на n).

Тем самым теорема 4 доказана: ее топологический смысл выражает именно приведенная лемма о прямоугольности диаграммы Юнга операции умножения на остаток a.

Теорема 4 приводит к очень естественному (но все еще решенному не до конца) вопросу: как ведет себя наименьший период $T(a,n)$ при $n \to \infty$ (аргумент a вставлен потому, что операции умножения на разные взаимно простые с n остатки имеют, вообще говоря, разные (наименьшие) периоды)?

Пример. Для $a = 2$ нетрудно найти следующие (наименьшие) периоды операции умножения на 2 остатков от деления на n:

n	3	5	7	9	11	13	15	17	19	21
T	2	4	3	7	10	12	4	8	18	6

Последовательность значений $T(n)$ ведет себя на вид довольно хаотическим образом. Средние арифметические

$$\hat{T}(2k+1) = \frac{\sum_{m=1}^{k} T(2m+1)}{k}$$

ведут себя более регулярным образом, но и их асимптотическое поведение изучено недостаточно.

Один из естественных подходов к этому вопросу состоит в следующем. Число делителей τ большого целого числа n растет при росте n в среднем как $\ln n$ Это – только рост среднего арифметического, сама величина $\tau(n)$ может сильно уклоняться от этого среднего: например, если $n = p$ простое число, то $\tau(p) = 2$, а если $n = m!$, то величина τ (при достаточно большом m) сколь угодно велика.

Можно сосчитать и средний рост суммы делителей с ростом числа n:

$$\Sigma(n) \sim cn$$

(постоянная c здесь есть $\zeta(2)$, и это можно усмотреть из приведенных выше доказательств теоремы Эйлера о вероятности несократимости дроби).

Аналогичным образом доказывается (средняя) асимптотика суммы s-х степеней делителей числа n,

$$\Sigma_s(n) \sim c_s n^s, \ c_s = \zeta(s+1).$$

Исходя из этих средних асимптотик, можно было бы ожидать соответствующей асимптотики для среднего арифметического делителей числа n,

$$D(n) = \frac{\Sigma(n)}{\tau(n)}.$$

Если бы среднее (по n) от дроби равнялось отношению среднего от числителя к среднему от знаменателя, то мы получили бы для среднего арифметического по n значения среднего делителя выражение

$$\widehat{D}(n) \sim ?\frac{cn}{\ln n}.$$

Однако эксперимент показывает, что средние арифметические средних делителей гораздо больше, и ответ на самом деле имеет вид

$$\widehat{D}(n) \sim \frac{\tilde{c}n}{\sqrt{\ln n}}.$$

Возвращаясь к наименьшему периоду $T(n)$ операции умножения на a остатков от деления на n, мы хотели бы использовать теорему Эйлера о том, что число $T(n)$ является одним из делителей числа $\varphi(n)$.

Если бы выполнялись следующие предположения:

1) свойства делимости (средние асимптотики) для числа делителей $\hat{\tau}(m)$, для суммы делителей $\hat{\Sigma}(m)$ и для среднего делителя $\widehat{D}(m)$ чисел m вида $\varphi(n)$ такие же, как для обычных чисел m такого же (в среднем) порядка величины,

2) выбираемый богом в качестве наименьшего периода $T(n)$ делитель числа $\varphi(n)$ ведет себя (асимптотически в среднем) как среднее арифметическое всех делителей этого целого числа,

то из предыдущих асимптотик можно было бы вывести предположительное среднее поведение периода $T(n)$ вида

$$\widehat{T}(n) \sim \widehat{D}\left(\hat{\varphi}(n)\right) \sim \frac{\tilde{\tilde{c}}\hat{\varphi}(n)}{\sqrt{\ln \hat{\varphi}(n)}} \sim \frac{c'n}{\sqrt{\ln n}}.$$

Но эксперименты (доведенные сейчас Ф.Аикарди до n порядка 10^{20}) указывают, по-видимому, на другое поведение средних $\widehat{T}$. Значит, хотя бы одно из выписанных выше предположений 1 и 2 неверно. Было бы интересно узнать, как именно нарушаются предположения 1 и 2. Это интересно не только ради исследования средних $\widehat{T}$, но и само по себе.

§2. Эйлерова теория вращения твердого тела и эйлерова гидродинамика

Моряки встретились к XVIII веку со следующей трудностью определения своего места на карте: для ориентирования измерялись координаты звезд на небесной сфере в момент измерения, и использовать эти измерения можно было, только зная точно, в какой именно момент измерения производились.

Сигналов точного времени по радио тогда еще не передавали, поэтому для определения времени приходилось пользоваться хронометрами. Но хронометр, особенно в длительном плавании, склонен начинать сильно врать. Сказываются и качка, и вращение Земли, и вариации поля тяготения, влияющие на период собственных колебаний маятника, и даже климатические условия (тропическая жара удлиняет маятник, а морозы укорачивают).

Английское адмиралтейство объявило поэтому большую премию за решение проблемы определения точного времени. Эйлер придумал остроумный путь решения этой проблемы: использовать в качестве часов Луну.

Движение четырех (открытых Галилеем) спутников Юпитера к тому времени уже пытались использовать вместо часов. Но для этого нужен, кроме хорошей теории вовсе не простого движения спутников, хороший телескоп, так как «циферблат» этих часов уж очень мал: Юпитер далеко, и спутники не всегда хорошо видны.

Луна гораздо ближе, наблюдать ее легко, так что задача была бы решена, если бы была построена достаточно точная теория малых колебаний Луны около своего центра тяжести (с учетом возмущений, вносимых прежде всего Солнцем и Землей в сложном орбитальном движении Земли вокруг Солнца и Луны вокруг Земли).

Вот эту-то теорию Эйлер и решил создать. Его замечательная работа на эту тему была опубликована в 1765 году – он рассматривал не только Луну, но и движение любого твердого тела вокруг своего центра тяжести прежде всего по инерции, а потом и вследствие возмущающих влияний других тел.

Замечательный результат этих исследований Эйлера доставляет, прежде всего, полное решение задачи об инерциальном движении произвольного твердого тела вокруг своего центра тяжести. Эта задача оказалась «вполне интегрируемой гамильтоновой системой», и Эйлер нашел нужную полную систему первых интегралов в инволюции.

Из его результатов вытекало, например, что стационарные вращения вокруг всех трех осей эллипсоида инерции твердого тела существуют, но вращение вокруг средней оси инерции неустойчиво, в то время как

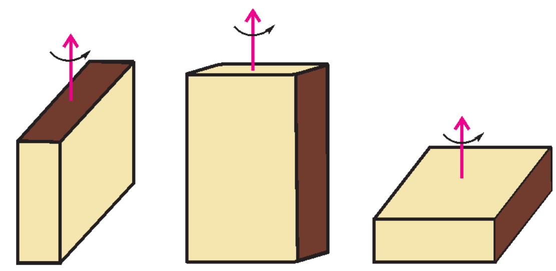


Рис.4. Устойчивое и неустойчивое вращение

и вращение вокруг большой оси инерции, и вращение вокруг малой оси инерции устойчивы (рис.4). Это значит, что, например, спичечный коробок, брошенный так, что он вращается вокруг длинной или вокруг короткой оси, так и будет вращаться, а если бросить его, закружив вокруг средней оси, то он будет кувыркаться хаотически (что я не раз демонстрировал студентам на лекции – здесь лучше всего бросать упакованную книгу, а не кирпич, и шесть граней бросаемого тела лучше выкрасить по-разному, чтобы неустойчивость была сразу видна).

Топологическая причина различия состоит в разнице линий пересечения эллипсоида со сферами с центром в начале координат (рис.5).

Около конца A большой полуоси эллипсоида расстояние до центра эллипсоида максимально, и линии, где это расстояние немного меньше длины большей полуоси OA, являются окружающими точку максимума A замкнутыми кривыми на поверхности эллипсоида. При малом отклонении направления оси вращения от направления OA соответствующий вектор переходит от вектора OA на одну из таких замкнутых кривых, близких к точке A, и начинает совершать вблизи OA малые колебания, так что движение, хотя и перестает быть стационарным вращением, остается к нему близким.

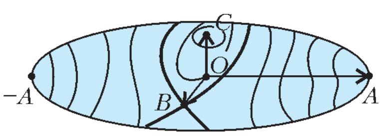


Рис.5. Линии уровня расстояний до начала координат на поверхности эллипсоида

Точно так же, около конца C малой оси расстояние до центра O достигает минимума, и линии, где оно лишь немного превышает минимальное расстояние $|OC|$, – замкнутые кривые на поверхности эллипсоида, близкие к точке C. Соответствующее возмущенное вращение остается близким к стационарному.

Напротив того, около конца B средней оси функция расстояния до центра эллипсоида O имеет седловую точку. Линия уровня, где расстояние точно равно $|OB|$, представляет собой две (пересекающиеся в точке B) окружности, а линия уровня, близкого к $|OB|$, состоит из двух замкнутых кривых, далеко уходящих от точки B (вплоть даже до противоположного конца, $-B$, средней оси). При возмущении стационарного вращения вокруг оси OB возникает совершенно непохожее на него «кувыркание», в результате которого тело может даже перевернуться почти что вверх ногами.

Луна сейчас благополучно совершает малые колебания, будучи повернута к Земле всегда в основном одной стороной и лишь немного колеблясь около этого «маятникового» положения. Напротив того, искусственные спутники Земли, в зависимости от того, как ими управляют, могут совершать все описанные Эйлером движения, так что теория Эйлера и сегодня является основой расчета борьбы с кувырканием спутников.

Теория Эйлера позволяет детально разобрать колебания Луны около своего обычного положения, так что, наблюдая фазу этих колебаний, можно использовать ее как стрелку часов и узнать момент наблюдения.

Адмиралтейство, однако, наградило не Эйлера, а часовщика, решившего проблему определения времени совершенно иным путем. А именно, он предложил подвешивать маятник AD трехзвенным подвесом $ABCD$ (рис.6). Стержни AB и CD имеют вдвое меньший коэффициент теплового расширения, чем соединяющий их стержень BC. В результате тепловое удлинение стержней AB и CD опускает груз на столько же, на сколько поднимает его тепловое удлинение стержня BC. Поэтому эффективная длина маятника AD при тепловом расширении стержней не меняется, а потому не меняется и период колебаний этого маятника: хронометр стал нечувствительным к изменению температуры!

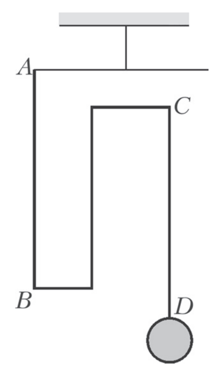


Рис.6. Компенсирующий тепловое расширение маятник

Разбирая к ее двухсотлетию статью Эйлера о вращении Луны, я заметил в 1965 году, что рассуждения Эйлера доказывают гораздо больше, чем он указал. А именно, вся теория Эйлера почти без изменений переносится на исследование геодезических линий на многообразиях групп Ли, снабженных левоинвариантной (или правоинвариантной) римановой метрикой.

Если начать с группы SO(3) вращений трехмерного евклидова пространства, то эти геодезические доставляют движения твердого тела относительно его центра тяжести, изученные Эйлером. Но теорию Эйлера можно применять и к другим группам, и получающиеся из его результатов заключения вовсе не очевидны.

В качестве очень простого примера можно взять двумерную группу аффинных преобразований прямой, $x \mapsto ax + b$. Считая преобразования сохраняющими ориентацию ($a > 0$), мы можем отождествить эту группу с полуплоскостью $\{a, \ b : a > 0\}$. В этом случае левоинвариантная метрика Эйлера доставляет в точности модель Пуанкаре геометрии Лобачевского,

$$ds^2 = \frac{da^2 + db^2}{a^2},$$

так что теория Эйлера превращается в геометрию Лобачевского. Роль стационарных вращений Эйлера играют в этом случае те прямые и окружности евклидовой полуплоскости $a > 0$ с декартовыми координатами (a, b), которые перпендикулярны линии «абсолюта», $a = 0$ (рис.7).

В качестве гораздо более богатого примера применения теории эйлерова вращения твердого тела рассмот-

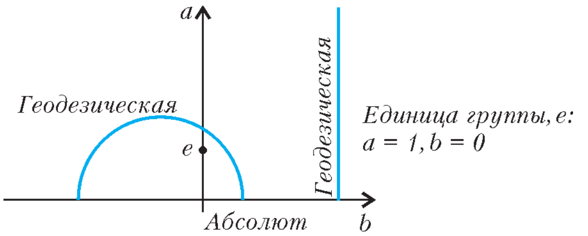


Рис.7. Геодезические модели Пуанкаре плоскости Лобачевского

рим группу SDiff M «несжимаемых» диффеоморфизмов многообразия M (т.е. диффеоморфизмов $M \to M$, сохраняющих некоторый элемент объема τ на M). Геодезические правоинвариантной метрики на этой группе представляют собой (эйлеровы) течения несжимаемой жидкости вдоль многообразия M.

Эйлерова теория устойчивости стационарных движений твердого тела превращается в этом случае в обобщение теоремы Рэлея об устойчивости двумерных течений несжимаемой жидкости, когда профиль скоростей не имеет точек перегиба (рис.8).

Течения с точками перегиба оказываются в этом

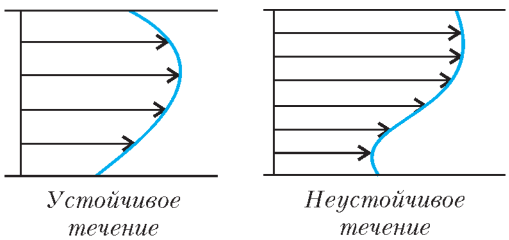


Рис.8. Теорема Рэлея об устойчивости плоскопараллельных течений несжимаемой жидкости

случае аналогичными стационарным вращениям твердого тела вокруг средней оси инерции – общая теорема устойчивости Эйлера применяется в обоих случаях одинаково, но при переходе от трехмерной группы SO(3) к бесконечномерной группе SDiff M из теоремы Эйлера получается (обобщенная) теорема Рэлея.

На устойчивость геодезических многообразия оказывает большое влияние его «секционные кривизны по двумерным направлениям». А именно, отрицательность кривизны вызывает экспоненциальное с течением времени разбегание геодезических (с близкими начальными условиями). Теория Эйлера позволяет вычислить эти секционные кривизны (для групп с левоинвариантными или правоинвариантными метриками).

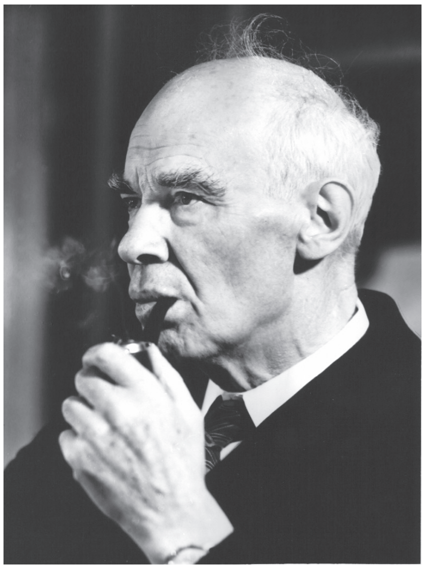
Применив эти вычисления к группам несжимаемых диффеоморфизмов поверхностей, я получил много двумерных направлений сильно отрицательной кривизны.

Например, применяя эти оценки к двумерной гидродинамике на поверхности тора (и к течениям пассатного типа), я убедился, что первоначально малые возмущения начального поля скоростей вырастают примерно в 10^5 раз (от километрового размера грозы до изменений погоды планетарного масштаба) за время порядка месяца. Это означает, что динамический прогноз погоды на сильно превышающее неделю время будет оставаться невозможным, как бы сильно ни будут усовершенствованы и компьютеры, и методы вычислений, и регистрирующие исходное состояние погоды датчики. Действительно, слегка изменив начальные скорости в каждом кубическом километре (даже так, чтобы средние по соседнему десятку кубических километров при этом не менялись), мы придем к такому новому начальному условию, которое датчики не отличат от старого, но которое приведет тайфун через пару недель не в Новый Орлеан, куда он должен был попасть по старому сценарию, а, скажем, в Бомбей.

Можно только поражаться, насколько значительными оказываются приложения фундаментальных теорий и идей Эйлера даже в тех случаях, когда сам он ограничился при их изложении первым содержательным случаем (группы SO(3) в нашем примере), а все далекие обобщения получены лишь недавно.

Вниманию наших читателей!

28 марта 2008 года исполняется сто лет со дня рождения выдающегося физика, академика Исаака Константиновича Кикоина. В связи с этим в нашей стране на высоком государственном уровне запланированы множественные специальные мероприятия. Для нас же Исаак Константинович Кикоин был прежде всего создателем и первым Главным редактором журнала «Квант».



Редакционная коллегия, редакционный совет и редакция журнала «Квант» объявляют ближайший год в журнале «Квант» – «годом Кикоина». И вот что под этим подразумевается.

Мы планируем в шести ближайших номерах журнала опубликовать разнообразные воспоминания об академике И.К.Кикоине, а в научных статьях и других материалах журнала уделить особое внимание тем областям физики и техники, в которых выдающимся образом раскрылся научный и организационный талант этого удивительного человека, в особенности – атомной и ядерной физике и энергетике. Нами готовится к изданию специальный, посвященный юбилею И.К.Кикоина выпуск серии «Библиотечка «Квант».

Те из нас, кто близко знали Исаака Константиновича, с благодарностью хранят в душе его незабываемый светлый образ. Мы очень хотим, чтобы этот образ был запечатлен в памяти и новых поколений наших читателей.