Wielomiany podziału koła – część 2

Bartłomiej BZDĘGA Uniwersytet im. A. Mickiewicza w Poznaniu

Przed przystąpieniem do lektury polecam zapoznać się z poprzednim kącikiem (Δ^1_{24}). Udowodniliśmy w nim istnienie ciągu wielomianów $\Phi_1(x)$, $\Phi_2(x)$, …, które dla każdej liczby naturalnej n spełniają

$$\prod_{d|n} \Phi_d(x) = x^n - 1. \tag{1}$$

W tym kąciku przyjrzymy się rozkładowi na czynniki pierwsze liczby $\Phi_n(a)$ dla $a \geqslant 2$. Niech p będzie liczbą pierwszą, która dzieli $\Phi_n(a)$. Ponieważ $\Phi_n(a) \mid a^n - 1$, więc $p \mid a^n - 1$. Istnieje zatem najmniejsza taka liczba całkowita dodatnia r, że $p \mid a^r - 1$. Nazywamy ją *rzędem a modulo p*. Rząd jest dzielnikiem każdej liczby naturalnej w spełniającej $p \mid a^w - 1$, w szczególności $r \mid n$. Zapiszmy $n = rmp^k$, przy czym $p \nmid m$. Niech $\nu_p(N)$ oznacza wykładnik największej potęgi p dzielącej N. Dla $p > 2$ otrzymujemy

$$\nu_p(a^r - 1) + k \overset{\text{(i)}}{=} \nu_p(a^n - 1) \overset{\text{(ii)}}{=} \sum_{D|n} \nu_p(\Phi_D(a)) \overset{\text{(iii)}}{=} \sum_{d|m} \sum_{j=0}^{k} \nu_p(\Phi_{rdp^j}(a)), \tag{2}$$

przy czym (i) wynika z lematu o zwiększaniu wykładnika p-adycznego (zob. kącik nr 24 w Δ^{12}_{20}), a (ii) wynika z (1). Równość (iii) wynika z obserwacji, że jeśli $\nu_p(\Phi_d(a))$ jest niezerowe, czyli $p \mid \Phi_D(a)$, to $p \mid a^D - 1$, a więc $r \mid D$; natomiast każdy podzielny przez r dzielnik n jest postaci rdp^j, w której $d \mid m$ i $j \leqslant k$.

Z równości (2) wnioskujemy kolejno, że:

(A) jeśli $n = r$ ($k = 0$ i $m = 1$), to $\nu_p(a^r - 1) = \nu_p(\Phi_n(a))$;
(B) jeśli $n = rp^k$ ($k > 0$ i $m = 1$), to $\nu_p(\Phi_n(a)) = 1$, co uzasadniamy indukcją po k;
(C) jeśli $n = rmp^k$ ($k > 0$ i $m > 1$), to $\nu_p(\Phi_n(a)) = 0$

Uzasadnienia powyższych implikacji można powtórzyć dla $p = 2$ i $n \geqslant 3$, wykorzystując część 2(c) lematu o zwiększaniu wykładnika, sformułowanego w kąciku nr 24. Dzielniki pierwsze liczby $\Phi_n(a)$ dla $n \geqslant 3$ można zatem podzielić na *trywialne* (spełniające $n = rp^k$ dla $k > 0$) i *nietrywialne* (spełniające $n = r$). Te pierwsze jest łatwo znaleźć, bo są dzielnikami n. Jest nawet prościej: zgodnie z Małym Twierdzeniem Fermata $a^{p-1} \equiv 1 \pmod p$, czyli $r \mid p - 1$ i $r < p$, a zatem z równości $n = rp^k$ wynika, że p jest największą liczbą pierwszą dzielącą n. Dlatego $\Phi_n(a)$ ma co najwyżej jeden dzielnik trywialny.

Trudniej znaleźć dzielniki nietrywialne. Wykażemy tu, że niemal zawsze jest co najmniej jeden taki dzielnik. Niech p będzie największym dzielnikiem pierwszym liczby n. Wystarczy wykazać, że $\Phi_n(a) > p$ – w takiej sytuacji nawet gdyby p okazał się dzielnikiem trywialnym, to równość $\nu_p(\Phi_n(a)) = 1$ implikuje istnienie dzielnika $\Phi_n(a)$ różnego od p, a zatem nietrywialnego. Zapiszmy $n = mp$. Nietrudno udowodnić, że dla $p \mid m$ zachodzi $\Phi_n(x) = \Phi_m(x^p)$, a w przeciwnym przypadku $\Phi_n(x)\Phi_m(x) = \Phi_m(x^p)$ – wystarczy porównać pierwiastki wielomianów po obu stronach (por. Δ^1_{24}). Ta pierwsza równość pozwala też wywnioskować, że jeśli każdy dzielnik pierwszy liczby t jest dzielnikiem pierwszym liczby m, to $\Phi_{mt}(x) = \Phi_m(x^t)$.

Ponieważ $(a-1)^{\varphi(n)} \leqslant \Phi_n(a) \leqslant (a+1)^{\varphi(n)}$ dla $a \geqslant 2$ (znów Δ^1_{24}), otrzymujemy

$$\Phi_n(a) \geqslant \frac{\Phi_m(a^p)}{\max\{1, \Phi_m(a)\}} \geqslant \frac{(a^p-1)^{\varphi(m)}}{(a+1)^{\varphi(m)}} \geqslant \frac{a^p-1}{a+1} \geqslant \frac{2^p-1}{3}.$$

Jest jasne, że $\frac{2^p-1}{3} > p$ dla $p > 3$. Jeżeli $p = 2$, to $n = 2^k = 2t$ oraz $\Phi_n(a) = a^t + 1 > 2$. Dla $p = 3$ możliwe są dwie sytuacje. Dla $n = 3^k = 3t$ mamy $\Phi_n(a) = a^{2t} + a^t + 1 > 3$. Jeśli $n = 2^{k_1}3^{k_2} = 6t$, to mamy $\Phi_n(a) = a^{2t} - a^t + 1$, co jest większe od 3, gdy $a > 2$ lub $t > 1$. W przypadku $a = 2$ i $t = 1$ mamy $\Phi_6(2) = 3$, i nie ma tu dzielnika nietrywialnego. Wykazaliśmy zatem:

Twierdzenie. *Jeśli $n \geqslant 3$, $a \geqslant 2$ oraz $(n, a) \neq (3, 2)$, to liczba $\Phi_n(a)$ ma nietrywialny dzielnik pierwszy p, tzn. rząd a modulo p wynosi n.*

Zadania

1. W zależności od różnych $m, n \geqslant 3$ oraz $a \geqslant 2$ wyznaczyć $\mathtt{NWD}(\Phi_n(a), \Phi_m(a))$.
2. Niech $\omega(n)$ oznacza liczbę różnych dzielników pierwszych liczby n. Udowodnić, że dla nieparzystego n zachodzi nierówność $\omega(2^n - 1) \geqslant 2^{\omega(n)} - 1$.
3. Rozważmy ciąg $\left(2^2 - 1,\ 2^3 - 1,\ 2^4 - 1,\ \ldots\right)$. Wykazać, że każdy wyraz tego ciągu ma dzielnik pierwszy, którego nie ma żaden wyraz poprzedni, z jednym tylko wyjątkiem: $2^6 - 1$. *(Bang, 1886)*
   (Jest to szczególny przypadek twierdzenia Zsigmondy'ego, o którym jeszcze kiedyś będzie mowa).
4. Udowodnić, że dla każdego naturalnego $n \geqslant 2$ istnieje nieskończenie wiele liczb pierwszych, które dają resztę 1 z dzielenia przez n.
   (Jest to szczególny przypadek twierdzenia Dirichleta).

Wskazówki do zadań

1. Dla różnych n dzielniki pierwsze nietrywialne liczb $\Phi_n(a)$ są różne (bo a ma jednoznaczny rząd modulo p).
2. Zob. poprzednią wskazówkę.
3. Zob. poprzednią wskazówkę.
4. Jeśli $p > n$ i $p \mid \Phi_n(a)$, to p jest nietrywialnym dzielnikiem $\Phi_n(a)$.
   Wówczas z tego, że rząd a modulo p wynosi n, wynika, że $p \equiv 1 \pmod n$.
   Wystarczy teraz wykazać, że jeśli $P(x)$ jest niestałym wielomianem o współczynnikach całkowitych, to zbiór liczb pierwszych dzielących którąkolwiek z liczb: $P(1), P(2), P(3), \ldots$ jest nieskończony.