Wielomiany podziału koła – część 1

Bartłomiej BZDĘGA Uniwersytet im. A. Mickiewicza w Poznaniu

Poniższe twierdzenia są podstawą tego kącika. Dla kompletności podaję ich dowody, w których wykorzystuje się liczby zespolone. Czytelnik nieznający liczb zespolonych może je bez obaw pominąć i przejść od razu do zadań.

Twierdzenie 1. Istnieją (i są określone jednoznacznie) takie wielomiany unormowane (tzn. mające współczynnik 1 przy najwyższej potędze zmiennej) $\Phi_1, \Phi_2, \Phi_3, \ldots$ o współczynnikach całkowitych, że dla każdego całkowitego dodatniego n zachodzi równość:

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

Wielomiany $\Phi_d(x)$ nazywamy *wielomianami podziału koła* (lub *cyklotomicznymi*).

Twierdzenie 2. Niech φ oznacza funkcję Eulera (zobacz kącik nr 45 w Δ_{22}^9). Dla $x \geqslant 1$ zachodzą nierówności:

$$(x-1)^{\varphi(n)} \leqslant \Phi_n(x) \leqslant (x+1)^{\varphi(n)}, \tag{2}$$

przy czym pierwsza z nich jest ostra dla $n \geqslant 2$, a druga dla $n \geqslant 3$. W szczególności dla $n \geqslant 2$ i $x \geqslant 2$ mamy $\Phi_n(x) > 1$.

Liczbę zespoloną ζ nazywamy *pierwiastkiem n-tego stopnia z* 1, jeśli $\zeta^n = 1$. Jeżeli ponadto $\zeta^m \neq 1$ dla $1 \leqslant m < n$, to liczbę ζ nazywamy *pierwotnym pierwiastkiem stopnia n z* 1. Niech $\zeta_n = e^{2\pi i/n} = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$. Wówczas zbiór $\mu_n = \{\zeta_n, \zeta_n^2, \zeta_n^3, \ldots, \zeta_n^n\}$ stanowią wszystkie pierwiastki stopnia n z jedności, a zbiór $\mu_n^\star = \{\zeta_n^k : 1 \leqslant k \leqslant n, \mathtt{NWD}(k,n) = 1\}$ stanowią wszystkie pierwiastki pierwotne.

Lemat. Wielomiany $\Phi_n(x) = \prod_{\zeta \in \mu_n^\star}(x - \zeta)$ spełniają równość (1).

Dowód. Wykażemy najpierw równość $\mu_n = \bigcup_{d \mid n} \mu_d^\star$. Ułamek a/n dla $a = 1, 2, \ldots, n$ możemy w sposób jednoznaczny przedstawić w postaci k/d, w której $d \mid n$, $1 \leqslant k \leqslant d$ oraz $\mathtt{NWD}(k,d) = 1$. Na odwrót, każdy taki ułamek k/d możemy jednoznacznie rozszerzyć do ułamka a/n. Na tej podstawie tworzymy bijekcję zbiorów μ_n i $\bigcup_{d \mid n} \mu_d^\star$ określoną przez $\zeta_n^a \mapsto \zeta_d^k$ (k/d jest postacią nieskracalną ułamka a/n). Pozostaje jeszcze zauważyć, że wówczas $\zeta_n^a = e^{2a\pi/n} = e^{2k\pi/d} = \zeta_d^k$, więc ta bijekcja jest identycznością.
Z udowodnionej równości wynika, że

$$x^n - 1 = \prod_{\zeta \in \mu_n}(x - \zeta) = \prod_{d \mid n} \prod_{\zeta \in \mu_d^\star}(x - \zeta),$$

co kończy dowód lematu.

Dowód twierdzenia 1. Oczywiście wielomiany $\Phi_m(x)$ z lematu są unormowane. Wybierzmy dowolne $n > 1$ i załóżmy indukcyjnie, że wielomiany Φ_m mają wszystkie współczynniki całkowite dla każdego $m < n$. Niech $\Psi_n(x) = \prod_{d \mid n, d < n} \Phi_d(x)$. Z lematu wynika, że $\Phi_n(x)\Psi_n(x) = (x^n - 1)$. Na mocy założenia indukcyjnego $\Psi_n(x)$ to unormowany wielomian o współczynnikach całkowitych, skąd (i z poprzedniej równości) $\Phi_n(x)$ też ma współczynniki całkowite, co kończy dowód indukcyjny i uzasadnienie istnienia postulowanych w twierdzeniu 1 wielomianów. Analogiczną indukcją dowodzimy jednoznaczności (wielomiany Φ_d opisane w twierdzeniu dla $d < n$, $d \mid n$ oraz równość (1) jednoznacznie wyznaczają wartości wielomianu Φ_n).

Dowód twierdzenia 2. Ponieważ $\Phi_1(x) = x - 1$ i $\Phi_2(x) = x + 1$, teza jest oczywista dla $n \leqslant 2$. Dalej niech $n \geqslant 3$. Jeśli $\zeta \in \mu_n^\star$, to $|\zeta| = 1$ i $\zeta \neq \pm 1$. Wobec tego $x - 1 < |x - \zeta| < x + 1$. Stopień wielomianu $\Phi_n(x)$ jest równy $|\mu_n^\star| = \varphi(n)$. Wynika z tego, że $(x-1)^{\varphi(n)} < |\Phi_n(x)| < (x+1)^{\varphi(n)}$. Pozostaje zauważyć, że dla $n \geqslant 3$ wielomian $\Phi_n(x)$ jest unormowany i nie ma pierwiastków rzeczywistych, więc $\Phi_n(x) > 0$ dla wszystkich rzeczywistych x, czyli $|\Phi_n(x)| = \Phi_n(x)$.

Zadania

1. Udowodnić, że istnieją liczby naturalne $a_1, a_2, \ldots, a_{15} > 1$ spełniające równość $a_1 a_2 \ldots a_{15} = 2^{2024} - 1$.
2. Wyznaczyć wszystkie liczby naturalne n, dla których liczba $n^{10} + n^5 + 1$ jest pierwsza.
3. Niech p i q będą dwiema różnymi liczbami pierwszymi i niech $n \geqslant 2$ będzie liczbą naturalną. Dowieść, że liczby $1 + n^p + n^{2p} + \ldots + n^{(q-1)p}$ i $1 + n^q + n^{2q} + \ldots + n^{(p-1)q}$ mają wspólny dzielnik większy niż 1.
4. Niech $a > 1$ będzie liczbą naturalną. Dowieść, że jeśli $a^{(k-1)n} + \ldots + a^{2n} + a^n + 1$ jest liczbą pierwszą, to k jest liczbą pierwszą, a n jest jej potęgą.
5. Niech p będzie dzielnikiem pierwszym liczby $2^{n!} - 1$. Udowodnić, że $p^{H_n} \leqslant 3^{n!}$, przy czym $H_n = 1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n}$.
6. Wykazać, że istnieje nieskończenie wiele liczb naturalnych a o następującej własności: każdy dzielnik pierwszy liczby $a^2 + a + 1$ jest mniejszy od $\sqrt{a}$.

Wskazówki do zadań

1. Liczba 2024 ma 16 dzielników.
Wykorzystać wzór (1) i nierówność (2).
2. Zachodzą równości:
$n^{10} + n^5 + 1 = \frac{n^{15}-1}{n^5-1} =$
$= \frac{\Phi_1(n)\Phi_3(n)\Phi_5(n)\Phi_{15}(n)}{\Phi_1(n)\Phi_5(n)} = \Phi_3(n)\Phi_{15}(n)$.
3. Te liczby to $\Phi_q(n)\Phi_{pq}(n)$ i $\Phi_p(n)\Phi_{pq}(n)$.
4. Mamy $a^{(k-1)n} + \ldots + a^{2n} + a^n + 1 = \frac{a^{kn}-1}{a^n-1} = \frac{\prod_{d \mid kn} \Phi_d(a)}{\prod_{d \mid n} \Phi_d(a)}$. Warunkiem koniecznym pierwszości tej liczby jest istnienie dokładnie jednego dzielnika liczby kn, który nie jest dzielnikiem liczby n.
5. Udowodnimy najpierw, że $\varphi(n!) \leqslant n!/H_n$.
Jeśli $p_1, p_2, \ldots, p_k$ są wszystkimi liczbami pierwszymi w zbiorze $\{1, 2, \ldots, n\}$, to $\varphi(n!) = n! \prod_{i=1}^k \left(1 - \frac{1}{p_i}\right)$. Trzeba zatem wykazać, że powyższy iloczyn nie przekracza $1/H_n$. Jego odwrotność jest równa $\prod_{i=1}^k \left(1 + \frac{1}{p_i} + \frac{1}{p_i^2} + \cdots\right)$, co jest nie mniejsze niż H_n, gdyż po wymnożeniu otrzymamy sumę, w której wystąpuje każda z liczb: $1, \frac{1}{2}, \frac{1}{3}, \ldots, \frac{1}{n}$.
Teraz pozostaje skorzystać z nierówności (2).
6. Weźmy $a = 2^{n^3/3}$ dla pewnego naturalnego $n \geqslant 3$. Wtedy $a^2 + a + 1 \mid a^3 - 1$, więc każdy pierwszy dzielnik $a^2 + a + 1$ jest dzielnikiem pierwszym liczby $2^{n!} - 1$. Tu można skorzystać z poprzedniego zadania – wystarczy dobrać odpowiednio duże n.