Odmnażanie wielomianów

Bartłomiej BZDĘGA

Uniwersytet im. A. Mickiewicza w Poznaniu

Rozważmy wielomiany

$$A(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + \ldots, \qquad B(x) = b_0 + b_1x + b_2x^2 + b_3x^3 + \ldots$$

W powyższych sumach tylko skończenie wiele współczynników jest niezerowych – indeks największego z nich to stopień wielomianu. Takie przedstawienie ma swój plus. Po pomnożeniu tych wielomianów otrzymamy wielomian

$$C(x) := A(x)B(x) = c_0 + c_1x + c_2x^2 + c_3x^3 + \ldots,$$

w którym

$$(*) \qquad c_k = a_0b_k + a_1b_{k-1} + a_2b_{k-2} + \ldots + a_{k-1}b_1 + a_kb_0.$$

Jeśli dla przykładu $k > \deg A$, to wcale się nie musimy przejmować tym, że w wielomianie $A(x)$ „nie ma” a_k. Ono tam jest i jest równe 0.

Mając dane wielomiany A i B, można łatwo obliczyć wielomian C. Rzeczą trudniejszą jest odtworzenie wielomianów A i B na podstawie wielomianu C. Pokażę metodę, która jest dobra dla wielomianów względnie niskich stopni, przy dodatkowym założeniu, że wszystkie rozważane wielomiany mają współczynniki całkowite. Wielomiany, które da się rozłożyć na iloczyn wielomianów niższych stopni o współczynnikach całkowitych, nazywamy *rozkładalnymi nad* $\mathbb{Z}$.

Przykładowo niech $C(x) = 6 + x + 6x^2 + x^3 + 2x^4$. Ponieważ $\deg C = 4$, wielomian C może być iloczynem wielomianów stopnia 1 i 3 albo 2 i 2. W pierwszym przypadku wielomian C musiałby mieć pierwiastek wymierny. Na mocy twierdzenia o pierwiastkach wymiernych może to być jedna z liczb: ±1, ±2, ±3, ±6, $\pm\frac{1}{2}$, $\pm\frac{3}{2}$. Bezpośrednio sprawdzamy, że żadna z nich nie jest pierwiastkiem wielomianu C. Pozostaje więc $\deg A = \deg B = 2$. W tym przypadku, na mocy $(*)$, otrzymujemy:

$$a_0b_0 = 6, \quad a_0b_1 + a_1b_0 = 1, \quad a_0b_2 + a_1b_1 + a_2b_0 = 6,$$
$$a_1b_2 + a_2b_1 = 1, \quad a_2b_2 = 2.$$

Para (a_2, b_2) jest jedną z par: $(1, 2)$, $(2, 1)$, $(-1, -2)$, $(-2, -1)$. Ze względu na możliwość zamiany miejscami wielomianów A i B (mają równe stopnie) oraz mnożenia ich obu przez -1 możemy przyjąć bez utraty ogólności, że $a_2 = 1$ i $b_2 = 2$. W dalszym ciągu możemy rozważyć wszystkich osiem możliwych par (a_0, b_0) o iloczynie 6, aż uzyskamy rozwiązanie $A(x) = x^2 + x + 2$, $B(x) = 2x^2 - x + 3$.

Uwaga. Gdyby *każda* z możliwości w powyższym rozwiązaniu prowadziła do sprzeczności, oznaczałoby to, że wielomian C jest nierozkładalny nad $\mathbb{Z}$.

Trudność tego zadania rośnie bardzo szybko wraz ze stopniem wielomianu C. Na koniec pokażę twierdzenie, które pozwala wykazać nierozkładalność w przypadku niektórych wielomianów, niezależnie od stopnia.

Kryterium Eisensteina. Niech $C(x) = c_0 + c_1x + c_2x^2 + \ldots$ będzie wielomianem stopnia k o współczynnikach całkowitych. Jeśli istnieje liczba pierwsza p, dla której:

$$p \nmid c_k, \qquad p \mid c_0, c_1, \ldots, c_{k-1}, \qquad p^2 \nmid c_0,$$

to wielomian C jest nierozkładalny nad $\mathbb{Z}$.

Dowód. Przypuśćmy, że C jest rozkładalny nad $\mathbb{Z}$ i $C(x) = A(x)B(x)$ jest jego rozkładem. Ponieważ $c_0 = a_0b_0$, przy czym $p \mid c_0$, ale $p^2 \nmid c_0$, więc wnioskujemy, że dokładnie jedna z liczb: a_0, b_0 dzieli się przez p. Niech to będzie a_0. Dla $j < k$, jeśli $p \mid a_0, a_1, \ldots, a_{j-1}$, to na mocy wzoru $(*)$ na c_j, wobec $p \nmid b_0$, otrzymujemy $p \mid a_j$. W ten sposób dowodzimy indukcyjnie, że $p \mid a_0, a_1, \ldots, a_{k-1}$. Dodatkowo $p \mid a_k$, gdyż $a_k = 0$, bo $k > \deg A$. Ale wtedy $p \mid c_k$ na mocy wzoru $(*)$ na c_k – sprzeczność.

Zadania

1. Rozłożyć nad $\mathbb{Z}$ poniższe wielomiany lub wykazać, że to niemożliwe:
   (a) $1 - 2x + 2x^2 - x^4 + x^5$, (b) $1 - 2x^2 - x^3 + x^4$.
2. Dla liczb naturalnych $n \geqslant m > 0$ rozłożyć wielomian
   $$1 + 2x + \ldots + mx^{m-1} + mx^m + \ldots + mx^{n-1} + \ldots + 2x^{n+m-3} + x^{n+m-2}.$$
3. Rozstrzygnąć, czy wielomian $721 + 7x^{21} + 21x^7 + x^{721}$ jest rozkładalny nad $\mathbb{Z}$.
4. Niech $f(N)$ oznacza liczbę takich $a \in \{1, 2, \ldots, N\}$, że dla każdego całkowitego dodatniego n wielomian $x^n + a$ jest nierozkładalny nad $\mathbb{Z}$. Dowieść, że $\lim_{N\to\infty} \frac{f(N)}{N} = 1$.
5. Liczba p jest pierwsza. Dowieść, że wielomian $\Phi_p(x) = 1 + x + x^2 + \ldots + x^{p-1}$ jest nierozkładalny nad $\mathbb{Z}$.

Wskazówki do zadań

1. Niech $A(x)B(x)$ będzie danym wielomianem. Twierdzenie o pierwiastkach wymiernych eliminuje czynniki liniowe w obu przypadkach. (a) Można przyjąć $\deg A = 2$ oraz $\deg B = 3$, bez straty ogólności $a_0 = b_0 = 1$. Mamy $a_2 = b_3 = \pm1$ – rozważamy dwa przypadki, jeden prowadzi do rozwiązania. (b) Postępujemy podobnie jak w (a), tylko w obu przypadkach otrzymamy sprzeczność, więc nie ma rozkładu nad $\mathbb{Z}$.
2. Zapisując kolejno $c_0, c_1, c_2, \ldots$, zauważamy, że równania są do pewnego momentu spełnione, gdy $a_0 = a_1 = a_2 = \ldots = 1$ oraz $b_0 = b_1 = b_2 = \ldots = 1$.
3. Wystarczy zastosować kryterium Eisensteina dla $p = 7$.
4. Nazwijmy liczbę a *dobrą*, jeśli istnieje liczba pierwsza spełniająca warunki: $p \mid a$ i $p^2 \nmid a$. Wtedy wielomian $x^n + a$ jest nierozkładalny na mocy kryterium Eisensteina dla tego p.
   Teraz wystarczy spojrzeć na zadanie 5 z kącika nr 31 w Δ^7_{21}. Zaprezentowana tam metoda pozwala wykazać, że w zbiorze $\{1, 2, \ldots, N\}$ jest co najwyżej $N^{5/6}$ liczb niedobrych.
5. Wielomian $\Phi_p(x)$ jest nierozkładalny wtedy i tylko wtedy, gdy wielomian $W(x) = \Phi_p(x+1)$ jest nierozkładalny. Mamy $\Phi_p(x) = \frac{x^p-1}{x-1}$, więc $W(x) = \frac{(x+1)^p-1}{x} = x^{p-1} + \sum_{k=1}^{p-1} \binom{p}{k} x^{p-1-k}$.