Wielomiany Cyklotomiczne

Łukasz Próchniak i Antoni Łuczak

14.03.2024

Wielomiany cyklotomiczne i ich podstawowe własności

Definicja 1 (Pierwiastek n-tego stopnia z jedynki)

Oznaczmy przez $\omega = \omega_n = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n} = e^{\frac{2\pi i}{n}}$ pierwiastek n-tego stopnia z jedynki o najmniejszym dodatnim argumencie.

Zauważmy, że $\omega, \omega^2, \ldots, \omega^n$ są pierwiastkami równania $X^n - 1 = 0$, więc korzystając z Zasadniczego Twierdzenia Algebry są to wszystkie pierwiastki tego wielomianu.

Pierwotnym pierwiastkiem n-tego stopnia z jedynki nazwiemy ω_n^k, że $\mathrm{NWD}(n,k) = 1$. Dla skrócenia zapisu oznaczamy $k \perp n$.

Definicja 2

Niech n będzie liczbą całkowitą dodatnią. Wielomian

$$\Phi_n(X) = \prod_{k\perp n}(X - \omega_n^k)$$

gdzie iloczyn rozciąga się po wszystkich takich k, że $1 \leqslant k \leqslant n$ oraz $\mathrm{NWD}(k,n) = 1$, nazywamy n-tym wielomianem cyklotomicznym.

Definicja ta może wydawać się na pierwszy rzut oka "bezużyteczna". Jednak okazuje się, że wielomiany cyklotomiczne są mocno powiązane z wielomianami $X^n - 1$. Zachodzi następująca równość.

Twierdzenie 1

$$X^n - 1 = \prod_{d|n}\Phi_d(X)$$

gdzie iloczyn rozciąga się po dzielnikach d liczby n.

Dowód. Możemy tutaj szukać analogii do znanej tożsamości $\sum_{d|n}\varphi(d) = n$ i słusznie. Jak już wcześniej wspomnieliśmy $X^n - 1 = (X-\omega)(X-\omega^2)\ldots(X-\omega^n)$. Pogrupujmy pierwiastki tego wielomianu. Zauważmy, że $\omega_n^k = \omega_{\frac{n}{d}}^{\frac{k}{d}}$ jest również pierwiastkiem wielomianu $\Phi_{\frac{n}{d}}$, gdzie $d = \mathrm{NWD}(n,k)$. W ten sposób tworząc bijekcję, otrzymujemy $X^n - 1 = \prod_{d|n}\Phi_{\frac{n}{d}}(X) = \prod_{d|n}\Phi_d(X)$ □

Aby oswoić się z notacją podamy kilka pierwszych wielomianów cyklotymicznych. Dla $n = 1$ otrzymujemy $\Phi_1 = X - 1$. Dla $n = 2$ otrzymujemy $\Phi_2 = X + 1$. W szczególności dla liczb pierwszych p otrzymujemy

$$\Phi_p = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \cdots + X + 1$$

Dla $n = 4, 6, 8, 9, 10$ dostaniemy kolejno

$$\Phi_4 = \frac{X^4}{\Phi_2\Phi_1} = \frac{X^4 - 1}{(X+1)(X-1)} = X^2 + 1$$
$$\Phi_6 = \frac{X^6 - 1}{\Phi_3\Phi_2\Phi_1} = \frac{X^6 - 1}{(X^2+X+1)(X+1)(X-1)} = X^2 - X + 1$$
$$\Phi_8 = \frac{X^8 - 1}{\Phi_4\Phi_2\Phi_1} = \frac{X^8 - 1}{(X^2+1)(X+1)(X-1)} = X^4 + 1$$
$$\Phi_{10} = \frac{X^{10} - 1}{\Phi_5\Phi_2\Phi_1} = \frac{X^{10} - 1}{(X^4+X^3+X^2+X+1)(X+1)(X-1)} = X^4 - X^3 + X^2 - X + 1$$

Wniosek 1. Porównując najwyższe stopnie w wielomianach w Lemacie 1. otrzymujemy równość $\sum_{d|n} \varphi(d) = n$.

Wprowadzimy pojęcie funkcji Möbiusa, która pozwoli wprowadzić nam nową definicję Φ_n.

Definicja 3 (Funkcja Möbiusa)

Funkcja Möbiusa $\mu : \mathbb{Z}_+ \to \{-1, 0, 1\}$ jest zdefiniowana następująco

$$\mu(n) = \begin{cases} 1 & \text{jeśli } n = 1 \\ (-1)^k & \text{jeśli } n \text{ jest liczbą bezkwadratową oraz } k \text{ jest liczbą dzielników pierwszych } n \\ 0 & \text{w pozostałych przypadkach} \end{cases}$$

Ćwiczenie 1. Pokazać, że μ jest funkcją arytmetyczną, to znaczy jeśli $a \perp b$, to $\mu(ab) = \mu(a) \cdot \mu(b)$.

Twierdzenie 2 (Inwersja Möbiusa)

Załóżmy, że $f : \mathbb{Z}_+ \to \mathbb{Z}_+$ jest funkcją arytmetyczną oraz F, H będą takimi funkcjami, że

$$F(n) = \sum_{d|n} f(d), \; H(n) = \prod_{d|n} f(d)$$

wtedy

$$f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) = \prod_{d|n} H\left(\frac{n}{d}\right)^{\mu(d)}$$

Dowód. Po dowód twierdzenia odsyłamy do załącznika [6]. □

Można zauważyć, że podobna sytuacja zachodzi dla wielomianów cyklotomicznych.

Twierdzenie 3

$$\Phi_n(X) = \prod_{d|n} (X^{\frac{n}{d}} - 1)^{\mu(d)}$$

Dowód. Dowód wynika natychmiastowo z inwersji Möbiusa. □

Rozpatrując kolejne wielomiany cyklotomiczne można dojść do wniosku, że być może współczynniki Φ_n są całkowite. Rzeczywiście tak jest. Aby tego dowieść wprowadźmy najpierw całkiem przydatny lemat.

Lemat 1 (Lemat Gaussa)

Niech $f(X) = X^m + a_{m-1}X^{m-1} + \cdots + a_1X + a_0$ oraz $g(X) = X^n + b_{n-1}X^{n-1} + \cdots + b_1X + b_0$ będą wielomianami o współczynnikach wymiernych. Niech $h = f \cdot g$ będzie wielomianem o współczynnikach całkowitych. Wtedy f oraz g również są wielomianami o współczynnikach całkowitych.

Dowód. Niech M i N będą najmniejszymi takimi liczbami, że $Mf(X)$ oraz $Ng(X)$ mają wszystkie współczynniki całkowite. Niech $A_i = Ma_i$ dla $i = 0, 1, \ldots, m-1$ oraz $A_m = M$. Zauważmy, że skoro h ma współczynniki całkowite, to $(MN)h$ ma wszystkie współczynniki podzielne przez MN. Wystarczy pokazać, że $MN = 1$. Załóżmy, że $MN > 1$. Weźmy dowolny dzielnik pierwszy p liczby MN. Wtedy istnieje liczba A_i, że $p \nmid A_i$. Jeśli $p \nmid M$, to $p \nmid A_m$. Załóżmy, że $p \mid M$. Wtedy dla każdego i zachodzi $p \mid A_i$, więc $A_i/p = (M/p)a_i \in \mathbb{Z}$. Oznacza to, że można byłoby zmniejszyć M do M/p, co jest sprzeczne z minimalnością M. Analogicznie istnieje B_j, że $p \nmid B_j$. Weźmy największe takie A_i oraz B_j spełniające powyższe własności. Rozpatrzmy współczynnik przy X^{i+j} w wielomianie h

$$[X^{i+j}] = \cdots + A_{i+1}B_{j-1} + A_iB_j + A_{i-1}B_{j+1} + \cdots = pk + A_iB_j$$

Zauważmy, że każdy składnik oprócz A_iB_j jest podzielny przez p, więc współczynnik przy X^{i+j} nie jest podzielny przez MN, sprzeczność. □

Lemat 2

Współczynniki wielomianu Φ_n są liczbami całkowitymi.

Dowód. Wykażemy tezę indukcyjnie. Teza zachodzi dla $n = 1$, otóż $\Phi_1 = X - 1$. Załóżmy, że teza zachodzi dla wszystkich $k < n$. Wtedy z Lematu 1. mamy

$$\Phi_n(X) = \frac{X^n - 1}{\prod_{d|n, d\neq n} \Phi_d(X)}$$

Zatem współczynniki Φ_n są wymierne, a z Lematu Gaussa całkowite. □

W tym rozdziale przedstawimy jeszcze bardzo przydatne nierówności dotyczące wielomianów cyklotomicznych i przejdziemy do paru zadanek.

Twierdzenie 4

Dla $x \geqslant 1$ zachodzą nierówności:

$$(x-1)^{\varphi(n)} \leqslant |\Phi_n(x)| \leqslant (x+1)^{\varphi(n)}$$

przy czym ostra nierówność po lewej stronie zachodzi dla $n \geqslant 2$, a dla prawej strony dla $n \geqslant 3$. W szczególności dla $n \geqslant 2$ i $x \geqslant 2$ zachodzi $\Phi_n(x) > 1$.

Dowód. Dla $n = 1, 2$ mamy $\Phi_1 = X - 1$ oraz $\Phi_2 = X + 1$. Załóżmy, że $n > 2$. Niech $\omega_n^k \neq 1, -1$ będzie pierwiastkiem pierwotnym Φ_n. Z nierówności trójkąta zachodzi $X - 1 = X - |\omega_n^k| < |X - \omega_n^k| < X + |\omega_n^k| = X + 1$. Mnożąc te nierówności dla wszystkich pierwiastków pierwotnych otrzymujemy tezę. □

Zadanka cz. I

1. Wyznaczyć wszystkie liczby n, że $n^{10} + n^5 + 1$ jest liczbą pierwszą.
2. Niech $a > 1$ będzie liczbą całkowitą. Dowieść, że jeśli $a^{(k-1)n} + \cdots + a^{2n} + a^n + 1$ jest liczbą pierwszą, to k jest liczbą pierwszą, a n jest jej potęgą.
3. Niech p będzie dzielnikiem pierwszym liczby $2^{n!} - 1$. Udowodnić, że $p^{H_n} \leqslant 3^{n!}$, przy czym $H_n = 1 + \frac{1}{2} + \cdots + \frac{1}{n}$.
4. Wykazać, że istnieje nieskończenie wiele liczb naturalnych a, że każdy dzielnik pierwszy liczby $a^2 + a + 1$ jest mniejszy od $\sqrt{a}$.

Więcej własności wielomianów cyklotomicznych

Lemat 3

Niech p będzie liczbą pierwszą. Wtedy

$$\Phi_{pn}(X) = \begin{cases} \Phi_n(X^p) & \text{jeśli } p \mid n \\ \frac{\Phi_n(X^p)}{\Phi_n(X)} & \text{jeśli } p \nmid n. \end{cases}$$

Dowód. Załóżmy najpierw, że $p \mid n$. Wtedy, korzystając z Lematu 3, otrzymujemy

$$\begin{aligned} \Phi_{pn}(X) &= \prod_{d \mid pn} (X^{\frac{n}{d}} - 1)^{\mu(d)} \\ &= \left(\prod_{d \mid n} (X^{\frac{pn}{d}} - 1)^{\mu(d)} \right) \left(\prod_{\substack{d \mid pn \\ d \nmid n}} (X^{\frac{n}{d}} - 1)^{\mu(d)} \right) \\ &= \Phi_n(X^p) \prod_{\substack{d \mid pn \\ d \nmid n}} (X^{\frac{n}{d}} - 1)^{\mu(d)} \end{aligned}$$

Jednak skoro $d \mid pn$ oraz $d \nmid n$, to $p^2 \mid d$, ponieważ $p \mid n$, więc $\mu(d) = 0$ i drugi iloczyn będzie równy 1, wiec $\Phi_{pn}(X) = \Phi_n(X^p)$. Załóżmy teraz, że $p \nmid n$. Wtedy

$$\begin{aligned} \Phi_{pn}(X) &= \prod_{d \mid pn} (X^{\frac{n}{d}} - 1)^{\mu(d)} \\ &= \left(\prod_{d \mid n} (X^{\frac{pn}{d}} - 1)^{\mu(d)} \right) \left(\prod_{d \mid n} (X^{\frac{pn}{pd}} - 1)^{\mu(pd)} \right) \\ &= \left(\prod_{d \mid n} (X^{\frac{pn}{d}} - 1)^{\mu(d)} \right) \left(\prod_{d \mid n} (X^{\frac{pn}{pd}} - 1)^{-\mu(d)} \right) \\ &= \frac{\Phi_n(X^p)}{\Phi_n(X)} \end{aligned}$$

□

Wniosek 2. Korzystając z Lematu 4. wielokrotnie otrzymujemy

$$\Phi_{p^k n}(X) = \begin{cases} \Phi_n(X^{p^k}) & \text{jeśli } p \mid n \\ \frac{\Phi_n(X^{p^k})}{\Phi_n(X^{p^{k-1}})} & \text{jeśli } p \nmid n. \end{cases}$$

Ćwiczenie 2. Udowodnić, że jeśli każdy dzielnik pierwszy t jest dzielnikiem pierwszym m, to $\Phi_{mt}(X) = \Phi_m(X^t)$.

Ćwiczenie 3. Udowodnić, że jeśli $n \equiv 2 \pmod 4$, to $\Phi_n(X) = \Phi_{n/2}(-X)$.

Twierdzenie 5

Dla dowolnych względnie pierwszych dodatnich liczb całkowitych a, n zachodzi

$$\Phi_n(x^a) = \prod_{d \mid n} \Phi_{nd}(x)$$

Dowód. Łatwo można sprawdzić, że stopnie wielomianów po obu stronach się zgadzają. Wystarczy pokazać, że każdy pierwiastek wielomianu po prawej stronie jest również pierwiastkiem po lewej stronie. Każdy pierwiastek z prawej strony jest postaci $x = \omega_{nd}^k$, gdzie $d \mid a, \mathrm{NWD}(k, nd) = 1$. Wtedy $x^a = \omega_{nd}^{ka} = \omega_n^{k\frac{a}{d}}$, gdzie $\mathrm{NWD}(ka/d, n) = \mathrm{NWD}(k, n) = \mathrm{NWD}(a/d, n) = 1$ jest pierwiastkiem $\Phi_n(x)$. □

Twierdzenie 6

Współczynniki wielomianu Φ_{pq} należą do zbioru $\{1, 0, -1\}$, gdzie p, q są różnymi liczbami pierwszymi.

Dowód. Zachodzi następująca tożsamość.

$$(X^{pq} - 1)\Phi_{pq}(X) = \Phi_q(X^p)\Phi_p(X^q)(X - 1)$$

którą otrzymuje się natychmiastowo z Lematu 3. oraz Twierdzenia 1.
Pokażemy najpierw następujący lemat. Jeśli p, q są różnymi liczbami pierwszymi, to współczynniki wielomianu $\Phi_p(X^q)\Phi_q(X^p)$ należą do zbioru $\{0, 1\}$.

$$\Phi_p(X^q)\Phi_q(X^p) = (X^{(p-1)q} + \cdots + X^q + 1)(X^{(q-1)p} + \cdots + X^p + 1) = \sum_{\substack{0 \leqslant m < q \\ 0 \leqslant n < p}} X^{mp+nq}$$

Załóżmy, że dla pewnych m, n, m', n' zachodzi $mp+nq = m'p+n'q$, wtedy $p(m-m') = q(n'-n)$, co prowadzi do sprzeczności. Wracając do początkowej tożsamości. Zauważmy, że stopień wielomianu $\Phi_{pq}(X)$, który jest równy $\varphi(pq) = (p-1)(q-1) < pq$, więc jeśli współczynniki $(X^{pq} - 1)\Phi_{pq}(X)$ należą do zbioru $\{1, 0, -1\}$, to $\Phi_{pq}(X)$ także. Zauważmy, że współczynniki $X\Phi_q(X^p)\Phi_p(X^q)$ należą do zbioru $\{0, 1\}$, natomiast współczynniki $-\Phi_q(X^p)\Phi_p(X^q)$ do zbioru $\{-1, 0\}$, więc rzeczywiście otrzymaliśmy tezę. □

Wniosek 3. Jeśli n ma co najwyżej dwa dzielniki pierwsze, to współczynniki wielomianu $\Phi_n(X)$ należą do zbioru $\{-1, 0, 1\}$.

Rozkład $\Phi_n(X)$ na dzielniki pierwsze

Definicja 4 (Wykładnik p-adyczny)

Niech p będzie liczbą pierwszą. Wykładnikiem p-adycznym liczby n nazwiemy największą taką liczbę całkowitą $v_p(n) = s$, że $p^s \mid n$.

Twierdzenie 7 (LTE)

Niech p będzie liczbą pierwszą, $n \geqslant 1$ liczbą naturalną, a, b liczbami całkowitymi niepodzielnymi przez p, takimi że $p \mid a - b$.

(1) Jeśli $p \neq 2$, to
$$v_p(a^n - b^n) = v_p(a - b) + v_p(n)$$

(2) Jeśli $p = 2$ oraz $4 \mid a - b$, to
$$v_2(a^n - b^n) = v_2(a - b) + v_2(n)$$

(3) Jeśli $p = 2$ oraz $4 \nmid a - b$, to
$$v_2(a^n - b^n) = v_2(a - b) + v_2(n) + v_2(a + b) - 1$$

Dowód. Po dowód twierdzenia odsyłamy do [3]. □

Definicja 5 (Rząd a modulo p)

Rzędem $r = \mathrm{ord}_p(a)$ nazwiemy najmniejszą liczbę całkowitą taką, że $a^r \equiv 1 \pmod{p}$.

Ćwiczenie 4. Jeśli $p \mid a^m - 1$, to $\mathrm{ord}_p(a) \mid m$.

Załóżmy, że $p \mid \Phi_n(a) \mid a^n - 1$. Wtedy $r = \mathrm{ord}_p(a) \mid n$. Oznaczmy $n = rmp^k$, przy czym $p \nmid m$. Dla $p > 2$ otrzymamy

$$v_p(a^r - 1) + k = v_p(a^n - 1) = \sum_{D|n} v_p(\Phi_D(a)) = \sum_{d|m} \sum_{j=0}^{k} v_p(\Phi_{rdp^j}(a))$$

Przy czym trzecia równość wynika z faktu, że $v_p(\Phi_D(a))$ jest niezerowe, gdy $p \mid \Phi_D(a) \mid a^D - 1$, czyli $r \mid D$. Z powyższej równości wynikają kolejno:

(i) jeśli $n = r$, to $v_p(\Phi_n(a)) = v_p(a^r - 1)$

(ii) jeśli $n = rp^k$, gdzie $k > 0$, to $v_p(\Phi_n(a)) = 1$

(iii) jeśli $n = rmp^k$, gdzie $k > 0, m > 1$, to $v_p(\Phi_n(a)) = 0$.

Dowód przebiega analogicznie dla $p = 2$ i $n \geqslant 3$. Pierwsza implikacja jest oczywista. Druga implikacja wynika z indukcji po k. Natomiast trzecia wynika z drugiej. *Dzielnikami trywialnymi* $\Phi_n(a)$ nazwiemy takie $p \mid \Phi_n(a)$, że $n = rp^k$. Natomiast *dzielnikami nietrywialnymi* $\Phi_n(a)$ nazwiemy takie, że $n = \mathrm{ord}_p(a)$. Zauważmy, że $\Phi_n(a)$ ma co najwyżej jeden dzielnik trywialny. Jest tak ponieważ $p \mid a^r - 1$ oraz $p \mid a^{p-1} - 1$ z Małego Twierdzenia Fermata, zatem $r \mid p - 1$, czyli $r < p$.

Pokażemy teraz, że prawie zawsze znajdziemy dzielnik nietrywialny. Niech p będzie największym dzielnikiem pierwszym liczby n. Wystarczy pokazać, że $\Phi_n(a) > p$. Wtedy nawet gdy p byłby dzielnikiem trywialnym, to z faktu, że $v_p(\Phi_n(a)) = 1$ istniałby inny dzielnik pierwszy - nietrywialny. Oznaczmy $n = pm$. Skorzystamy z udowodnionej wcześniej tożsamości w Lemacie 3 oraz nierówności Twierdzenia 2.

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

Jest oczywiste, że $\frac{2^p-1}{3} > p$ dla $p > 3$. Natomiast jeśli $p = 2$, to $n = 2^k = 2t$, więc $\Phi_n(a) = \Phi_2(a^t) = a^t + 1 > 2$. Dla $p = 3$ mamy dwie możliwości. Jedna to $n = 3^k = 3t$ mamy $\Phi_n(a) = \Phi_3(a^t) = a^{2t} + a^t + 1 > 3$. Jeśli $n = 2^{k_1}3^{k_2} = 6t$, to mamy $\Phi_n(a) = \Phi_6(a^t) = a^{2t} - 2^t + 1$, 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 mamy poszukiwanego dzielnika nietrywialnego. Pokazaliśmy zatem następujące twierdzenie:

Twierdzenie 8 (Tw. Bzdęgi)

Jeśli $n \geqslant 3, a \geqslant 2$ oraz $(n, a) \neq (6, 2)$, to liczba $\Phi_n(a)$ ma nietrywialny dzielnik pierwszy p, czyli $n = \mathrm{ord}_p(a)$ dla pewnego p.

Na koniec dodaję całkiem przydatny lemat, którzy przyda się w niektórych zadaniach i w późniejszych dowodach.

Lemat 4

Dane są liczby całkowite względnie pierwsze $a > b > 1$ oraz $n \geqslant m \geqslant 1$. Zachodzi wówczas równość

$$\mathrm{NWD}(a^n - b^n, a^m - b^m) = a^{\mathrm{NWD}(n,m)} - b^{\mathrm{NWD}(n,m)}$$

Dowód. Dla uproszczenia ustalmy oznaczanie $x_n = a^n - b^n$. Jest oczywiste, że jeśli $m \mid n$, to $x_m \mid x_n$ i $x_{\mathrm{NWD}(n,m)} \mid \mathrm{NWD}(x_m, x_n)$. Pokażemy implikację w drugą stronę. Zauważmy, że

$$x_n = a^m x_{n-m} + b^{n-m} x_m$$

Zatem skoro x_n jest względnie pierwsze z a, to $\mathrm{NWD}(x_n, x_m) \mid x_{n-m}$. Zatem indukcyjnie przechodzimy z pary (n, m) do $(n - m, m)$. Na końcu dostajemy parę $(\mathrm{NWD}(n, m), 0)$, czyli $\mathrm{NWD}(x_n, x_m) \mid x_{\mathrm{NWD}(n,m)}$. Mamy podzielności w dwie strony, więc $\mathrm{NWD}(x_n, x_m) = x_{\mathrm{NWD}(n,m)}$. □

Zadanka cz. II

1. Udowodnić, że jeśli $\mathrm{NWD}(\Phi_n(a), \Phi_m(a)) > 1$, to $\frac{m}{n} = p^\alpha$ dla pewnej liczby pierwszej p.
2. Niech $\omega(n)$ oznacza liczbę różnych dzielników pierwszych n. Wykazać, że dla nieparzystego n zachodzi $\omega(2^n - 1) \geqslant 2^{\omega(n)} - 1$.
3. (a) Udowodnić, że każdy wyraz ciągu $2^2 - 1, 2^3 - 1, 2^4 - 1, \ldots$ ma dzielnik pierwszy, którego nie ma żaden wyraz poprzedni, za wyjątkiem $2^6 - 1$.
   (b) Udowodnić, że każdy wyraz ciągu $2^1 + 1, 2^2 + 1, 2^3 + 1, \ldots$ ma dzielnik pierwszy, którego nie ma żaden wyraz poprzedni, za wyjątkiem $2^3 + 1$.
4. Znajdź wszystkie liczby całkowite dodatnie $a, n > 1$ oraz k, że $3^k - 1 = a^n$.
5. Znajdź wszystkie trójki liczb naturalnych $a, m, n \geqslant 2$, dla których zachodzi równość $a^m + 1 = (a+1)^n$.
6. (ISL 2006) Znajdź wszystkie liczby całkowite x, y spełniające równanie:
$$\frac{x^7 - 1}{x - 1} = y^5 - 1$$
7. *(Szczególny case tw. Dirichleta)* Udowodnić, że dla każdego $n \geqslant 1$ całkowitego istnieje nieskończenie wiele liczb pierwszych w ciągu arytmetycznym $an + 1$.
8. (upgrade ISL 2002) Niech $p_1, \ldots, p_n$ będą różnymi liczbami pierwszymi większymi niż 3. Udowodnij, że $2^{p_1 p_2 \cdots p_n} + 1$ ma co najmniej $2^{2^{n-1}}$ dzielników.
9. Udowodnić, że istnieje nieskończenie wiele liczb naturalnych n, których nie można przedstawić w postaci
$$\frac{p^a - p^b}{p^c - p^d}$$
gdzie p jest liczbą pierwszą, a, b, c, d są liczbami całkowitymi dodatnimi.

Dowód Twierdzenia Zsigmondy'ego

Wprowadzimy nowe oznaczenia, które pozwolą nam opisywać liczby postaci $a^n - b^n = b^n \prod_{d|n} \Phi_d(a/b)$.

Definicja 6

$$\Phi_n = \Phi_n(a, b) = b^{\varphi(n)} \Phi_n\left(\frac{a}{b}\right)$$

Wtedy oczywiście zachodzą równości udowodnione wcześniej dla $\Phi_n(a)$:

(i) $a^n - b^n = \prod_{d|n} \Phi_d(a, b)$

(ii) $\Phi_n(a, b) = \prod_{d|n} (a^{\frac{n}{d}} - b^{\frac{n}{d}})^{\mu(d)}$

(iii) Niech $n = p^\alpha r$, gdzie $\alpha = v_p(n) \geqslant 1$. Wtedy $\Phi_n(a, b) = \frac{\Phi_r\left(a^{p^\alpha} - b^{p^\alpha}\right)}{\Phi_r\left(a^{p^{\alpha-1}}, b^{p^{\alpha-1}}\right)}$

Od tej pory będziemy rozważać jedynie przypadki $a > b \geqslant 1$, $a \perp b$. Wprowadzimy oznaczenie $z_n = a^n - b^n$. Liczbę pierwszą p nazwiemy *dzielnikiem pierwotnym* liczby z_n, jeśli dla $p \nmid z_k$ dla każdego $k < n$. Zauważmy, że możemy ograniczyć rozpatrywanie k do dzielników n, ponieważ jeśli $p \mid z_m$ oraz $p \mid z_n$, to z Lematu 4. $p \mid z_{\mathrm{NWD}(m,n)}$. Wprowadźmy oznaczenia $P_n = P_n(a, b)$, czyli zbiór dzielników pierwotnych z_n oraz $D(n)$, czyli zbiór dzielników pierwszych n. Udowodnimy następujące twierdzenie:

Twierdzenie 9 (Twierdzenie Zsigmondy'ego)

Niech a, b będą liczbami całkowitymi, że $\mathrm{NWD}(a,b) = 1$ oraz $n > 1$. Wtedy dla każdego n istnieje dzielnik pierwszy, który dzieli $a^n - b^n$, ale nie dzieli żadnej z liczb $a^k - b^k$ dla wszystkich $k < n$ poza następującymi przypadkami

- $2^6 - 1^6$
- $n = 2$ oraz $a + b = 2^s$

Dowód przebiega analogicznie do przeprowadzanego wcześniej dla $a^n - 1$, będziemy mieć jedynie więcej przypadków granicznych.

Krok I: $P_n \subseteq D(\Phi_n)$ oraz $P_n \cap D(\Phi_k) = \varnothing$ dla $k \mid n$ oraz $k < n$.
Zauważmy najpierw, że $D(z_n) = \bigcup_{k|n} D(\Phi_k)$. Gdyby $p \in P_n$ należałoby do $D(\Phi_k)$ dla pewnego k, to $p \mid a^k - b^k$, więc p nie byłoby dzielnikiem pierwotnym z_n. Zatem $P_n \cap D(\Phi_k) = \varnothing$ dla $k \mid n$ oraz $k < n$, z czego wynika, że $P_n \subseteq D(\Phi_n)$. Wprowadźmy oznaczenie λ_n jako zbiór dzielników niepierwotnych, że $D(\Phi_n) = P_n \sqcup \lambda_n$. Będziemy chcieli pokazać, że $P_n \neq \varnothing$ ograniczając λ_n. **Krok II:** $p^\alpha \mid \Phi_n(a,b) \iff p \nmid b$ oraz $p^\alpha \mid \Phi_n(ab^{-1})$, gdzie $\alpha \geqslant 1$.
Niech p będzie dzielnikiem pierwszym $p^\alpha \mid \Phi_n = b^{\varphi(n)}\Phi_n(a/b)$. Wtedy $p^\alpha \mid a^n - b^n$. Gdyby $p^\alpha \mid b$, to $p^\alpha \mid a$ oraz $\mathrm{NWD}(a,b) > 1$, sprzeczność. Zatem $p \nmid b$, czyli istnieje odwrotność b^{-1} modulo p^α. Możemy zatem napisać $p^\alpha \mid \Phi_n(ab^{-1})$.

Krok III: Korzystając z dowodu Tw. Bzdęgi mamy, że istnieje maksymalnie jeden dzielnik niepierwotny $p \in \lambda_n$(będącym dzielnikiem n), a gdy $p > 2$, to zachodzi dodatkowo dla niego $v_p(\Phi_n(a,b)) = v_p(\Phi(ab^{-1})) = 1$. Tak jak wtedy chcemy pokazać, że $\Phi_n(a,b) > p$. Pozostaje rozpatrzeć graniczne przypadki. Jednak jeszcze przed tym przedstawimy ogólniejszą wersję nierówności z Twierdzenia 2, która od razu z niej wynika:

$$(a-b)^{\varphi(n)} \leqslant |\Phi_n(a,b)| \leqslant (a+b)^{\varphi(n)} \tag{1}$$

Krok IV: Jeżeli $\lambda_n = \{2\}$ i $P_n = \varnothing$, to $n = 2$ oraz $a + b = 2^s$.
Wtedy $\Phi_n = 2^s$ dla $s \geqslant 1$. Z kroku III mamy, że $2 \mid n$, więc jeśli oznaczymy $n = 2^\alpha r$, to skoro r jest rzędem modulo $p = 2$, to $r = 1$, więc $n = 2^\alpha$. Zachodzi

$$\Phi_n(a,b) = \frac{\Phi_1\left(a^{2^\alpha} - b^{2^\alpha}\right)}{\Phi_1\left(a^{2^{\alpha-1}}, b^{2^{\alpha-1}}\right)} = a^{2^{\alpha-1}} + b^{2^{\alpha-1}} = 2^s$$

Łatwo widząc, że $a + b > 2$, czyli $s \geqslant 2$ mamy, że $\alpha = 1$. Gdyby $\alpha \geqslant 2$, to zapisując $a = 1 + 2c, b = 1 + 2d$, mamy $2^s = 2 + 2^2 A$.
Krok V: Jeśli $\lambda_n = \{p\}$, $p > 2$ oraz $a - b \geqslant 2$, to $P_n \neq \varnothing$.
Wtedy $\Phi_n = p$. Z założenia, że $a - b \geqslant 2$ oraz nierówności (1) wynika, że $p > 2^{\varphi(n)} \geqslant 2^{p-1}$, ponieważ $p \mid n$, co prowadzi do sprzeczności.
Krok VI: Jeżeli $\lambda_n = \{p\}$, $p > 2$ i $P_n = \varnothing$ oraz $a - b = 1$, to $n = 6$ i $a = 2, b = 1$.
Wtedy $\Phi_n = p$. Tak jak w Kroku IV $n = p^\alpha r$, gdzie $\alpha \geqslant 1$. Załóżmy najpierw, że $\alpha \geqslant 2$. Dostajemy

$$p = \Phi_n = \Phi_{n/p}(a^p, b^p) \geqslant (a^p - b^p)^{\varphi(n/p)} \geqslant (a^p - b^p)^{p-1}$$

co nie ma sensu dla $a - b = 1$ oraz $a > b \geqslant 1$.
Pozostaje przypadek $\alpha = 1$. Wtedy

$$\Phi_n = \frac{\Phi_r(a^p, b^p)}{\Phi_r(a,b)} \geqslant \frac{(a^p - b^p)^{\varphi(r)}}{(a+b)^{\varphi(r)}} \geqslant \frac{a^p - b^p}{a+b} \geqslant \frac{2^p - 2}{3}$$

gdzie trzecia nierówność wynika ze zworu dwumiennego:

$$\frac{a^p - b^p}{a+b} = \frac{(b+1)^p - b^p}{2b+1} = \frac{b}{2b+1}\left(\sum_{j=0}^{p-1} \binom{p}{j} b^{j-1}\right) \geqslant \frac{1}{3}(2^p - 2)$$

bo $\frac{b}{2b+1} \geqslant \frac{1}{3}$ dla $b \geqslant 1$, a $2^p - 2 = (1+1)^p - 2 = \sum_{i=0}^{p-1} \binom{p}{i}$. Nierówność $3p \geqslant 2^p - 2$ jest prawdziwa jedynie dla $p = 3$. Więc $n = 3r$. Wiedząc, że $3 \mid (ab^{-1})^r - 1$ mamy, że $r \mid p - 1 = 2$,

więc $n = 3$ lub $n = 6$. Przypadek $n = 3$ odpada, bo $z_1 = a - b = 1$. Pozostaje $n = 6$. Wtedy $\Phi_6(a, b) = a^2 - ab + b^2 = b^2 + b + 1$. Skąd $(b - 1)(b + 2) = 0$. Ostatecznie $b = 1$ i $a = 2$.

Twierdzenie 10 (Plusowe Twierdzenie Zsigmony'ego)

Niech a, b będą liczbami całkowitymi, że $\mathrm{NWD}(a, b) = 1$ oraz $n > 1$. Wtedy dla każdego n istnieje dzielnik pierwszy, który dzieli $a^n + b^n$, ale nie dzieli żadnej z liczb $a^k + b^k$ dla wszystkich $k < n$ poza przypadkiem $2^3 + 1^3$.

Dowód. Pomijamy szczególne przypadki. Zauważmy, że $(a^n - b^n)(a^n + b^n) = (a^{2n} - b^{2n})$. Jednak wystarczy wziąć dowolny pierwotny dzielnik $p \mid a^{2n} - b^{2n}$, który nie będzie pierwotnym dzielnikiem $a^n - b^n$. Co więcej nie jest to także pierwotny dzielnik $a^{2k} - b^{2k} = (a^k - b^k)(a^k + b^k 0$ dla $k < n$, więc $p \nmid a^k + b^k$ dla $k < n$. □

Nierozkładalność Wielomianów Cyklotomicznych

Zacznijmy od udowodnienia następującego lematu:

Lemat 5

Niech $\mathbb{K}$ będzie dowolnym ciałem. Wielomian $f \in \mathbb{K}[x]$ jest względnie pierwszy ze swoją pochodną. Wtedy dla dowolnego niestałego wielomianu $g \in \mathbb{K}[x]$, f nie jest podzielny przez g^2.

Dowód. Załóżmy, że $f = hg^2$ dla pewnego wielomianu $h \in \mathbb{K}[x]$. Różniczkując tę równość obustronnie dostajemy

$$f' = h'g^2 + 2g'gh.$$

Prawa strona równości jest podzielna przez g, zatem wielomian g dzieli wielomian f'. Jednak z założenia wielomian f jest podzielny przez g, zatem dostajemy, że g jest wspólnym dzielnikiem wielomianów f, f', co przeczy założeniu. □

Przejdźmy teraz do udowodnienia następującego twierdzenia

Twierdzenie 11 (Nierozkładalność Wielomianów Cyklotomicznych)

Dla dowolnej liczby naturalnej n, wielomian Φ_n jest nierozkładalny nad $\mathbb{Q}$.

Dowód. Niech ω będzie n-tym pierwotnym pierwiastkiem z jedności oraz niech f będzie jego wielomianem minimalnym nad $\mathbb{Q}$. Niech p będzie liczbą pierwszą nie dzielącą n oraz niech g będzie wielomianem minimalnym liczby ω^p. Zauważmy, że f oraz g dzielą $x^n - 1$, zatem oba mają współczynniki całkowite. Załóżmy nie wprost, że $f \neq g$. W takim razie wielomiany te są względnie pierwsze w $\mathbb{Q}[x]$. W takim razie dla pewnego wielomianu $h \in \mathbb{Z}[x]$ zachodzi

$$x^n - 1 = f(x)g(x)h(x).$$

Zauważmy, że ω jest pierwiastkiem wielomianu $g(x^p)$, zatem $g(x^p) = f(x)k(x)$ dla pewnego wielomianu $k \in \mathbb{Z}[x]$ (ponieważ f jest wielomianem minimalnym ω). Zredukujmy teraz nasze wielomiany modulo p. Mamy teraz

$$g(x)^p = g(x^p) = f(x)k(x).$$

W takim razie, jeśli $q \in \mathbb{F}_p[x]$ jest wielomianem nierozkładalnym, który dzieli f, to również dzieli g. Skoro

$$x^n - 1 = f(x)g(x)h(x),$$

to wielomian $x^n - 1$ jest podzielny przez q^2 w $\mathbb{F}_p[x]$. Stosując poprzedni lemat dla ciała $\mathbb{F}_p$ oraz wielomianów $x^n - 1$, q, dostajemy, że $x^n - 1$ nie może być względnie pierwszy ze swoją pochodną. Jednak $x^n - 1$ jest względnie pierwszy z x oraz n nie jest podzielne przez p, zatem

$$x^n - 1 \perp nx^{n-1},$$

co oznacza sprzeczność. W takim razie rozpatrując nasze wielomiany ponownie nad ciałem $\mathbb{Q}$ dostajemy $f = g$.

Niech teraz ω^m będzie $n-$tym pierwotnym pierwiastkiem z jedności. Skoro jest on pierwotny, to $m = p_1 p_2 \dots p_k$, gdzie $p_1, p_2, \dots, p_k$ są liczbami pierwszymi względnie pierwszymi z n. Wiemy, że ω oraz ω^{p_1} mają ten sam wielomian minimalny. Podobnie dostajemy, że ω^{p_1} oraz $\omega^{p_1 p_2}$ mają ten sam wielomian minimalny itd. Powtarzając to rozumowanie dostajemy, że ω oraz ω^m mają ten sam wielomian minimalny, zatem wszystkie $n-$te pierwotne pierwiastki z jedności mają wspólny wielomian minimalny f. W takim razie dzieli on Φ_n. Jednak stopnie wielomianów f, Φ_n są równe $\varphi(n)$, zatem skoro nasze wielomiany są unormowane, to muszą być sobie równe.

□

Zadanka cz. III

1. (AoPS) Niech a, b będą liczbami całkowitymi dodatnimi, że $a^n + b^n \mid c^n$ jest spełnione dla każdego $n > 1$. Udowodnij, że $a = b$.

2. (Japonia TST 2017) Znajdź wszystkie liczby całkowite k, że istnieje ciąg $a_1, a_2, \dots,$ oraz $r_1, r_2, \dots,$ że spełniane są warunki

   - $a_1 < a_2 < a_3 < \dots$
   - $a_1^k + a_2^k + \dots + a_n^k = (a_1 + a_2 + \dots + a_n)^{r_n}$

3. Niech a będzie ustaloną liczbą całkowitą. Udowodnij, że $\frac{p-1}{\mathrm{ord}_p(a)}$ nie jest ograniczone, gdzie p jest dowolną liczbą pierwszą.

4. Udowodnić, że w nieskończonym ciągu

   $$10001, 100010001, 1000100010001, \dots$$

   nie występuje liczba pierwsza

5. Niech $p \geqslant 3$ będzie liczbą pierwszą. Udowodnij, że jeśli p-kąt ma wszystkie boki wymiernej długości i wszystkie kąty równe, to jest foremny.

Wskazówki do zadań

1.1 Przekształć wyrażenie do $\Phi_3(n)\Phi_{15}(n)$.

1.2 Przekształć wyrażenie do $\frac{\prod_{d|kn}\Phi_d(a)}{\prod_{d|n}\Phi_d(a)}$. Warunkiem koniecznym pierwszości tej liczby jest istnienie dokładnie jednego dzielnika liczby kn, który nie jest dzielnikiem liczby n.

1.3 Wykaż, że $\varphi(n!) \leqslant n!/H_n$

1.4 Weźmy $a = 2^{n!/3}$

2.1 Popatrz na dzielniki trywialne.

2.2 Prawie każdy wielomian $\Phi_n(a)$ ma dzielnik unikalny dzielnik nietrywialny.

2.3 Popatrz na dzielniki nietrywialne

2.4 Popatrz na dzielniki nietrywialne $a+1, a^n+1$.

2.5 Skorzystaj z 2.4

2.6 Popatrz na dzielniki pierwsze $\Phi_7(x)$. Jakie reszty może dawać $y-1 \pmod 7$.

2.7 Udowodnij, że jeśli wielomian $P(x)$ o współczynnikach całkowitych jest niestały, to zbiór liczb pierwszych dzielących którąkolwiek z liczb $P(1), P(2), \ldots$ jest nieskończony.

2.8 Wystarczy udowodnić, że ta liczba ma 2^{n-1} różnych dzielników pierwszych, a potem skorzystać z 3(b); Udowodnić, że można wybrać $2^n - 1$ dzielników liczby $p_1p_2\ldots p_n$, że żadnych dwóch a, b z tych liczb nie da się przedstawić jako $a/b = 2^\alpha$.

2.9 Pokaż, że liczby $2r$, gdzie r jest liczbą pierwszą, są szukanymi liczbami; Pokaż, że podany ułamek musiałby być postaci $\frac{p^{q^a}-1}{p^{q^{a-1}}-1}$. Potem pokaż, że jedyna możliwość to $2r = 2^{q^\alpha}+1$. Wystarczy rozpatrzeć odpowiednie modulo np. 3 oraz 5.

3.1 Popatrzyć na względnie pierwsze a_1, b_1. Wtedy z tw. Zsigmondy'ego otrzymujemy dowolnie duży dzielnik pierwszy $a_1^n + b_1^n$.

3.2 Udowodnij z tw. Zsigmondy'ego, że jedyne działające $k = 1, 3$. Dla $k = 1$ $a_i = i, r_i = 1$. Natomiast dla $k = 3 a_i = i, r_i = 2$.

3.3 Ustalmy dowolne n. Rozpatrz taką liczbę pierwszą q, że $q > a$ oraz każda z liczb $qm+1$ dla $m = 1, \ldots, n$ nie jest liczbą pierwszą. Weźmy dowolny dzielnik pierwszy $p \mid phi_q(a)$. Można sprawdzić, że $p \nmid q$. Zatem $q = \mathrm{ord}_p(a)$, więc $q \mid p-1$. Niech $p = qN+1$. Wiemy, że $N > n$. Wtedy $\frac{p-1}{\mathrm{ord}_p(a)} = \frac{qN}{q} = N$.

3.4 Wystarczy zauważyć, że dla $n \geqslant 2$ mamy

$$(m+1) \mid (n+1) \Longrightarrow (1 + 10^4 + \cdots + 10^{4m}) \mid (1 + 10^4 + \cdots + 10^{4n]})$$

Wystarczy udowodnić tezę dla $n+1 \in \mathbb{P}$. Wiemy, że $1 + 10^4 + \cdots + 10^{4n} = \Phi_{n+1}(10^4) = \Phi_{n+1}(10)\Phi_{2(n+1)}(10)\Phi_{4(n+1)}(10)$ z Twierdzenia 5.

3.5 Niech $a_0, \ldots, a_{p-1} \in \mathbb{Q}$ będą bokami tego wielokąta. Rozpatrzmy wielomian $P(x) = \sum_{i=0}^{p-1} x^k$. Zauważmy, że $P(\omega) = 0$. Wiemy, że wielomian $\Phi_p(x)$ jest nierozkładalny, więc jest to także wielomian minimalny ω. Skoro $\deg P = \deg \Phi_p$, to są to te same wielomiany, więc $P(x) = c\Phi_p(x)$ dla pewnej stałej c, a wiemy, że $\Phi_p(x) = 1 + x + \cdots + x^{p-1}$.

Bibliografia

[1] Yimin Ge, *Elemntary Properties Of Cyclotomic Polynomials*

[2] Bart Michels, *Zsigmondy's Theorem*
https://pommetatin.be/files/zsigmondy_en.pdf

[3] Jakub Byszewski, *Lemat o podnoszeniu wykładnika otaz twierdzenie Zsigmondy'ego. Jagiellońskie Warsztaty Olimpijskie*
https://satori.tcs.uj.edu.pl/view/Subpage/6401343/content_files/Jakub_Byszewski_JWO.pdf/Jakub_Byszewski_JWO.pdf

[4] Adam Neugebauer, *Alegbra i teoria liczb*

[5] Bartłomiej Bzdęga, *Wielomiany podziału koła - część 1, część 2*
https://www.deltami.edu.pl/2024/01/wielomiany-podzialu-kola-czesc-1/
https://www.deltami.edu.pl/2024/02/wielomiany-podzialu-kola-czesc-2/

[6] Evan Chen, *Summations*
https://web.evanchen.cc/handouts/Summation/Summation.pdf

[7] Julia Jenkins, *Sicherman Dice*
http://buzzard.ups.edu/courses/2010spring/projects/jenkins-sicherman-dice-ups-434-2010.pdf