167. Лекции в 1998/9 учебном году

Малая теорема Ферма и теорема Вильсона

Малая теорема Ферма. Если p простое, то $a^p \equiv a \pmod p$.

◀ Посмотрим на диаграмму умножения на a: остаток x соединяем с остатком ax стрелкой. Будет цикл, состоящий из нуля, а остальные циклы будут одной и той же длины (равной наименьшей степени, в которой остаток a равен 1). Поэтому длины всех циклов делят $p-1$. ▶

Теорема Вильсона. Если p простое, то $(p-1)!+1$ делится на p.

◀ Все ненулевые остатки разбиваются на пары взаимно обратных, кроме 1 и $-1=p-1$, которые обратны сами себе. Группируя остатки по парам, получим, что $(p-1)! \equiv 1\cdot(-1) \pmod p$ (все остальные пары дают единицы), что и требовалось. ▶

Теорема Брианшона

Теорема Брианшона. Если шестиугольник описан около окружности, то три его большие диагонали (соединяющие вершины через три) будут пересекаться в одной точке.

◀ Представим себе, что наклонную прямую вращают вокруг вертикальной оси. Если ось проходит через точку этой прямой, получится конус. Если не проходит, получится более сложная фигура, называемая гиперболоидом. Гиперболоид заметается двумя семействами прямых. Прямые первого семейства пересекаются с прямыми второго (кроме редких случаев, когда их проекции на горизонтальную ось параллельны — в этом случае они скрещиваются).

Если смотреть на всё это сверху, то горлышко гиперболоида (окружность, где образующие прямые подходят ближе всего к оси вращения) со всех сторон окружено касательными. Каждая касательную можно считать видом сверху двух прямых — из одного семейства и из другого.

Рассмотрим наш шестиугольник. Каждая его сторона является проекцией двух обращающих (из разных семейств). Выбирая образующие по очереди из двух семейств (для одной стороны из первого, для следующей — из второго и т.д.) получим, что этот (плоский) шестиугольник есть проекция пространственного. Каждая большая диагональ есть проекция прямой пересечения пары плоскостей, каждая из которых проходит через две противоположные стороны пространственного шестиугольника. Все три плоскости (кроме редких случаев, которые мы не будем рассматривать) имеют общую точку, через проекцию которой и проходят все три большие диагонали. ▶

Производящие функции

Пусть мы хотим найти общую формулу для чисел Фибоначчи, в которых $f_0=1$, $f_1=1$ и $f_{n+2}=f_n+f_{n+1}$. Для этого запишем формальный ряд

$$F(x)=f_0+f_1x+f_2x^2+\ldots$$

Тогда $xF(x)$ будет иметь те же коэффициенты, сдвинутые вправо на 1, а $x^2F(x)$ — на два. Поэтому $xF(x)+x^2F(x)$ почти равно $F(x)$, если не считать два младших коэффициента, которые будут $0, 1$ вместо $1, 1$. Получаем тождество $(x+x^2)F(x) = F(x) - 1$, то есть $(1-x-x^2)F(x) = 1$. Отсюда можно формально заключить $F(x) = 1/(1-x-x^2)$, затем представить правую часть как сумму дробей вида $a_1/(1-\alpha_1 x)$ и $a_2/(1-\alpha_2 x)$, после чего каждую дробь заменить на геометрическую прогрессию $1 + \alpha_1 x + \alpha_1^2 x^2 + \ldots$ и получить выражение для чисел Фибоначчи как суммы двух геометрических прогрессий.

Теорема Кантора–Бершнтейна

Теорема Кантора–Бернштейна. Если A равномощно подмножеству B, а B равномощно подмножеству A, то A и B равномощны.

◀ Пусть $\phi\colon A \to B$ и $\psi\colon B \to A$ — взаимно-однозначные соответствия из условия теоремы. Будем говорить, что элемент $a \in A$ имеет порядок k, если существуют прообразы $\psi^{-1}(a)$, $\phi^{-1}(\psi^{-1}(a))$, $\ldots$, (по очереди применяем обратные отображения менее k раз), а k раз применить обратные отображения невозможно. Элементы, у которых нет конечного порядка, будем считать элементами бесконечного порядка. Пусть A_k — множество элементов порядка k, A_∞ — множество элементов бесконечного порядка. Аналогично определим B_k и B_∞.

Отображение ϕ взаимно-однозначно отображает A_k на B_{k+1}, а A_∞ — на B_∞. Отображение ψ — B_l на A_{l+1} и B_∞ на A_∞.

Взаимно-однозначное соответствие между A и B строится по частям: $A_1 \cup A_3 \cup A_5 \cup \ldots \to B_2 \cup B_4 \cup B_6 \cup \ldots$ с помощью ϕ, $B_1 \cup B_3 \cup B_5 \cup \ldots \to A_2 \cup A_4 \cup A_6 \cup \ldots$ с помощью ψ, $A_\infty \to B_\infty$, например, с помощью ϕ. ▶

Описание всех пифагоровых троек

«Несократимые» пифагоровы тройки находятся во взаимно-однозначном соответствии с точками на единичной окружности, имеющими рациональные координаты. Легко проверить, что точка на окружности имеет рациональные координаты тогда и только тогда, когда прямая, соединяющая её с точкой $(-1, 0)$ имеет рациональный наклон.

Рассматривая прямую $y = kx + k$ (k рационально), находим вторую точку пересечения с окружностью: $(\frac{1-k^2}{k^2+1}, \frac{2k}{k^2+1})$. Если $k = a/b$ — несократимая дробь, то получаем $(\frac{b^2-a^2}{a^2+b^2}, \frac{2ab}{a^2+b^2})$. Если среди a и b одно чётное число и одно нечётное, то обе дроби несократимы. Если оба числа a и b нечётны, то числители и знаменатели следует разделить на 2. Полагая $a_1 = (b-a)/2$, $b_1 = (a+b)/2$, получаем

$$(a^2 + b^2)/2 = a_1^2 + b_1^2, \quad (a^2 - b^2)/2 = 2a_1 b_1, \quad 2ab = b_1^2 - a_1^2,$$

т. е. $(\frac{b^2-a^2}{a^2+b^2}, \frac{2ab}{a^2+b^2}) = (\frac{2a_1 b_1}{a_1^2+b_1^2}, \frac{b_1^2-a_1^2}{a^2+b^2})$. При этом a_1 и b_1 уже имеют разную чётность, поэтому обе последние дроби несократимы.

Итак, несократимые пифагоровы тройки (с точностью до перестановки первых двух чисел) описываются формулами $(b^2 - a^2, 2ab, a^2 + b^2)$, где a и b взаимно просты и имеют разную чётность.

Системы линейных уравнений

Теорема. Если неизвестных больше, чем уравнений, то у системы есть ненулевое решение.

◀ Рассмотрим коэффициенты при первой неизвестной x_1. Если все они равны нулю, то у системы есть ненулевое решение (например, $(1, 0, \ldots, 0)$). Если это не так, то в каком-то из уравнений (можно считать, что в первом) коэффициент при x_1 отличен от нуля. Вычитая это уравнение из остальных с подходящими коэффициентами, получим эквивалентную систему, в которой x_1 содержится только в первом уравнении. Забудем про x_1 и про первое уравнение, и будем действовать аналогично.

Возможны две ситуации:

1) На каком-то шаге все коэффициенты при x_k равны нулю. Положив $x_k = 1$, $x_{k+1} = \ldots = x_n = 0$ и последовательно выразив $x_{k-1}, \ldots, x_1$ из предыдущих уравнений, получим нетривиальное решение системы.

2) После m шагов мы исчерпаем все уравнения. Взяв произвольные значения $x_{m+1}, \ldots, x_n$, выразим первые m неизвестных (как и в п. 1) и получим нетривиальное решение системы. ▶

Основная теорема алгебры

Теорема. Всякий многочлен с комплексными коэффициентами степени больше 1 (то есть не константа) имеет хотя бы один корень. (Следствие: имеет линейный множитель. Следствие: разлагается на линейные множители.)

Доказательство. Пусть $P(z)$ многочлен степени $n > 1$. Можно считать старший коэффициент равным 1: $P(z) = z^n + \ldots + a_1 z + a_0$. Пусть z делает один оборот, двигаясь по окружности радиуса r. Посмотрим, сколько оборотов при этом сделает $P(z)$. Это число может зависеть от r, обозначим его $n(r)$. При больших r основную роль играет z^n; значение многочлена отстоит от z^n на величину, много меньшую r^n (если дама делает n оборотов по большому кругу, то собака на короткой цепочке сделает столько же оборотов). При малых r собака топчется около a_0, и потому $n(r) = 0$. Но траектория непрерывно зависит от r; если бы она никогда не проходила через нуль, что $n(r)$ не могло бы измениться (число оборотов тоже бы менялось непрерывно, оставаясь целым).

Кососимметрические формы в $\mathbb{R}^2$ и $\mathbb{R}^3$

Числовая функция от k векторов на плоскости (или в пространстве) называется *кососимметрической k-формой*, если она линейна по каждому аргументу и меняет знак при перестановке любых двух аргументов.

Приведём пример кососимметрической 2-формы на плоскости. Поставим в соответствие векторам a и b *ориентированную площадь* $S(a, b)$ параллелограмма, натянутого на векторы a и b (со знаком плюс, если вращение от a к b происходит по часовой стрелке, и со знаком минус в другом случае). Легко проверить, что $S(a, b)$ — кососимметрическая 2-форма. Все остальные формы ей пропорциональны. В самом деле, выразив a и b через базисные векторы e_1 и e_2 и воспользовавшись билинейностью и кососимметричностью, мы получим, что в нашей власти лищь менять $S(e_1, e_2)$ — после этого остальное определится однозначно.

Аналогичное рассуждение проходит и для 3-форм в пространстве (такая форма существует и единсивенна с точностью до пропорциональности), но вместо ориентированной площади рассматривается ориентированный объём $V(a, b, c)$ параллелепипеда, натянутого на векторы a, b, c (знак выбирается по правилу левой руки). Проведя вычисление, получаем также формулу для объёма параллелепипеда: если $a = a_1e_1 + a_2e_2 + a_3e_3$, $b = b_1e_1 + b_2e_2 + b_3e_3$, $c = c_1e_1 + c_2e_2 + c_3e_3$, то

$$V(a, b, c) = (a_1b_2c_3 + a_2b_3c_1 + a_3b_1c_2 - a_1b_3c_2 - a_2b_1c_3 - a_3b_2c_1)V(e_1, e_2, e_3).$$

Векторное произведение и его свойства

Здесь мы будем интересоваться 1-формами в пространстве (т. е. числовыми линейными функциями от векторов). Пусть F такая функция, e_1, e_2, e_3 — некоторый базис в пространстве, $a = a_1e_1 + a_2e_2 + a_3e_3$. Тогда $F(a) = a_1F(e_1) + a_2F(e_2) + a_3F(e_3)$. Обозначим вектор с координатами $(F(e_1), F(e_2), F(e_3))$ через f. Тогда $F(a) = (f, a)$ (скалярное произведение). Итак, любой линейной функции на векторах (её ещё называют ***функционалом***) соответствует некоторый вектор. Наоборот, для любого вектора f формула $F(a) = (a, f)$ определяет линейный функционал. Легко проверить, что это соответствие взаимно-однозначно (разным векторам соответсвуют разные функционалы).

Рассмотрим теперь функционал $F(c) = V(a, b, c)$, где V — ориентированный объём, a и b — фиксированные векторы. Как мы видели выше, этому функционалу соответствует некоторый вектор, который мы обозначим через $a \times b$: $V(a, b, c) = (a \times b, c)$. Этот вектор называется ***векторным произведением*** векторов a и b.

Из определения легко получить несколько свойств: $a \times a = 0$, $a \times b = -b \times a$, вектор $a \times b$ билинейно зависит от a и b. Геометрическая интерпертация: $a \times b$ перпендикулярен плоскости, проходящей через a и b, равен по длине площади параллелограмма на векторах a и b и направлен по правилу левой руки. Координаты его несложно выразить через координаты a и b: $a \times b = (a_2b_3 - a_3b_2)e_1 + (a_3b_1 - a_1b_3)e_2 + (a_1b_2 - a_2b_1)e_3$.

Индукция и фундированные множества

На множестве с отношением порядка принцип индукции можно записать в следующей форме ($A(x)$ — утверждение, зависящее от x):

$$\frac{\forall x < y A(x) \Rightarrow A(y)}{\forall x A(x)}$$

(из утверждения над чертой следует утверждение под чертой). Заметим, что здесь мы не выделяем специально базу индукции.

Для произвольного упорядоченного множества принцип индукции неверен. Например, для целых чисел $(x - 2\text{чётно}) \Rightarrow (x\text{чётно})$, но не все целые числа чётны. Чтобы принцип индукции можно было применять, нужно дополнительное условие.

Множество X с отношением порядка называется ***фундированным***, если в нём нет бесконечной убывающей последовательности $x_1 > x_2 > x_3 > \dots$. Для фундированных множест принцип индукции верен: если $A(x)$ неверно, то $A(y)$ неверно для некоторого $y < x$, тогда $A(z)$ неверно для некоторого $z < y$ и т. д. — получаем бесконечную убывающую последовательность.

Введём на множестве наборов натуральных чисел фиксированной длины k ***лексикографическое отношение порядка***: сравниваем сначала первые члены, если они равны — вторые и т. д. (как слова в словаре). Можно проверить, что это множество фундировано.

Основная теорема о симметрических многочленах

Многочлен $P(x_1, \dots, x_n)$ называется *симметрическим*, если он не меняется при любых перестановках неизвестных (или, что то же самое, вместе с членом $x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}$ содержит все члены $x_{\sigma(1)}^{i_1} x_{\sigma(2)}^{i_2} \dots x_{\sigma(n)}^{i_n}$, причём с тем же коэффициентом).

Примеры симметрических многочленов легко привести. По теореме Виета коэффициенты приведённого многочлена есть многочлены от его корней, причём симметрические (если корни переставить, коэффициенты, конечно, не изменятся). Отбросив знаки, обозначим

$$\sigma_k = \sum_{i_1 < \ldots < i_k} x_{i_1} \dots x_{i_k},$$

где $k = 1, \dots, n$. Многочлены $\sigma_1, \dots, \sigma_n$ называются *элементарными симметрическими многочленами*.

Теорема. Любой симметрический многочлен есть линейная комбинация произведений элементарных симметрических многочленов.

◀ Упорядочим одночлены лексикографически (как наборы n чисел). Доказательство проводится индукцией по старшему члену. Если $x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}$ — старший член симметрического многочлена, то $i_1 \geq i_2 \geq \ldots \geq i_n$ (иначе этот член не старший). Вычитая $\sigma_1^{i_1 - i_2} \sigma_2^{i_2 - i_3} \dots \sigma_{n-1}^{i_{n-1} - i_n} \sigma_n^{i_n}$ с подходящим коэффициентом, мы уменьшим старший член и применим предположение индукции. ▶

Конечные поля. Мультипликативная группа конечного поля

Множество F с двумя операциями $+$ (сложение) и $\cdot$ (умножение) и с двумя выделенными элементами 0 и 1 ($0 \neq 1$) называется *полем*, если

1) F — группа по сложению с единичным элементом 0;

2) $F \setminus \{0\}$ — группа по умножению с единичным элементом 1 (она называется *мультипликативной группой поля* и обозначается F^*);

3) $(a + b)c = ac + bc$ для всех $a, b, c \in F$.

Например, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ — поля. Поле называется *конечным*, если в нём конечное число элементов.

Пусть F — конечное поле. Легко проверить, что суммы единиц образуют в F подполе, которое совпадает с полем $\mathbb{Z}_p$ остатков по простому модулю p (для некоторого p). Поле F, следовательно, является векторным пространством над $\mathbb{Z}$. Отсюда легко получается, что количество элементов в F (количество линейных комбинаций базисных векторов) есть степень p. Пусть F содержит p^k элементов. Обозначим $l = p^k - 1$.

Теорема. Группа F^* — циклическая.

◀ Схема доказательства такова. Сначала нужно доказать, что если k делит l, то в F^* имеется ровно k элементов, порядок которых делит k. Это следует их теоремы Безу (многочлен степени k имеет не более k корней) и такого соображения: если у уравнения $x^k = 1$ меньше k решений, то у уравнения $x^{n/k} = a$ для некторого a окажется более n/k решений, а это невозможно.

Затем доказывается (индукцией по k), что число элементов порядка РОВНО k в F^* и в циклической группе порядка l одинаковое количество. В частности, в F^* есть элемент порядка l, поэтому она сама циклическая. ▶

Вложенные параллелепипеды

Сумма измерений внутреннего параллелепипеда меньше суммы измерений внешнего. Три доказательства: сравнение диагоналей и площадей поверхности, скорость роста ε-окрестностей и средний вертикальный размер случайно повёрнутого параллелепипеда.