# От результанта до взаимности

Г. Мерзон*

осень 2024

Целые числа и многочлены от одной переменной в некоторых аспектах похожи. И те, и другие можно делить с остатком, и для тех, и для других верна основная теорема арифметики (и проходит по сути одно и то же доказательство)... Но связывают их и менее четкие — но не менее полезные — аналогии. Про одну из них и поговорим: увидим, чем результант похож на символ Лежандра, обсудим доказательство квадратичного закона взаимности для многочленов над конечным полем и для целых чисел.

**1.** Пусть $P$ и $Q$ — два многочлена от одной переменной с коэффициентами в поле $\mathcal{K}$. Как проверить, являются ли они взаимно простыми?

Взаимная простота равносильна обратимости $Q$ по модулю $P$. Умножение на $Q$ является линейным преобразованием пространства остатков по модулю $P$. Линейное преобразование обратимо тогда и только тогда, когда не равен нулю его определитель.

**Определение 1.** Будем обозначать $(P, Q)$ определитель оператора «умножение на $Q$» на пространстве $\mathcal{K}[t]/P$.

Пусть далее $\mathcal{K}$ — это поле комплексных чисел, или еще какое-то алгебраически замкнутое поле. Определитель $(P, Q)$ дает явный способ проверить, имеют ли многочлены $P$ и $Q$ общие корни. (Конкретнее: этот определитель представляет собой многочлен от коэффициентов $P$ и $Q$, обращающийся в 0, если и только если у $P$ и $Q$ есть общие корни.)

Пусть $P(t) = (t - p_1) \dots (t - p_n)$ и все его корни $p_i$ различные. Тогда по Китайской теореме об остатках для многочленов

$$\mathcal{K}[t]/P \cong \mathcal{K}[t]/(t - p_1) \times \dots \times \mathcal{K}[t]/(t - p_n).$$

То есть кольцо $\mathcal{K}[t]/P$ изоморфно $\mathcal{K}^n$, причем изоморфизм задается вычислением значений многочлена в корнях многочлена $P$: $Q \mapsto (Q(p_1), \dots, Q(p_n))$. В таких координатах умножение на $Q$ действует диагонально и его определитель легко найти:

$$(*) \qquad (P, Q) = Q(p_1) \cdot \dots \cdot Q(p_n).$$

*МЦНМО, МИАН; email: merzon@mccme.ru

Так что если $Q(t) = (t - q_1) \dots (t - q_m)$, то

$$(**) \qquad (P, Q) = \prod (p_i - q_j),$$

где произведение берется по всем корням многочленов $P$ и $Q$.

В частности, мы доказали, что для многочленов со старшим коэффициентом 1 это выражение — оно, кстати, называется *результантом* многочленов $P$ и $Q$ — практически симметрично по $P$ и $Q$. А конкретнее, верно следующее.

**Предложение 1.** $(P, Q) = (Q, P) \cdot (-1)^{\deg P \cdot \deg Q}$ для многочленов со старшим коэффициентом 1.

> В рассуждении выше использовалось отсутствие у многочленов кратных корней, но это требование не существенно: например, многочлены без кратных корней плотны в пространстве всех многочленов. Не существенно и требование алгебраической замкнутости поля: можно считать, что корни мы рассматривали в алгебраическом замыкании.
>
> А вот то, что старший коэффициент многочленов равен 1, существенно: $(P, Q)$ вообще не меняется если умножить $P$ на константу, но меняется, если умножить $Q$ на константу. Для произвольных многочленов правильное определение результанта дается ниже (определение 3).

Доказанное нами утверждение — простейший частный случай *закона взаимности Вейля* для мероморфных функций на римановых поверхностях. Первые подробности (и дополнительные ссылки) можно узнать из популярного текста Н. Калинина и М. Магина [9]. А мы пойдем в другом направлении — не в аналитическом или геометрическом, а в арифметическом.

**2.** Выше мы думали прежде всего про случай $\mathcal{K} = \mathbb{C}$. Теперь, наоборот, сосредоточимся на случае, когда $\mathcal{K}$ — это конечное поле (например, поле остатков по простому модулю).

Определитель произведения равен произведению определителей. Поэтому $(P, Q_1 Q_2) = (P, Q_1) \cdot (P, Q_2)$. В частности, если $Q$ является квадратом в $\mathcal{K}[X]/P$, то $(P, Q)$ является квадратом в $\mathcal{K}$. Но верно и обратное!

**Лемма 2.** Пусть $P$ и $Q$ — неприводимые многочлены со старшим коэффициентом 1 с коэффициентами в конечном поле $\mathcal{K}$ нечетной характеристики. Тогда $Q$ — квадратичный вычет по модулю $P$ тогда и только тогда, когда $(P, Q)$ квадратичный вычет в $\mathcal{K}$.

> Доказательство леммы можно прочитать[1] в [9] или в [7]. Отметим, что аналогичное утверждение можно сформулировать и доказать не только для степени 2, но и для произвольной степени $d$.

[1] Или попробуйте доказать ее самостоятельно. Указание: $(P, Q) = Q \cdot Q^p \cdot Q^{p^2} \cdot \ldots \cdot Q^{p^{\deg P - 1}}$ — ср. с формулой (*).

Как мы уже знаем, выражение $(P, Q)$ симметрично по $P$ и $Q$ с точностью до знака. Получаем следующее замечательное следствие (для простоты формулировки начнем со случая, когда $-1$ является квадратом в $\mathcal{K}$ и возникающий знак не играет роли).

**Теорема 3.** Пусть $P$ и $Q$ — неприводимые многочлены со старшим коэффициентом 1 с коэффициентами в поле из $4k+1$ элемента. Тогда $P$ — квадрат по модулю $Q$ тогда и только тогда, когда $Q$ квадрат по модулю $P$.

Приведем и более общее утверждение. Пусть $P, Q \in \mathbb{F}_q[t]$ неприводимые со старшим коэффициентом 1, а число $d$ делит $q-1$. Тогда

$$\left(\frac{P}{Q}\right)_d = \left(\frac{Q}{P}\right)_d \cdot (-1)^{\deg P \cdot \deg Q \cdot \frac{q-1}{d}}.$$

Таким образом, из симметрии результанта получается простое доказательство квадратичной взаимности (а на самом деле, и взаимности степени $d$) для многочленов над конечными полями. Такое доказательство нашел в 1920-е годы F. K. Schmidt, [2].

Хотелось бы перенести подобное рассуждение и на доказательство «настоящей» квадратичной взаимности — для целых чисел. Это дальше и обсудим.

**3.** Уже в определении 1 мы пользовались тем, что кольцо $\mathcal{K}[t]$ является алгеброй над полем $\mathcal{K}$. Сразу возникает трудность: кольцо целых чисел алгеброй ни над каким полем не является. Тем не менее в каком-то смысле аналогичное определение дать можно.

Можно сказать, что мы рассматриваем $\mathbb{Z}$ как «алгебру над полем $\mathbb{F}_1$ из одного элемента». Полей из одного элемента в обычном смысле, разумеется, не существет. Зато существуют разные «$\mathbb{F}_1$-аналоги» понятий линейной алгебры. Эти аналоги бывают довольно нетривиальными (см., например, [3] и [4]), но здесь ограничимся следующим небольшим словариком

| $\mathcal{K}$-векторные пространства | множества |
|---|---|
| размерность | количество элементов |
| $GL_n(\mathcal{K})$ | $S_n$ |
| $SL_n(\mathcal{K})$ | $A_n$ |
| определитель | знак |

**Определение 2.** Если $p$ и $q$ — взаимно простые целые числа, то умножение на $q$ является перестановкой ненулевых остатков по модулю $p$. Определим $(p, q)$ как знак этой перестановки (и как 0, если $p$ и $q$ не взаимно просты).

Ясно, что $(p, q_1 q_2) = (p, q_1) \cdot (p, q_2)$. В частности, если $q$ — квадратичный вычет по простому модулю $p$, то $(p, q) = 1$. Но верно и обратное!

**Лемма 4.** Умножение на $q$ по простому модулю $p$ является четной перестановкой тогда и только тогда, когда $q$ — квадратичный вычет по модулю $p$. Другими словами, $(p, q)$ — это символ Лежандра[2] $\left(\frac{q}{p}\right)$.

[2]Напомним, что символ Лежандра $\left(\frac{a}{p}\right)$ по определению равен 0, если $a$ делится на $p$, а иначе $+1$, если $a$ является квадратом по модулю $p$, и $-1$ в противном случае.

Один из способов доказать эту *лемму Золотарева* — заметить, что первообразному корню соответствует цикл длины $p-1$, а это перестановка нечетная.

Другое доказательство: для произвольной перестановки

$$\operatorname{sign}(\sigma) = \prod_{i<j} \frac{\sigma(i)-\sigma(j)}{i-j},$$

поэтому

$$(p,q) = \prod_{i<j} \frac{qi-qj}{i-j} = q^{\frac{p(p-1)}{2}} = q^{\frac{p-1}{2}} = \left(\frac{q}{p}\right) \pmod p.$$

Теперь хотелось бы связать между собой знаки $(p,q)$ и $(q,p)$. Но наше доказательство соответствующего утверждения для многочленов опиралось на выражение $(P,Q)$ через корни многочленов. И не очень ясно, что могло бы быть аналогом такого рассуждения для целых чисел...

Вернемся временно к многочленам. Нельзя ли сделать так, чтобы симметрия была лучше видна уже на уровне *определения* для $(P,Q)$? Оказывается, можно.

Если многочлены $P$ и $Q$ не взаимно просты, то существуют такие ненулевые многочлены $X$ и $Y$ (степени строго меньше $\deg Q$ и $\deg P$ соответственно), что $XP+YQ=0$. Наоборот, если $P$ и $Q$ взаимно просты, то выражение $XP+YQ$ все время принимает различные ненулевые значения.

**Определение 3.** Запишем матрицу отображения $(X,Y) \mapsto XP+YQ$ в стандартном базисе. Определитель этой матрицы называется *результантом* многочленов $P$ и $Q$.

Откуда куда это отображение? Можно считать, что из пар многочленов степеней меньше $\deg Q$ и $\deg P$ в многочлены степени меньше $\deg P \cdot \deg Q$. Еще лучше, пожалуй, считать, что из $(\mathcal{K}[t]/Q) \oplus (\mathcal{K}[t]/P)$ в $\mathcal{K}[t]/(PQ)$. В любом случае, это отображение между *разными* пространствами, поэтому для вычисления определителя нужно зафиксировать в обоих пространствах некоторую дополнительную структуру. Например, выделенный базис.

Пусть $P$ и $Q$ многочлены со старшим коэффициентом 1. Рассмотрим их результант как многочлен от корней $P$ и $Q$. Этот многочлен имеет степень $\deg P \cdot \deg Q$ и обращается в 0, когда $P$ и $Q$ имеют общий корень, то есть он совпадает с $(P,Q) = \prod(p_i - q_j)$ с точностью до множителя. Можно проверить, что результант в точности равен $(P,Q)$ для многочленов со старшим коэффициентом 1 (последнее условие существенно!).

Отметим, что матрица из последнего определения не совпадает с матрицей из первого определения (у них даже разные размеры). Устроена она довольно просто: например, для многочленов степеней 3 и 2 такая матрица имеет вид

$$\begin{pmatrix} a_0 & 0 & b_0 & 0 & 0 \\ a_1 & a_0 & b_1 & b_0 & 0 \\ a_2 & a_1 & b_2 & b_1 & b_0 \\ a_3 & a_2 & 0 & b_2 & b_1 \\ 0 & a_3 & 0 & 0 & b_2 \end{pmatrix}.$$

Легко понять, что происходит с определителем, когда мы меняем $P$ и $Q$ местами: чтобы переставить первые $\deg Q$ и последние $\deg P$ столбцов нужно $\deg P \cdot \deg Q$ раз поменять местами соседние столбцы.

Но если симметрия для такого определителя очевидна, то мультипликативность $(P, Q_1Q_2) = (P, Q_1) \cdot (P, Q_2)$ (и связь с квадратичным характером второго аргумента по модулю первого) лучше видна из определения 1.

Попробуем перенести это определение на кольцо целых чисел. Если целые числа $p$ и $q$ взаимно просты, то отображение $(x, y) \mapsto xp + yq$ является биекцией $\mathbb{Z}/q \times \mathbb{Z}/p$ на $\mathbb{Z}/pq$. И, если зафиксировать порядок на всех этих множествах, то можно определить знак возникающей перестановки. Если числа $p$ и $q$ нечетные простые положительные, то этот знак совпадает со знаком перестановки, рассматривавшейся выше, т. е. с символом Лежандра.

Докажем это. Упорядочим пары лексикографически. Тогда пара $(i, j)$ до перестановки имеет номер $pi+j$, а после перестановки — номер $pi+qj \bmod pq$, что соответствует клетке $(i + \lfloor qj/p \rfloor \bmod q, qj \bmod p)$. То есть $j$-й столбец мы переставляем на место столбца $qj \bmod p$, да еще внутри столбца делаем циклический сдвиг $\lfloor qj/p \rfloor$ раз. Циклические перестановки нечетной длины (длины $q$) не влияют на знак. Поэтому знак всей перестановки равен знаку перестановки столбцов (тут мы снова пользуемся тем, что число $q$ нечетное). А перестановка столбцов как раз имеет знак $(p, q)$.

Так как получившееся определение симметрично по $p$ и $q$ с точностью до несложного знака, получается доказательство *квадратичного закона взаимности Гаусса.*

**Теорема 5.** Если $p$ и $q$ — нечетные положительные простые числа, то

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \cdot (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

Почему вообще знаки $(p/q)$ и $(q/p)$ отличаются — ведь мы связали их со знаком одного и того же, казалось бы, отображения: $(x, y) \mapsto xp + yq$? Дело в том, что эти два знака получаются для разных порядков на множестве $\{0, \ldots, q-1\} \times \{0, \ldots, p-1\}$: когда мы упорядочиваем пары сначала по первому элементу, а потом по второму, и когда поступаем наоборот.

Так что нужно выяснить, сколько беспорядков у перестановки, переводящей один порядок в другой. Другими словами, сколько таких пар $(i, J)$, $(I, j)$, что $i < I$, но $J > j$. Ясно, что $\{i, I\}$ можно выбрать $\frac{q(q-1)}{2}$ способами, а $\{j, J\}$ — $\frac{p(p-1)}{2}$ способами. То есть знак равен $(-1)^{\frac{p(p-1)}{2} \cdot \frac{q(q-1)}{2}}$. Так как числа $p$ и $q$ нечетные, тот же знак равен $(-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$.

Отметим, что все эти вычисления знаков перестановок не использовали простоту $p$ и $q$, только их нечетность. Так что утверждение теоремы 5 верно для произвольных нечетных положительных $p$ и $q$, если понимать символы как символы Якоби.

По существу приведенное доказательство совпадает с доказательством Золотарева [1].

Другие изложения этого доказательства см. в статье [6][3] и в книге [5][4].

Отметим, что квадратичный закон взаимности для целых чисел можно доказать и при помощи обыкновенных результантов многочленов (а не их «$\mathbb{F}_1$-аналогов»). Подробности можно найти, например, в [8]. Или попробуйте восстановить их самостоятельно — указание: перечитайте тригонометрическое доказательство Эйзенштейна, где в нем возникает формула, напоминающая (**)?

* * *

Я благодарен Г. Б. Шабату за полезные обсуждения, а также А. Г. Хованскому, рассказавшему мне про взаимность Вейля.

**Список литературы**

[1] G. Zolotareff. Nouvelle démonstration de la loi de réciprocité de Legendre // Nou. Ann. Math. (2), 1872, 11, 354–362.

[2] F. K. Schmidt. Zur Zahlentheorie in Körpern von der Charakteristik p // Sitz. Phys-Med Soc. zu Erlangen 58–59 (1926–1927), 159–172.

[3] M. Kapranov, A. Smirnov. Cohomology determinants and reciprocity laws: number field case // Preprint, 1995.

[4] C. Soulé. On the field with one element // Talk given at the Arbeitstagung, Bonn, June 1999; Preprint IHES/M/99/55.

[5] П. Ноден, К. Ките. Алгебраическая алгоритмика // М.: 1999.

[6] В. Прасолов. Доказательство квадратичного закона взаимности по Золотареву // Матем. просв., сер. 3, 4, МЦНМО, М., 2000, 140–144.

[7] K. Conrad. Quadratic reciprocity in odd characteristic
`https://kconrad.math.uconn.edu/blurbs/ugradnumthy/QRcharp.pdf`

[8] P. L. Clark, P. Pollack. Reciprocity by resultant in $k[t]$ // Enseign. Math. 65 (2019), 1/2, 101–116

[9] Н. Калинин, М. Магин. Закон взаимности Вейля: от теоремы Виета до квадратичного закона взаимности (to appear)

[3] Предупреждение: буквально приведенное там рассуждение верно для простых модулей, но не для произвольных нечетных.

[4] Изложение в виде упражнений на с. 530–531, их решения на с. 561–563. Благодарю рецензента, рассказавшего про эту интересную книгу.