# Физическое доказательство малой теоремы Ферма

 \*  
  
**Г. Гутфройнд, У. Литтл**  
Physics Department, Stanford University, Stanford, Calif. 94305.  
В теории чисел немаловажное значение имеют простые числа, которые образуют базис, или представление, всех составных чисел. Здесь мы покажем, что существует связь между разложением целых чисел на простые множители и свойствами симметрии спиновых конфигураций в модели Изинга. Это позволит нам предложить «физическую» интерпретацию простых чисел, которую, как мы надеемся, по достоинству оценят физики, широко использующие соображения симметрии.

Так называемая малая 1 теорема Ферма — одна из наиболее известных теорем о делимости в элементарной теории чисел, сыгравшая важную роль в развитии последней. Формулируется малая теорема Ферма следующим образом: для любого числа p и положительного целого числа a, не кратного p,

ap–1 ≡ 1 (mod p),

т.е. ap–1 – 1 делится на p без остатка. Доказательство этой теоремы, приводимое обычно в учебниках по теории чисел, основано на арифметике вычетов [1]. Мы приведём доказательство малой теоремы Ферма, основанное на свойстве симметрии спиновых конфигураций в одномерной модели Изинга. Для ясности разобьём доказательство на три этапа.

Во-первых, докажем, что если p — любое простое число, то 2p – 2 делится на p без остатка. Для этого рассмотрим окружность с p узлами и каждому узлу i припишем какое-то значение спиновой переменной Изинга si = ±1. В пространстве 2p возможных конфигураций α = (s1, s2, ..., sp) зададим оператор сдвига T. Действие его на данную конфигурацию сводится к сдвигу всех спиновых переменных на один узел, скажем, по часовой стрелке. Разобьём все конфигурации на классы следующим образом: две конфигурации α и β считаются принадлежащими одному и тому же классу, если при некотором целом n выполняется равенство β = T nα. Конфигурация, в которой все спины обращены «вверх» (или все спины обращены «вниз»), сама по себе образует класс. Очевидно также, что для любой конфигурации α справедливо равенство α = T pα, поскольку T p соответствует полному повороту. Мы утверждаем, что если p — простое число, то при любой спиновой конфигурации α (отличной от двух тривиальных конфигураций, в которых все спины направлены в одну сторону)

α ≠ T nα       при   n<p.

Установив это, мы можем утверждать, что каждая конфигурация принадлежит какому-то классу, содержащему p различных элементов. Следовательно, число всех конфигураций за вычетом двух тривиальных конфигураций делится на p без остатка. Ясно, что равенство α = T nα может выполняться только в том случае, когда конфигурация содержит целое число повторяющихся подпериодов длиной n. При n<p отсюда следовало бы, что n — делитель числа p. Поскольку p — простое число, такое возможно только в том случае, когда n=1; это даёт две тривиальные конфигурации.

То, что число p является простым, означает, что в рассматриваемом нами случае ни одна (нетривиальная) конфигурация не имеет более высокую симметрию, чем полный поворот. Иными словами, абелева группа поворотов на угол 2π/p не имеет подгрупп.

Во-вторых, заметим, что число 2p – 2, которое делится на p без остатка, должно делиться и на 2p, так как число 2p – 2 чётно, а p, как простое число, нечётно. Таким образом, 2p–1 – 1 делится на p без остатка. Используя спиновые конфигурации в модели Изинга, мы можем получить этот результат непосредственно. Определим оператор инверсии I, который, действуя на данную конфигурацию, приводит к обращению знаков всех спиновых переменных. Разобьём, как и прежде, конфигурации на классы: две конфигурации α, β будем считать принадлежащими одному и тому же классу, если β = (TI)nα при некотором целом n. При любой конфигурации α справедливо равенство α = (TI)2pα, поскольку p, будучи простым числом, должно быть нечётным, и, следовательно, один поворот содержит нечётное число инверсий. Конфигурация переходит в самоё себя лишь после двукратного поворота. Как и прежде, мы заключаем, что каждая конфигурация (за исключением двух тривиальных, образующих класс из двух элементов) принадлежит какому-то классу из 2p различных элементов.

Наконец, обобщим соображения, приведённые выше для a = 2, на случай произвольного a, чтобы получить малую теорему Ферма в её обычной форме. Для этого рассмотрим спин j, причём 2j+1=a и каждая спиновая переменная Изинга si, совпадает с одной из 2j+1 возможных проекций спина (–j, –j+1, ..., j). Всего существует ap конфигураций, из которых необходимо вычесть a трансляционно-инвариантных конфигураций. Из приведённых выше соображений следует, что для любого a разность ap – a делится на p без остатка. Чтобы обобщить второй этап доказательства, введём оператор инверсии I, действие которого на данную конфигурацию увеличивает переменные si на единицу, за исключением того случая, когда si = j (в этом случае si под действием оператора I переходит в si = –j). Ясно, что для любой конфигурации α мы имеем a = (TI)apα. Если потребовать, чтобы a не было кратным p, то при любом n < ap имеем α ≠ (TI)nα. В противном случае мы получили бы α = (TI)aα для любого α. Следовательно, если a не кратно p, то каждая конфигурация принадлежит какому-то классу из ap различных элементов, так что (ap – a)/ap и (ap–1 – 1)/p являются целыми числами. Тем самым малая теорема Ферма полностью доказана.

Заметим, что, потребовав, чтобы a не было кратным p, мы исключили возможность симметрии, более высокой, чем произведение полных поворотов положений узлов и спиновых переменных.

Ещё одно достоинство предложенного нами метода доказательства состоит в том, что он позволяет легко обобщить малую теорему Ферма на случай некоторых составных чисел. Например, если m — произведение двух различных простых чисел p1 и p2, то можно показать, что

(am–1 –1) – (ap1–1 –1) – (ap2–1 –1)

делится на m без остатка. Члены, вычитаемые из (am–1 –1), представляют собой число конфигураций, которые попадают в классы с циклической структурой, имеющие менее чем m элементов. Малая теорема Ферма допускает обобщение и на случай более сложных составных чисел. Рассмотрим, например, число m = p1a1p2a2... pnan, где pi — простые, а ai — целые числа. Пусть a не делится на m без остатка. Тогда можно показать, что на m делится без остатка следующее выражение:

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  | | --- | --- | --- | --- | --- | | (am–1 –1) – | ∑ | (am/pi –1 –1) + | ∑ | (am/pi pj –1 –1) – ... + (–1)k(am/p1 p2 ... pn –1 –1). | |  | i |  | i,j |  | |

Примечания

H. Gutfreund, W.A. Little. "Physicist's proof of Fermat's theorem of primes". — Amer. J. Phys., March 1982, p. 219–220. Перевод с английского Ю.А. Данилова.

1. Более известна другая (так называемая «великая» или «последняя») теорема Ферма, утверждающая, что ни при каких целых n ≥ 3 уравнение xn + yn = zn не имеет решений в целых числах x, y, z. Ей посвящена обширная литература, из которой назовём лишь издания: Хинчин А. Я. Великая теорема Ферма, изд. 2-е. — М.–Л.: Гостехтеоретиздат, 1932; Постников М. М. Теорема Ферма. — М.: Наука, 1978; Эдвардс Г. Последняя теорема Ферма. — М.: Мир, 1980. — Прим. перев.

Список литературы

1. Ogilvy С.S., AndersonJ.T. Excursions in Number Theory. — New York: Oxford University Press, 1966. [См. также: Виноградов И.М. Основы теории чисел. — М.: Наука, 1972; Оре О. Приглашение в теорию чисел. — М.: Наука, 1980. — Прим. перев.]

2. Golomb S.W.— Amer. Math. Monthly, 1956, v. 63, p. 718.