УДК 512.622

Л.Я. ЛЬВОВСКИЙ
Пермский государственный технический университет

К ВОПРОСУ О ДЕЛЕНИИ МНОГОЧЛЕНОВ

Приводится оригинальный алгоритм деления многочленов с остатком, дается пример.

На практике часто приходится сталкиваться с задачами, касающимися делимости многочленов и разложения их на множители. В частности, очень популярна следующая задача: «Найти многочлен $P(x)$, который при делении на многочлен $Q^{(1)}(x)$ дает остаток $R^{(1)}(x)$, а при делении на многочлен $Q^{(2)}(x)$ – остаток $R^{(2)}(x)$». Решение таких задач, как правило, сводится к более или менее удачному перебору, особенно если делители $Q^{(1)}(x)$ и $Q^{(2)}(x)$ – нелинейны.

Выделение ситуации когда делители линейны не случайно, т.к. в этом случае остатки $R^{(1)}(x)$ и $R^{(2)}(x)$ представляют собой константы: $R^{(i)}(x)=\beta_i$ $(i=1,2)$, а делители $Q^{(1)}(x)$ и $Q^{(2)}(x)$ также определяются заданием только одной величины – свободного члена для каждого делителя, т. к. в качестве делителей, не ограничивая общности задачи, всегда можно рассматривать приведенные многочлены: $Q^{(i)}(x)=x-\alpha_i$ $(i=1,2)$. Такая задача может быть решена в явном виде даже тогда, когда заданы не две пары делителей и остатков, а произвольное число таких пар.

Рассмотрим общий случай, когда степени многочленов-делителей (или хотя бы одного из них) $Q^{(1)}(x)$ и $Q^{(2)}(x)$ больше единицы. В этом случае даже для двух делителей задача не является тривиальной и явного решения не имеет.

Итак, требуется найти многочлен $P(x)$ (желательно наименьшей возможной степени), который при делении на многочлены $Q^{(i)}(x)$ дает соответственно остатки $R^{(i)}(x)$ $(i=1,2)$.

Переформулируем условие задачи на алгебраический язык. Получим систему уравнений:

$$\begin{cases} P(x) = B^{(1)}(x)Q^{(1)}(x) + R^{(1)}(x), & N\left(R^{(1)}(x)\right) < N\left(Q^{(1)}(x)\right) \\ P(x) = B^{(2)}(x)Q^{2)}(x) + R^{(2)}(x), & N\left(R^{(2)}(x)\right) < N\left(Q^{(2)}(x)\right) \end{cases} \quad (2)$$

(под $N\left(T(x)\right)$ здесь и в дальнейшем будем обозначать степень многочлена $T(x)$).

Здесь многочлены $Q^{(i)}(x)$ и $R^{(i)}(x)$ ($i = 1,2$) – известны, а многочлены $B^{(i)}(x)$ ($i = 1,2$) (и выражаемый через них многочлен $P(x)$) – неизвестны.

Вычтем из первого уравнения системы (2) второе:

$$B^{(1)}(x)Q^{(1)}(x) - B^{(2)}(x)Q^{(2)}(x) = R^{(2)}(x) - R^{(1)}(x). \quad (3)$$

Значит, решение задачи сведется к решению эквивалентной задачи: «Решить уравнение первого порядка с двумя неизвестными многочленами $U(x)$ и $V(x)$:

$$A(x)U(x) + B(x)V(x) = C(x), \quad (4)$$

где $A(x)$, $B(x)$ и $C(x)$ – заданные (известные) многочлены (многочлены $A(x)$ и $B(x)$ отличны от нуля)».

Пусть (для определенности) в (4) степень многочлена $A(x)$ не ниже степени многочлена $B(x)$ ($N\left(A(x)\right) \geq N\left(B(x)\right)$).

Суть процедуры состоит в параллельном проведении трех процессов.

Первый из них представляет собой процесс последовательного «деления» многочлена большей степени ($A(x)$):

$$\begin{gathered} A(x) = B(x)Q_{1,1}(x) + R_{1,1}(x); \\ B(x) = R_{1,1}(x)Q_{2,1}(x) + R_{2,1}(x); \\ R_{1,1}(x) = R_{2,1}(x)Q_{3,1}(x) + R_{3,1}(x); \\ \cdots \\ R_{i-2,1}(x) = R_{i-1,1}(x)Q_{i,1}(x) + R_{i,1}(x); \\ \cdots \\ R_{n-2,1}(x) = R_{n-1,1}(x)Q_{n,1}(x) + R_{n,1}(x); \\ R_{n-1,1}(x) = R_{n,1}(x)Q_{n+1,1}(x). \end{gathered} \quad (5)$$

Этот процесс в точности совпал с алгоритмом Евклида, и, значит, многочлен $R_{n,1}(x)$ будет равен наибольшему общему делителю многочленов $A(x)$ и $B(x)$.

Как уже отмечалось, в результате выполнения этих операций степень многочленов понижается (по определению деления многочленов с остатком): $N\left(B(x)\right) > N\left(R_{1,1}(x)\right) > N\left(R_{2,1}(x)\right) > \quad > \cdots > N\left(R_{i,1}(x)\right) > \cdots$. Поэтому этот процесс конечен. На каком-то шаге (не позднее, чем на шаге с номером, равным степени многочлена $B(x)$), если деление нацело не произойдет раньше, мы получим многочлен нулевой степени, и деление нацело на следующем шаге заведомо произойдет $(R_{n+1,1}(x) \equiv 0)$.

Второй процесс представляет собой последовательность операций деления с остатком многочлена $C(x)$ и получающихся остатков на те же делители, что и в первом процессе:

$$C(x) = B(x)Q_{1,2}(x) + R_{1,2}(x);$$

$$R_{1,2}(x) = R_{1,1}(x)Q_{2,2}(x) + R_{2,2}(x);$$
$$R_{2,2}(x) = R_{2,1}(x)Q_{3,2}(x) + R_{3,2}(x);$$
$$\cdots$$
$$R_{i-1,2}(x) = R_{i-1,1}(x)Q_{i,1}(x) + R_{i,2}(x);$$
$$\cdots$$

Здесь могут возникнуть две ситуации.

Процесс закончится делением нацело не позднее, чем на $(n+1)$-шаге. Если это произошло раньше, чем на $(n+1)$-шаге, мы можем «продолжать» деление до $(n+1)$-шага, получая нулевые частные и остатки. Таким образом, мы формально можем представить результат этого процесса в виде

$$
\begin{aligned}
C(x) &= B(x)Q_{1,2}(x) + R_{1,2}(x);\\
R_{1,2}(x) &= R_{1,1}(x)Q_{2,2}(x) + R_{2,2}(x);\\
R_{2,2}(x) &= R_{2,1}(x)Q_{3,2}(x) + R_{3,2}(x);\\
&\dots\\
R_{i-1,2}(x) &= R_{i-1,1}(x)Q_{i,2}(x) + R_{i,2}(x);\\
&\dots\\
R_{n-1,2}(x) &= R_{n-1,1}(x)Q_{n,2}(x) + R_{n,2}(x);\\
R_{n,2}(x) &= R_{n,1}(x)Q_{n+1,2}(x).
\end{aligned}
\qquad (6)
$$

В этом случае, т.к. многочлен $R_{n,1}(x)$ является общим делителем многочленов $A(x)$ и $B(x)$, он делит также (по свойству делимости многочленов в соответствии с первым процессом) все многочлены-остатки $R_{i,1}(x)$. Тогда, т.к. в соответствии с последним равенством второго процесса многочлен $R_{n,1}(x)$ является делителем многочлена $R_{n,2}(x)$, двигаясь в этом процессе снизу вверх по тому же свойству делимости многочленов, убедимся в том, что многочлен $R_{n,1}(x)$ делит также все многочлены-остатки $R_{i,2}(x)$ и (из первого равенства) многочлен $C(x)$. Мы доказали, что если второй процесс закончится делением нацело не позднее, чем на $(n+1)$-шаге, то многочлен $C(x)$ делится нацело на наибольший общий делителель многочленов $A(x)$ и $B(x)$.

Рассмотрим теперь случай, когда второй процесс не заканчивается делением нацело на $(n+1)$-шаге: $R_{n,2}(x) = R_{n,1}(x)Q_{n+1,2}(x) + R_{n+1,2}(x)$, где $R_{n+1,2}(x) \neq 0$. Если бы и в этом случае многочлен $C(x)$ делился нацело на наибольший общий делителель $R_{n,1}(x)$ многочленов $A(x)$ и $B(x)$, то рассуждая так же как и в первом случае, но двигаясь во втором процессе сверху вниз, мы установим, что на многочлен $R_{n,1}(x)$ делятся также и все многочлены-остатки $R_{i,2}(x)$. Полученное противоречие доказывает, что вторая ситуация возникает лишь в случае, когда многочлен $C(x)$ не делится нацело на наибольший общий делителель многочленов $A(x)$ и $B(x)$.

Однако если выполняется равенство (4), то по свойству делимости многочленов многочлен $C(x)$ обязан делиться нацело на наибольший общий делителель многочленов $A(x)$ и $B(x)$, поэтому, если второй процесс не заканчивается делением нацело на $(n+1)$-шаге, мы вы-

нуждены сделать вывод, что уравнение (4) решений не имеет, и далее этот случай можно не рассматривать.

Итак, мы имеем право считать, что оба процесса заканчиваются одновременно, и можно переходить к третьему процессу.

Выразим из уравнения (4) многочлен $V(x)$:

$$V(x)=\frac{-A(x)U(x)+C(x)}{B(x)}=\frac{-\left(B(x)Q_{1,1}(x)+R_{1,1}(x)\right)U(x)+\left(B(x)Q_{1,2}(x)+R_{1,2}(x)\right)}{B(x)}=$$

$$=-Q_{1,1}(x)U(x)+Q_{1,2}(x)+\frac{-R_{1,1}(x)U(x)+R_{1,2}(x)}{B(x)}=-Q_{1,1}(x)U(x)+Q_{1,2}(x)+W_1(x),$$

причем функция $W_1(x)=\dfrac{-R_{1,1}(x)U(x)+R_{1,2}(x)}{B(x)}$ должна быть многочленом.

Освобождаясь в выражении для $W_1(x)$ от знаменателя, запишем:

$$B(x)W_1(x)+R_{1,1}(x)U(x)=R_{1,2}(x).$$

Выразим из уравнения (16) многочлен $U(x)$:

$$U(x)=\frac{-B(x)W_1(x)+R_{1,2}(x)}{R_{1,1}(x)}=\frac{-\left(R_{1,1}(x)Q_{2,1}(x)+R_{2,1}(x)\right)W_1(x)+\left(R_{1,1}(x)Q_{2,2}(x)+R_{2,2}(x)\right)}{R_{1,1}(x)}=$$

$$=-Q_{2,1}(x)W_1(x)+Q_{2,2}(x)+\frac{-R_{2,1}(x)W_1(x)+R_{2,2}(x)}{R_{1,1}(x)}=-Q_{2,1}(x)W_1(x)+Q_{2,2}(x)+W_2(x),$$

причем функция $W_2(x)=\dfrac{-R_{2,1}(x)W_1(x)+R_{2,2}(x)}{R_{1,1}(x)}$ должна быть многочленом.

Освобождаясь в выражении для $W_2(x)$ от знаменателя, запишем:

$$R_{1,1}W_2(x)+R_{2,1}(x)W_1(x)=R_{2,2}(x)\,.$$

Продолжая этот процесс, получим последовательно:

$$R_{1,1}W_2(x)+R_{2,1}(x)W_1(x)=R_{2,2}(x)\Rightarrow W_1(x)=-Q_{3,1}(x)W_2(x)+Q_{3,2}(x)+W_3(x);$$

$$\dots$$

$$R_{i-1,1}W_i(x)+R_{i,1}(x)W_{i-1}(x)=R_{i,2}(x)\Rightarrow W_{i-1}(x)=-Q_{i+1,1}(x)W_i(x)+Q_{i+1,2}(x)+W_{i+1}(x);$$

$$\dots$$

$$R_{n-2,1}W_{n-1}(x)+R_{n-1,1}(x)W_{n-2}(x)=R_{n-1,2}(x)\Rightarrow W_{n-2}(x)=-Q_{n,1}(x)W_{n-1}(x)+Q_{n,2}(x)+W_n(x).$$

Рассмотрим последний шаг более подробно. На этом шаге ($R_{n-1,1}W_n(x)+R_{n,1}(x)W_{n-1}(x)=R_{n,2}(x)$) мы получили, что функция $W_n(x)=\dfrac{-R_{n,1}(x)W_{n-1}(x)+R_{n,2}(x)}{R_{n-1,1}(x)}$ должна быть многочленом, после чего, освобождаясь в этом выражении от знаменателя и выражая многочлен $W_{n-1}(x)$, запишем (с применением формул, полученных в первых двух процессах):

$$W_{n-1}(x)=\frac{-R_{n-1,1}(x)W_n(x)+R_{n,2}(x)}{R_{n,1}(x)}=-Q_{n+1,1}(x)W_n(x)+Q_{n+1,2}(x),$$ т.к. на этом шаге оба деления выполняются нацело.

Отбросив все промежуточные вычисления и преобразования, выпишем цепочку равенств, которая и будет являться реализацией третьего процесса:

$$\begin{gathered}
V(x)=-Q_{1,1}(x)U(x)+Q_{1,2}(x)+W_1(x);\\
U(x)=-Q_{2,1}(x)W_1(x)+Q_{2,2}(x)+W_2(x);\\
W_1(x)=-Q_{3,1}(x)W_2(x)+Q_{3,2}(x)+W_3(x);\\
\dots\\
W_{i-1}(x)=-Q_{i+1,1}(x)W_i(x)+Q_{i+1,2}(x)+W_{i+1}(x);\\
\dots\\
W_{n-2}(x)=-Q_{n,1}(x)W_{n-1}(x)+Q_{n,2}(x)+W_n(x);\\
W_{n-1}(x)=-Q_{n+1,1}(x)W_n(x)+Q_{n+1,2}(x).
\end{gathered}\qquad(7)$$

Собственно говоря, цепочку равенств (7) можно было выписать (без единного вычисления и преобразования) сразу же, после получения цепочек равенств (5) и (6). Здесь мы проделали такую большую работу для того, чтобы стало понятным, откуда эта цепочка появилась и какую роль в реализации третьего процесса играют первые два.

Рассмотрим внимательно цепочку равенств (7). В ней есть один свободный многочлен $W_n(x)$, и давая ему различные значения (можно

взять абсолютно любой многочлен), двигаясь в этой цепочке снизу вверх, мы получим различные варианты искомых значений многочленов $U(x)$ и $V(x)$, т. е. различные решения нашего уравнения (4). Очевидно, что для того, чтобы получить решение наименьшей возможной степени, надо положить $W_n(x) \equiv 0$.

Таким образом, уравнение (4) имеет решение для любых отличных от нуля многочленов $A(x)$ и $B(x)$, если (и только если) многочлен $C(x)$ делится нацело на наибольший общий делителель многочленов $A(x)$ и $B(x)$ (в частности всегда, если многочлены $A(x)$ и $B(x)$ – взаимно просты).

Попробуем определить структуру общего решения уравнения (4), получающегося из цепочки равенств (10) при произвольном многочлене $W_n(x)$.

Вводя в цепочке (7) в рассмотрение три новых многочлена, обозначим: $W_{-1}(x) \equiv V(x)$, $W_0(x) \equiv U(x)$ и, кроме того, положим $W_{n+1}(x) \equiv 0$. Тогда все равенства системы (7) приобретают единную структуру:

$$W_{i-1}(x) = -Q_{i+1,1}(x)W_i(x) + Q_{i+1,2}(x) + W_{i+1}(x), (i = \overline{0,n}).$$

Методом полной математической индукции, двигаясь в цепочке равенств (7) снизу вверх, нетрудно получить, что в наших обозначениях справедливо представление:

$$W_i(x) = (-1)^{n-i} T_{n-i}(x)W_n(x) + S_{n-i}(x), (i = \overline{-1,n}),$$

где многочлены $T_i(x)$ и $S_i(x)$ могут быть найдены из реккурентных соотношений:

$$\begin{aligned} &T_0(x) = 1, \quad T_1(x) = Q_{n+1,1}(x), \quad T_{i+1}(x) = Q_{n-i+1,1}(x)T_i(x) + T_{i-1}(x), i = \overline{1,n}; \\ &S_0(x) = 0, \quad S_1(x) = Q_{n+1,2}(x), \quad S_{i+1}(x) = -Q_{n-i+1,1}(x)S_i(x) + S_{i-1}(x) + Q_{n-i+1,2}(x), \quad (8) \\ &i = \overline{1,n} \end{aligned}$$

причем многочлены $T_i(x)$ зависят только от исходных многочленов $A(x)$ и $B(x)$ и не зависят от многочлена $C(x)$.

В частности,

$$U(x) = W_0(x) = (-1)^n T_n(x) W_n(x) + S_n(x),$$
$$V(x) = W_{-1}(x) = (-1)^{n-i+1} T_{n+1}(x) W_n(x) + S_{n+1}(x). \quad (9)$$

Поскольку при $C(x) \equiv 0$ все $S_i(x) \equiv 0$ (это следует из цепочки равенств (6) и реккурентного представления (8)), то пара многочленов

$$U(x) = W_0(x) = (-1)^n T_n(x) W_n(x),$$
$$V(x) = W_{-1}(x) = (-1)^{n-i+1} T_{n+1}(x) W_n(x)$$

является общим решением однородного уравнения:

$$A(x)U(x) + B(x)V(x) = 0. \quad (10)$$

Но общее решение однородного уравнения (10) легко получить в явном виде.

Пусть многочлены $A(x)$ и $B(x)$ имеют наибольший общий делитель $D(x)$, тогда $A(x) = D(x)\overline{A}(x)$ и $B(x) = D(x)\overline{B}(x)$, причем многочлены $\overline{A}(x)$ и $\overline{B}(x)$ взаимно просты. Подставляя эти представления в уравнение (10) и сокращая на $D(x)$, получим:

$$\overline{A}(x)U(x) + \overline{B}(x)V(x) = 0.$$

Но из взаимной простоты многочленов $\overline{A}(x)$ и $\overline{B}(x)$ следует, что многочлен $U(x)$ должен делиться нацело на многочлен $\overline{B}(x)$, а многочлен $V(x)$ должен делиться нацело на многочлен $\overline{A}(x)$. Окончательно общее решение уравнения (10) можно записать в виде:

$$U(x) = \frac{B(x)}{D(x)} W(x),$$
$$V(x) = -\frac{A(x)}{D(x)} W(x),$$

где $W(x)$ – произвольный многочлен.

С другой стороны, если пары многочленов $\left(U^{(1)}(x), V^{(1)}(x)\right)$ и $\left(U^{(2)}(x), V^{(2)}(x)\right)$ являются решениями (какими-нибудь) уравнения (4), из системы:

$$\begin{cases} A(x)U^{(1)}(x) + B(x)V^{(1)}(x) = C(x) \\ A(x)U^{(2)}(x) + B(x)V^{(2)}(x) = C(x) \end{cases}$$

мы получаем, что разность этих решений $\left(U^{(1)}(x) - U^{(2)}(x), V^{(1)}(x) - V^{(2)}(x)\right)$ должна быть решением однородного уравнения (10). Верно и обратное, если пара многочленов $\left(U^{(1)}(x), V^{(1)}(x)\right)$ является решением (каким-нибудь) уравнения (4), а пара многочленов $\left(U^{(1)}(x) - U^{(2)}(x), V^{(1)}(x) - V^{(2)}(x)\right)$ является решением (каким-нибудь) однородного уравнения (10), то пара многочленов $\left(U^{(2)}(x), V^{(2)}(x)\right)$ также будет являться решением уравнения (4). Таким образом, мы приходим к выводу, что справедлива «классическая формула»: общее решение неоднородного уравнения (4) = частное решение уравнения (4) + общее решение однородного уравнения (10):

$$U(x) = \frac{B(x)}{D(x)} W(x) + S_n(x),$$
$$V(x) = -\frac{A(x)}{D(x)} W(x) + S_{n+1}(x),$$

где $D(x)$ – наибольший общий делитель многочленов $A(x)$ и $B(x)$ ($D(x) \equiv R_{n,1}(x)$), многочлены $S_i(x)$ могут быть найдены из реккурентного соотношения (8), а $W(x)$ – произвольный многочлен.

Остается заметить, что длина цепочек равенств (5) и (6) и (7) равна $\mathrm{Max}(N\left(A(x)\right), N\left(B(x)\right) - N\left(D(x)\right) + 1$, где $D(x)$ – наибольший общий делитель многочленов $A(x)$ и $B(x)$ (это следует из алгоритмов получения этих цепочек), то есть невелика для реально встречающихся уравнений вида (4), поэтому получение многочленов $S_n(x)$ и $S_{n+1}(x)$ – несложно.

Пример. Первый процесс – алгоритм Евклида (см. цепочку равенств (5)):

$$x^4+2x^3+3x^2+4x+5=(x+2)(x^3+1)+(3x^2+3x+3);$$
$$x^3+1=\frac{x-1}{3}(3x^2+3x+3)+2;$$
$$3x^2+3x+3=\frac{3x^2+3x+3}{2}\cdot 2.$$

Второй процесс (см. цепочку равенств (6)):

$$x^4+x^2+1=x(x^3+1)+(x^2-x+1);$$
$$x^2-x+1=(1/3)(3x^2+3x+3)-2x;$$
$$-2x=(-x)\cdot 2.$$

Третий процесс (см. цепочку равенств (7)):

$$W_2(x)=0;$$
$$W_1(x)=-x;$$
$$U(x)=-\frac{x-1}{3}(-x)+\frac{1}{3}=\frac{x^2-x+1}{3};$$
$$V(x)=-(x+2)\frac{x^2-x+1}{3}+x-x=-\frac{x^3+x^2-x+2}{3}.$$

или (см. реккурентное соотношение (5) и представления (6)):

$$S_0(x)=0;$$
$$S_1(x)=-x;$$
$$U(x)=S_2(x)=-\frac{x-1}{3}(-x)+\frac{1}{3}=\frac{x^2-x+1}{3};$$
$$V(x)=S_3(x)=-(x+2)\frac{x^2-x+1}{3}+x-x=-\frac{x^3+x^2-x+2}{3}.$$