О проекте

Научно-популярный
физико-математический журнал
"Квант"
(издается с января 1970 года)

МЦНМО
Редакция журнала "Квант"

Янтаров И. , **Коммутирующие многочлены.**

kvant.mccme.ru

И. Янтаров

Коммутирующие многочлены

От редакции

Обычно математические задачи, предлагающиеся школьникам, либо весьма косвенно связаны с новыми результатами, либо касаются их отдельных деталей и не дают возможности увидеть картину в целом. Наверное, это происходит потому, что в математике все взаимосвязано и, как правило, для того, чтобы полностью разобраться даже во вполне элементарном вопросе, приходится привлекать соображения из неэлементарных областей математики.

Задача о коммутирующих многочленах, которой посвящена эта статья, — счастливое исключение: здесь удается достаточно близко подойти к проблематике, имеющей общематематический интерес, пользуясь лишь элементарными средствами.

Нам эта задача стала известна из письма, присланного два года назад в «Квант» Э. Туркевичем, которому принадлежат здесь первые результаты. Задача эта, дополненная некоторыми пунктами, предлагалась на исследовательском туре XI Всесоюзной олимпиады и была помещена в Задачнике «Кванта» (М455).

Формулировка задачи

Многочлены P и Q от одной переменной называются коммутирующими *), если $P(Q(x)) = Q(P(x))$. Выписанное равенство означает, что если в обеих частях равенства раскрыть все скобки и привести подобные члены, то получатся одинаковые многочлены. Это эквивалентно тому, что для любого действительного числа d выполняется численное равенство $P(Q(d)) = Q(P(d))$.

В задаче М455 рассматриваются только многочлены со старшим коэффициентом 1; такие многочлены мы будем называть *унитарными*. (Как мы увидим ниже, вопрос о произвольных коммутирующих многочленах можно свести к вопросу о многочленах со старшим коэффициентом, равным ± 1.)

а) *Для любого числа α найдите все многочлены степени не выше трех, коммутирующие с многочленом $P(x) = x^2 - \alpha$.*

б) *Докажите, что существует не более одного многочлена заданной степени, коммутирующего с данным многочленом P степени два.*

в) *Найдите все многочлены степеней 4 и 8, коммутирующие с данным многочленом P степени два.*

г) *Докажите, что если два многочлена Q и R коммутируют с некоторым многочленом P степени два, то они коммутируют между собой.*

д) *Докажите, что существует такая последовательность многочленов $P_1, P_2, \ldots, P_k, \ldots$, коммутирующих между собой, что степень многочлена P_k равна k и $P_2(x) = x^2 - 2$.*

Решение задач а)—г)

а) Пусть $Q(x) = x^3 + ax^2 + bx + c$. Распишем равенство $P(Q(x)) = Q(P(x))$:

$$(x^3 + ax^2 + bx + c)^2 - \alpha = (x^2 - \alpha)^3 + a(x^2 - \alpha)^2 + b(x^2 - \alpha) + c.$$

Прежде чем раскрывать скобки, заметим, что справа стоят только четные степени x, а слева коэффициент при x^5 равен $2a$. Значит, $a = 0$. Но тогда слева коэффициент при x^3 равен $2c$, так что и $c = 0$. Поэтому $Q(x) = x^3 + bx$. Раскрыв скобки и приравняв коэффициенты, получаем систему

$$\begin{cases} 2b = -3\alpha, \\ b^2 = 3\alpha^2 + b, \\ \alpha = \alpha^3 + b\alpha. \end{cases}$$

Пусть $\alpha = 2\gamma$; тогда $b = -3\gamma$. Из 2-го уравнения $9\gamma^2 = 12\gamma^2 - 3\gamma$, то есть $\gamma^2 - \gamma = 0$. Значит, $\gamma = 0$ или

kvant.mccme.ru

Таким образом, многочлен 3-й степени Q, коммутирующий с многочленом $P(x) = x^2 - \alpha$, существует только при $\alpha = 0$ ($P(x) = x^2$, $Q(x) = x^3$) и при $\alpha = 2$ ($P(x) = x^2 - 2$, $Q(x) = x^3 - 3x$).

Аналогично доказывается, что если степень Q равна 2, то $Q = P$, а если она равна 1, то $Q(x) = x$.

Этот пункт очень простой. Он давался школьникам на олимпиаде, чтобы они лучше разобрались в условии задачи и немножко привыкли к ней. Кроме того, если внимательно разобраться в уравнениях, которые были выписаны, то возникает идея, как решать пункт б) — один из ключевых пунктов задачи.

б) Пусть $Q(x) = x^k + a_1x^{k-1} + a_2x^{k-2} + \dots + a_{k-1}x + a_k$, $P(x) = x^2 + px + q$. Распишем равенство

$$(x^k + a_1x^{k-1} + \dots + a_k)^2 + p(x^k + \dots + a_k) + q - (x^2 + px + q)^k - a_1(x^2 + px + q)^{k-1} - \dots - a_k = 0.$$

Приравнивая к нулю коэффициенты при x^{2k}, x^{2k-1}, ..., x, x^0, мы получаем систему уравнений для $a_1, a_2, \dots, a_k, p, q$. Решить эту систему и даже просто выписать ее довольно трудно. Однако легко заметить, что коэффициенты $b_1, b_2, \dots, b_k$ при степенях $x^{2k-1}, x^{2k-2}, \dots, x^k$ имеют следующую форму:

$b_1 = 2a_1 + R_1(p, q) = 0,$
$b_2 = 2a_2 + R_2(p, q, a_1) = 0,$
. . . . . .
$b_k = 2a_k + R_k(p, q, a_1, \dots, a_{k-1}) = 0.$

Здесь R_i — некоторое алгебраическое выражение от $p, q, a_1, \dots, a_{i-1}$. Из первого уравнения вытекает, что a_1 выражается через p и q; из второго — что a_2 выражается через p, q и a_1 и, значит, выражается через p и q; из третьего — что a_3 выражается через p, q, a_1 и a_2 и, значит, выражается через p и q, ... Итак, мы видим, что все коэффициенты $a_1, \dots, a_k$ выражаются через p и q, то есть коэффициенты многочлена Q, коммутирующего с P, однозначно выражаются через p и q, что и требовалось доказать.

Легко проверить, что аналогичная степень была больше 1 (а Q был унитарным), то есть утверждение пункта б) верно для любого такого многочлена.

Пункт б) является ключевым в задаче. Из него уже легко вытекают пункты в) и г).

в) Докажем, что многочлен $Q(x) = P(P(x))$ коммутирует с P. Действительно, $Q(P(x)) = P(P(P(x))) = P(Q(x))$. Многочлен Q имеет степень четыре и в силу б) является единственным многочленом такой степени, коммутирующим с P. Аналогично доказывается, что единственным многочленом степени 8, коммутирующим с P, является многочлен $R(x) = P(P(P(x)))$.

г) Пусть $S(x) = Q(R(x))$ и $T(x) = R(Q(x))$. Поскольку P коммутирует с Q и R, то $P(S(x)) = P(Q(R(x))) = Q(P(R(x))) = Q(R(P(x))) = S(P(x))$; значит, P коммутирует с многочленом S. Аналогично проверяется, что P коммутирует с многочленом T. Кроме того, ясно, что S и T — унитарные многочлены одинаковой степени (если Q и R имеют степени k и l, то степени многочленов S и T равны kl). Из б) вытекает, что $S = T$, то есть $Q(R(x)) = R(Q(x))$, что и требовалось.

Так же, как и в пункте б), утверждение остается верным, если P — любой многочлен степени больше 1, а Q и R унитарны.

Многочлены Чебышева. Решение пункта д)

Пункт д) намного сложнее остальных пунктов. Мы приведем несколько различных подходов к его решению.

Первый способ. Пусть $x = t + t^{-1}$. Тогда легко проверить, что x^k имеет вид

$x^k = (t + t^{-1})^k = (t^k + t^{-k}) + a_1(t^{k-1} + t^{-(k-1)}) + a_2(t^{k-2} + t^{-(k-2)}) + \dots + a_{k-1}(t + t^{-1}) + a_k$, где $a_1, \dots, a_k$ — некоторые фиксированные числа. Индукцией по k отсюда выводится, что $t^k + t^{-k}$ представляется в виде

$x^k + b_1x^{k-1} + \dots + b_{k-1}x + b_k$,

где $b_1, \dots, b_k$ — некоторые фикси-

$P_k(x)$. По определению $P_k(t+t^{-1}) = t^k + t^{-k}$, так что $P_k(P_l(t+t^{-1})) = P_k(t^l + t^{-l}) = t^{kl} + t^{-kl} = P_{kl}(t+t^{-1})$. Таким образом, $P_k(P_l(x)) = P_{kl}(x) = P_l(P_k(x))$, то есть любые два из многочленов P_k коммутируют. Поскольку $P_2(x) = x^2 - 2$, мы построили искомую последовательность многочленов.

Второй способ. Приведем способ получения многочленов P_k при помощи *многочленов Чебышева* T_k. Мы не будем давать прямого определения этих многочленов, но приведем соотношения, которым они удовлетворяют (и которые определяют их однозначно):

$$T_k(\cos t) = \cos kt.$$

Можно доказать, что T_k — многочлен степени k. Легко проверить, что многочлены Чебышева коммутируют:

$$T_k(T_m(x)) = T_{km}(x) = T_m(T_k(x))$$

— дело сводится к тому, что $\cos k(mt) = \cos kmt = \cos m(kt)$. Но T_k — не унитарный многочлен: его старший коэффициент равен 2^{k-1}. Этот недостаток легко исправить, «растянув» с помощью замены переменной аргумент и значение многочлена в два раза, т. е. положив $P_k(x) = 2T_k(x/2)$. От такой процедуры коммутативность не нарушится (проверьте это!). Замечательная последовательность многочленов Чебышева, появляющихся в самых разных вопросах анализа (особенно в теории приближения функций многочленами), оказывается последовательностью коммутирующих многочленов. Именно таким способом построил последовательность P_k Э. Туркевич.

Оба описанных способа основаны на одной идее. Пусть имеется некоторая функция f, принимающая бесконечное число значений и такая, что для каждого натурального n

$$f(nt) = Q_n(f(t)),$$

где Q_n — многочлен. Тогда многочлены Q_m и Q_n коммутируют. Например, если $f(t) = e^t$, то получаем серию коммутирующих многочленов $F_n(x) = x^n$. Если $f(t) = e^t + e^{-t}$, построения многочленов P_n, только t заменено здесь на e^t). Если $f(t) = \cos t$, то получаем серию многочленов T_n. (Те, кто знаком с комплексными числами и формулой $\cos\varphi = (e^{i\varphi} + e^{-i\varphi})/2$, без труда найдут объяснение, почему функции $e^t + e^{-t}$ и $\cos t$ приводят по существу к одной и той же, с точностью до растяжения вдвое, последовательности многочленов.)

Приведенные решения пункта д) очень красивы, но обладают одним недостатком: совершенно непонятно, как до них можно додуматься. Мы приведем еще одно решение; оно будет менее коротким, но зато будет ясно, как его придумали и как быстро выписывать многочлены P_n.

Третий способ. Как вытекает из пункта б), может существовать только один многочлен P_k степени k, коммутирующий с $P_2(x) = x^2 - 2$. Выпишем несколько первых таких многочленов:

$$P_1(x) = x,$$
$$P_2(x) = x^2 - 2,$$
$$P_3(x) = x^3 - 3x,$$
$$P_4(x) = x^4 - 4x^2 + 2,$$
$$P_5(x) = x^5 - 5x^3 + 5x,$$
$$P_6(x) = x^6 - 6x^4 + 9x^2 - 2$$

(здесь $P_4(x) = P_2(P_2(x))$, $P_6(x) = P_2(P_3(x))$, $P_5(x)$ находится так же, как в пункте а)). Посмотрев на эту последовательность многочленов, можно заметить, что она удовлетворяет рекуррентной формуле $P_{k+1}(x) = xP_k(x) - P_{k-1}(x)$. Естественно предположить, что эта формула верна при всех $k > 1$.

Итак, определим последовательность многочленов $P_1, P_2, \ldots, P_n, \ldots$ по индукции, считая, что

$$P_1(x) = x, \quad P_2(x) = x^2 - 2,$$

а при $k > 1$

$$P_{k+1}(x) = xP_k(x) - P_{k-1}(x).$$

Докажем, что все многочлены P_k коммутируют с многочленом P_2; тогда они все коммутируют между собой (пункт г)).

Проведем доказательство по индукции. Ясно, что многочлены P_1

kvant.mccme.ru

..., P_k коммутируют с P_2, и докажем, что многочлен P_{k+1} коммутирует с P_2.

Нам нужно показать, что

$$P_{k+1}(x^2-2) = (P_{k+1}(x))^2 - 2.$$

Подставляя в это равенство рекуррентную формулу для P_{k+1}, перепишем его в виде

$$(x^2-2)\,P_k(x^2-2) - P_{k-1}(x^2-2) = \\ = (xP_k(x) - P_{k-1}(x))^2 - 2.$$

Теперь используем предположение индукции:

$$(x^2-2)\,(P_k(x)^2-2) - (P_{k-1}(x)^2-2) = \\ = (xP_k(x) - P_{k-1}(x))^2 - 2.$$

Раскрывая скобки и приводя подобные члены, получим такое равенство:

$$-2\,(P_k(x)^2 - xP_k(x)\,P_{k-1}(x) + \\ + P_{k-1}(x)^2) = 2x^2 - 8$$

или

$$P_k(x)^2 - xP_k(x)\,P_{k-1}(x) + \\ + P_{k-1}(x)^2 = 4 - x^2. \quad (*)$$

Обозначим левую часть (*) через $S_k(x)$. Нам остается доказать, что $S_k(x)$ не зависит от k (и равно $4-x^2$). Действительно, пусть $k>2$. Тогда

$$S_k(x) = P_k(x)^2 - xP_k(x)\,P_{k-1}(x) + \\ + P_{k-1}(x)^2 = P_k(x)\,[P_k(x) - \\ - xP_{k-1}(x)] + P_{k-1}(x)^2 = \\ = -P_k(x)\,P_{k-2}(x) + P_{k-1}(x)^2 = \\ = P_{k-2}(x)^2 - xP_{k-1}(x)\,P_{k-2}(x) + \\ + P_{k-1}(x)^2 = S_{k-1}(x),$$

т. е. $S_k(x) = S_{k-1}(x)$. Поскольку $S_2(x) = 4-x^2$, $S_k(x) = 4-x^2$ при всех $x \geqslant 2$. Таким образом, мы показали, что P_k коммутирует с P_2 при любом k.

Задачи о коммутирующих многочленах

Мы хотим обсудить задачи, связанные со следующей общей проблемой: *описать все пары коммутирующих* (не обязательно унитарных) *многочленов* P и Q.

Задача 1. Докажите, что два многочлена P и Q первой степени коммутируют в том и только том случае, если они имеют общую неподвижную точку, т. е. такое x_0, что $P(x_0) = Q(x_0) = x_0$.

Задача 2. Решите общую проблему для случая, когда степень одного из многочленов P, Q равна 1.

В дальнейшем мы будем считать, что степени многочленов P и Q больше 1.

Пусть $P(x) = a_0x^k + a_1x^{k-1} + \cdots + a_{k-1}x + a_k$, $Q(x) = b_0x^\ell + \cdots + b_{\ell-1}x + b_\ell$. Прежде всего покажем, что можно свести общую задачу к случаю, когда коэффициенты a_1 и b_1 равны 0 (многочлены такого вида называются *приведенными*). Для этого воспользуемся следующей операцией. Зафиксируем число a и с его помощью построим из каждого многочлена R новый, «сдвинутый» многочлен $R^{(a)}$ по формуле $R^{(a)}(x) = R(x-a)+a$. Ясно, что многочлен R восстанавливается по многочлену $R^{(a)}$: $R(x) = R^{(a)}(x+a)-a$.

Задача 3. а) Докажите, что если многочлены P и Q коммутируют, то $P^{(a)}$ и $Q^{(a)}$ тоже коммутируют.

б) Докажите, что любая пара коммутирующих многочленов P и Q степени больше 1 имеет вид $P = S^{(a)}$, $Q = T^{(a)}$, где a — некоторое число, а S и T — коммутирующие приведенные многочлены.

В дальнейшем мы будем считать, что многочлены P и Q приведены. Кроме того, мы будем считать, что они унитарны, то есть их старшие коэффициенты равны 1. Ясно, что это — наиболее интересный частный случай. Кроме того, рассуждения, аналогичные проведенным выше, показывают, что можно свести общую задачу к случаю, когда старшие коэффициенты многочленов P и Q равны ± 1, так что этот частный случай не сильно отличается от общего (в этих рассуждениях надо использовать операцию «растяжения», которая каждому многочлену R сопоставляет многочлен $R^{\{\lambda\}}$ по формуле $R^{\{\lambda\}}(x) = \lambda R(x/\lambda)$). Опишем несколько серий коммутирующих многочленов:

1. Пусть R — многочлен степени r. Рассмотрим серию многочленов $P_0(x) = x$, $P_1(x) = R(x)$, $P_2(x) = R(R(x))$, $P_3(x) = R(R(R(x)))$ (вообще $P_{i+1}(x) = P_i(R(x))$).

Ясно, что все многочлены P_i

kvant.mccme.ru

2. Серия многочленов $F_k(x) = x^k$. Все многочлены F_k коммутируют и степень многочлена F_k равна k.

3. $\{P_k\}$ — серия многочленов, построенная при решении пункта д) задачи М455. Эти многочлены определяются условием $P_k(t + t^{-1}) = t^k + t^{-k}$. Степень многочлена P_k равна k.

4. Определим серию многочленов $H_1, H_3, H_5, \ldots$ таким условием: $H_k(t - t^{-1}) = t^k - t^{-k}$ (k — нечетно). Легко проверить, что такие многочлены существуют и однозначно определяются выписанным условием. Все эти многочлены коммутируют и степень многочлена H_k равна k.

На самом деле, примеры 3 и 4 являются частными случаями более общего примера. Чтобы описать этот общий пример, сделаем одно замечание о коэффициентах многочленов. Мы до сих пор считали, что эти коэффициенты — действительные числа. Однако в большинстве алгебраических вопросов лучше работать с комплексными числами. Поэтому давайте считать, что коэффициентами наших многочленов могут быть любые комплексные числа.

5. Фиксируем натуральное число m и такое комплексное число λ, что $\lambda^m = 1$ (для каждого m существует $m - 1$ такое число, отличное от 1).

Рассмотрим такие пары чисел (u, v), что $u \cdot v = \lambda$, и положим $x = u + v$. Легко проверить, что $u^k + v^k = x^k + a_1 x^{k-1} + \ldots + a_k$, где $a_1, \ldots, a_k$ — некоторые числа, зависящие от λ. Положим $P_k(x) = x^k + a_1 x^{k-1} + \ldots + a_k$; многочлен P_k характеризуется таким условием: $P_k(u + v) = u^k + v^k$, если $uv = \lambda$.

Пусть l — число, дающее при делении на m остаток 1. Тогда $u^l v^l = (uv)^l = \lambda^l = \lambda$, так что $P_k(u^l + v^l) = u^{kl} + v^{kl}$. Таким образом, если k и l дают при делении на m остаток 1, то $P_k(P_l(u + v)) = u^{kl} + v^{kl} = P_l(P_k(u + v))$, то есть многочлены P_k и P_l коммутируют. Мы построили по числу λ серию коммутирующих многочленов $P_1, P_{m+1}, P_{2m+1}, \ldots$ Все эти многочлены унитарны, приведены и степень P_k равна k.

При $m = 1$, $\lambda = 1$ мы получаем пример 3, при $m = 2$, $\lambda = -1$ — пример 4.

Примеры 1—5 исчерпывают все известные примеры коммутирующих многочленов, так что можно высказать гипотезу, что если P и Q — коммутирующие унитарные приведенные многочлены степени больше 1 с комплексными коэффициентами, то они входят

Можно, не решая общей проблемы, попытаться ответить на некоторые частные вопросы:

1. При каких α многочлен $P(x) = x^2 - \alpha$ коммутирует с каким-нибудь многочленом нечетной степени.

2. Пусть P — унитарный многочлен степени больше 1. Отметим степени всех унитарных многочленов Q, коммутирующих с P. Какое подмножество в натуральных числах при этом может получиться?

Например, в примере 1 это — геометрическая прогрессия; в примере 5 — арифметическая.

3. Пусть P, Q — коммутирующие унитарные многочлены степеней k и l. Предположим, что l делится на k. Верно ли, что Q имеет вид $Q(x) = P(R(x))$, где R — унитарный многочлен, коммутирующий с P?

Можно сформулировать более общую проблему — найти все коммутирующие рациональные функции P и Q. В этом случае появляется много новых интересных примеров.

Здесь также годится общий способ, о котором мы говорили в решении пункта д) для многочленов. Пусть имеется функция f (принимающая бесконечное число значений) такая, что

$$f(nt) = P_n(f(t)),$$

где P_n — рациональная функция. Тогда для разных n и m функции P_n и P_m коммутируют.

Возникает интересный вопрос: для каких функций f можно при любом n подобрать такую рациональную функцию P_n, чтобы $P_n(f(t)) = f(nt)$. Например, легко проверить, что этому условию удовлетворяет функция $f(t) = \operatorname{tg} t$.

Можно построить другие примеры функций f, используя теорию эллиптических функций. Поскольку это — неэлементарная теория, мы не будем здесь описывать соответствующее построение.

Все эти примеры показывают, что задача об описании коммутирующих многочленов (и, более общо, коммутирующих рациональных функций) непосредственно связана с очень глубокими и красивыми математическими теориями. Решение этой задачи, видимо, откроет какие-то новые, неизвестные ранее факты. Короче го-

Copyright ©1996-2002 МЦНМО
Пишите нам: kvant@mccme.ru
Проект осуществляется при поддержке Московского комитета образования, Московского Института Открытого Образования, Электронного журнала "Курьер образования"