Praca nagrodzona złotym medalem na XXIX Konkursie Uczniowskich Prac z Matematyki, Warszawa 2007

Zbiory kresowe dla wielomianów o współczynnikach całkowitych

Tomasz KOBOS

Niech f będzie wielomianem o współczynnikach całkowitych. Zajmować się będziemy dzielnikami pierwszymi liczb $f(x)$ dla x całkowitego oraz potęgami, w których te dzielniki występują. Na przykład, powszechnie wiadomo, że jeżeli tylko wielomian f nie jest stały, to zbiór takich liczb pierwszych p, iż $p|f(x)$ dla pewnego x całkowitego, jest nieskończony. Można postawić ogólniejsze pytanie: czy dla każdej liczby naturalnej m zbiór takich liczb pierwszych p, że $p^m|f(x)$ dla pewnego całkowitego x, jest nieskończony? Warto też zastanowić się nad zbiorem tych liczb pierwszych, które nie dzielą wartości wielomianu f dla żadnego argumentu całkowitego. Na początek jednak wprowadzimy kilka pojęć, które przydadzą się w dalszych rozważaniach.

Dla liczby pierwszej p, która nie dzieli współczynnika przy najwyższej potędze w wielomianie f, definiujemy jej *kres* względem wielomianu f jako największą liczbę całkowitą nieujemną m, dla której istnieje $x \in \mathbb{Z}$, takie, że $p^m|f(x)$. Jeśli takie największe m nie istnieje, przyjmujemy, że kres jest nieskończony i oznaczamy symbolem ∞. Kres liczby pierwszej p względem wielomianu f będziemy oznaczać jako $\kappa_f(p)$.

Dla przykładu rozważmy wielomian $f(x) = x^2 + 3$. Jeśli $3|f(x)$, to oczywiście $3|x$, ale wtedy $9|x^2$, a zatem $9 \not| f(x)$ dla $x \in \mathbb{Z}$. Czyli $\kappa_f(3) = 1$. Mamy też $f(1) = 4$, czyli kres liczby 2 wynosi co najmniej 2. Jednakże, bezpośrednie sprawdzenie wszystkich reszt modulo 8 pokazuje, że $8 \not| f(x)$ dla $x \in \mathbb{Z}$, a więc $\kappa_f(2) = 2$. Analogicznie sprawdzamy, że $5 \not| f(x)$ dla $x \in \mathbb{Z}$, czyli $\kappa_f(5) = 0$. Używając nieco bardziej wyrafinowanych metod, możemy udowodnić, że dla każdej liczby naturalnej m istnieje $x \in \mathbb{Z}$, dla którego $7^m|f(x)$. Zatem, zgodnie z przyjętą umową, piszemy $\kappa_f(7) = \infty$.

Wprowadźmy jeszcze jedno pojęcie. Dla danego wielomianu f i danego $m \in \mathbb{N} \cup \{\infty\}$ definiujemy zbiór $\mathbb{P}_f^m$ jako zbiór wszystkich liczb pierwszych, których kres względem wielomianu f wynosi m. Zbiór ten będziemy nazywać *zbiorem kresowym o kresie m.*

Zaczniemy od własności pewnej szczególnej rodziny zbiorów kresowych – zbiorów kresowych o kresie 0. Dla danego wielomianu f jego zbiór kresowy o kresie 0 jest więc zbiorem tych liczb pierwszych, przez które wartości wielomianu **nie są** podzielne dla żadnego argumentu całkowitego (pomijamy liczby pierwsze dzielące współczynnik przy najwyższej potędze). Taki zbiór oczywiście nie musi być nieskończony, za przykład wystarczy wziąć dowolny wielomian stopnia 1. Jednak już wśród wielomianów kwadratowych możemy znaleźć takie, których zbiór kresowy o kresie 0 jest nieskończony, za przykład służy bowiem wielomian $f(x) = x^2 + 1$, którego wartości w punktach całkowitych nie mają dzielników pierwszych postaci $4k + 3$. Okazuje się, że dla dowolnego $n > 1$ istnieje wielomian f stopnia n, dla którego zbiór $\mathbb{P}_f^0$ jest nieskończony. Konstrukcja takiego wielomianu w przypadku $n > 2$ nie jest już zupełnie prostym zadaniem, ale stosunkowo łatwo można wykazać, że jeśli p jest daną liczbą pierwszą, a n ustaloną liczbą naturalną, to istnieje wielomian f stopnia n, taki, że $\kappa_f(p) = 0$.

W rzeczywistości wskazanie wielomianu f stopnia n, dla którego zbiór $\mathbb{P}_f^0$ jest nieskończony, nie jest kłopotliwe. Trudniejszym zadaniem jest pokazanie, że dany wielomian faktycznie spełnia żądany warunek. Zupełnie elementarnie można jednak dowieść, że jeśli p jest dowolnym dzielnikiem pierwszym liczby n, to takim wielomianem jest $f(x) = x^n - p$.

Przejdźmy teraz do własności zbiorów kresowych o kresie będącym liczbą całkowitą dodatnią. Podobnie jak poprzednio, jesteśmy w stanie udowodnić, że dla danej liczby pierwszej p i ustalonych $n > 1$, $m \in \mathbb{Z}_+$ można znaleźć wielomian f stopnia n, dla którego $\kappa_f(p) = m$. Do skonstruowania takiego wielomianu przydaje się istnienie wielomianu F stopnia n, dla którego $\kappa_F(p) = 0$. Idźmy dalej: jeśli dla danych liczb pierwszych $p_1, p_2, \ldots, p_s$ mamy s wielomianów $f_1, f_2, \ldots, f_s$ stopnia n, takich, że $\kappa_{f_i}(p_i) = m$, to, używając Chińskiego Twierdzenia o Resztach, bez trudu możemy dowieść, że istnieje wielomian f (oczywiście również stopnia n), dla którego $\{p_1, p_2, \ldots, p_s\} \subseteq \mathbb{P}_f^m$. W szczególności oznacza to, że mocy zbiorów kresowych nie da się ograniczyć przez żadną liczbę naturalną – tzn. dla każdego C zawsze

znajdziemy wielomian f, dla którego $|\mathbb{P}_f^m| > C$ (wystarczy dobrać odpowiednio duże s). Nasuwa się pytanie: czy moc zbioru $\mathbb{P}_f^m$ może być nieskończona dla $m > 0$? (dla $m = 0$ wiemy, że jest to możliwe). Odpowiedź na to pytanie jest negatywna. Jesteśmy w stanie udowodnić nawet więcej, gdyż prawdziwe jest następujące

Twierdzenie. *Dla danego wielomianu f o współczynnikach całkowitych niech $\delta_f = \bigcup_{i\in\mathbb{Z}_+} \mathbb{P}_f^i$. Wówczas $|\delta_f|$, moc zbioru δ_f, jest skończona.*

Kluczem do dowodu powyższego twierdzenia okazuje się być poniższy

Lemat. *Niech f będzie wielomianem o współczynnikach całkowitych, m liczbą całkowitą dodatnią, p taką liczbą pierwszą, że $p \in \mathbb{P}_f^m$, natomiast k niech będzie taką liczbą całkowitą, że $p^m|f(k)$. Wówczas $p|f'(k)$.*

Dowód opiera się na prostej do udowodnienia za pomocą rozwinięcia dwumianowego Newtona kongruencji: $f(tp^m + k) \equiv p^m t f'(k) + f(k) \bmod p^{m+1}$. Jeżeli p nie dzieliłoby $f'(k)$, to moglibyśmy tak dobrać t, by $p^{m+1}|f(tp^m + k)$. To jest jednak sprzeczne z warunkiem $p \in \mathbb{P}_f^m$.

Żeby zobaczyć, w jaki sposób powyższy lemat można wykorzystać do oszacowania mocy zbiorów kresowych od góry, zatrzymajmy się na chwilę przy wielomianie kwadratowym: $f(x) = ax^2 + bx + c$. Załóżmy, że wyróżnik tego wielomianu $\Delta = b^2 - 4ac$ jest niezerowy. W przeciwnym przypadku nietrudno sprawdzić, że $\mathbb{P}_f^m = \emptyset$ dla każdego m. Niech $p \in \mathbb{P}_f^m$ dla pewnego $m \in \mathbb{Z}_+$, a k niech spełnia warunek $p^m|f(k)$. Wówczas mamy też $p|f(k) = ak^2 + bk + c$ oraz, z powyższego lematu, $p|f'(k) = 2ak + b$. Zauważmy teraz, iż:

$$p|2a(2f(k) - kf'(k)) - bf'(k) =$$
$$= 2a(2ak^2 + 2bk + 2c - 2ak^2 - bk) - 2abk - b^2 =$$
$$= 2a(bk + 2c) - 2abk - b^2 = 4ac - b^2 = -\Delta.$$

Oznacza to, że wszystkie elementy zbioru δ_f są dzielnikami niezerowej liczby całkowitej, wyróżnika wielomianu f. Czyli rzeczywiście $|\delta_f|$ jest skończona.

Co ciekawe, do przypadku wielomianu kwadratowego można podejść w zupełnie inny sposób, wykorzystując postać kanoniczną wielomianu oraz fakt, że jeśli liczba całkowita a, niepodzielna przez daną liczbę pierwszą p, jest resztą kwadratową modulo p, to wtedy jest też resztą kwadratową modulo p^m dla każdego $m \in \mathbb{Z}_+$.

Naturalna jest próba uogólnienia powyższej metody na wyższy stopień wielomianu. Wykorzystując relacje $p|f(k)$ i $p|f'(k)$, chcielibyśmy uzyskać podzielność $p|c$, gdzie c jest stałą zależną tylko od wielomianu f. Jednakże ręczne wykonanie obliczeń już w przypadku wielomianu sześciennego jest dosyć kłopotliwe. Okazuje się jednak, że jest sposób obejścia tego problemu.

Niech f będzie dowolnym wielomianem o współczynnikach całkowitych, $p \in \mathbb{P}_f^m$ dla pewnego $m > 0$, a k niech będzie takie, że $p^m|f(k)$. Możemy też założyć, że wielomian f jest nierozkładalny – rzeczywiście, jeśli $f(x) = p(x)q(x)$ i $|\delta_f|$ jest nieskończona, to wtedy $|\delta_p|$ jest nieskończona lub $|\delta_q|$ jest nieskończona. Wówczas jest on względnie pierwszy ze swoją pochodną, gdyż jest ona wielomianem o stopniu mniejszym. Istnieją więc wielomiany $A(x)$, $B(x)$ o współczynnikach całkowitych, oraz niezerowa liczba całkowita c, dla których:

$$A(x)f(x) + B(x)f'(x) = c.$$

Mówimy, że wielomian f jest *nierozkładalny*, jeżeli nie da się go przedstawić w postaci iloczynu dwóch wielomianów o współczynnikach całkowitych, z wyjątkiem iloczynu $f(x) = 1 \cdot f(x)$ oraz $f(x) = -1 \cdot (-f(x))$.

Wielomiany $p(x), q(x)$ o współczynnikach całkowitych są względnie pierwsze, jeśli nie istnieje wielomian $r(x)$ o współczynnikach całkowitych i o stopniu dodatnim, taki, że $r(x)|p(x)$ oraz $r(x)|q(x)$.

Fakt, który tutaj wykorzystujemy, jest wielomianowym odpowiednikiem podobnego twierdzenia dla liczb całkowitych. Wstawiając do powyższej równości $x = k$ i korzystając z podzielności $p|f(k)$ oraz $p|f'(k)$, dostajemy natychmiast $p|c$. Czyli, tak jak poprzednio, stwierdzamy, że wszystkie elementy zbioru δ_f są dzielnikami niezerowej liczby całkowitej c. A to oznacza, że zbiór δ_f jest skończony.

Na koniec przyjrzymy się zbiorom kresowym o kresie nieskończonym. Okazuje się, że jeśli wielomian f nie jest stały, to zbiór $\mathbb{P}_f^\infty$ jest nieskończony. W szczególności dla każdej liczby naturalnej m istnieje nieskończenie wiele takich liczb pierwszych p, że $p^m|f(x)$ dla pewnego $x \in \mathbb{Z}$. Jest to więc uogólnienie wspomnianego na początku artykułu rezultatu teorii liczb. Dowód opiera się na zastosowaniu twierdzenia udowodnionego powyżej. Jeśli wiemy, że istnieje nieskończenie wiele takich liczb pierwszych p, że $p|f(x)$ dla pewnego x, to po odrzuceniu z nich liczb należących do δ_f dostaniemy właśnie zbiór $\mathbb{P}_f^\infty$.

Jest z pewnością jeszcze wiele pytań, które można postawić w związku z zagadnieniem zbiorów kresowych. Można się, na przykład, zastanowić nad rozszerzeniem jednego z uzyskanych rezultatów: czy dla danej liczby pierwszej p i ustalonych $m, n \in \mathbb{Z}_+$ istnieje wielomian f stopnia n, dla którego $\kappa_f(p) = m$ oraz przynajmniej jeden ze współczynników wielomianu f (nie licząc współczynnika wiodącego) jest niepodzielny przez p (przykład skonstruowany przeze mnie nie spełnia tego warunku)? Mimo że obliczenia przeprowadzone na komputerze dla małych liczb pierwszych mogą sugerować, że jest to prawda, to problemu tego nie udało mi się rozwiązać. A może Czytelnik podejmie to wyzwanie?