LEMAT O PODNOSZENIU WYKŁADNIKA ORAZ TWIERDZENIE ZSIGMONDY'EGO

JAGIELLOŃSKIE WARSZTATY OLIMPIJSKIE

JAKUB BYSZEWSKI

1. Lemat o podnoszeniu wykładnika

Stosujemy standardowe oznaczenia: $\mathbf{Z}$ to liczby całkowite, $\mathbf{Q}$ to liczby wymierne, $\mathbf{N}$ to liczby naturalne (z zerem), $\mathbf{N}_+$ to liczby naturalne dodatnie, a $\mathbf{C}$ to liczby zespolone.

Zacznijmy od następującego problemu.

Zadanie 1.1. Niech n będzie liczbą naturalną. Wyznaczyć największą potęgę trójki, która dzieli $2^n + 1$.

Rozwiązanie. Próbę rozwiązania zadania warto rozpocząć od wyznaczenia potęgi trójki w rozkładzie na czynniki pierwsze $2^n + 1$ dla małych wartości n; pozostawiamy to czytelnikom.

Ustalmy najpierw dla jakich n liczba $2^n + 1$ jest podzielna przez 3 i przez 9. W tym celu rozważmy wartości $2^n \bmod 9$:

n	0	1	2	3	4	5
$2^n \bmod 9$	1	2	4	8	7	5

Jeśli n jest parzyste, to $2^n \equiv 1 \bmod 3$ i zatem $2^n + 1$ nie jest podzielne przez 3.

Jeśli n jest nieparzyste oraz niepodzielne przez 3, to $2^n \equiv 2 \bmod 9$ lub $2^n \equiv 5 \bmod 9$, i zatem $2^n + 1$ jest podzielne przez 3, ale nie przez 9.

W ogólnej sytuacji, gdy n jest nieparzyste przy pomocy powyższej tabeli wyznaczamy wartość

$$\frac{2^{3n}+1}{2^n+1} = 2^{2n} - 2^n + 1 \equiv 3 \bmod 9.$$

Oznacza to, że potęga trójki dzieląca $2^{3n}+1$ jest dokładnie o jeden większa niż potęga trójki dzieląca 2^n+1. Pozwala nam to wywnioskować, że gdy n jest nieparzyste, to potęga trójki w rozkładzie $2^n + 1$ na czynniki pierwsze jest dokładnie o jeden większa niż potęga trójki w rozkładzie n na czynniki pierwsze. □

Warto wprowadzić notację na oznaczenie najwyższej potęgi liczby pierwszej p dzielącej daną liczbę. Dowolną niezerową liczbę wymierną x można zapisać w postaci $x = p^s \frac{a}{b}$, gdzie s, a, b są liczbami całkowitymi oraz a i b są niepodzielne przez p. Jeśli dodatkowo założymy, że a i b są względnie pierwsze i $b > 0$, rozkład taki jest jednoznaczny.

Definicja 1.2. Niech p będzie liczbą pierwszą. *Waluacją p-adyczną* liczby wymiernej $x \neq 0$ nazywamy taką liczbę całkowitą $v_p(x) = s$, że $x = p^s \frac{a}{b}$, s, a, b są liczbami całkowitymi oraz a i b są niepodzielne przez p; dla $x = 0$ kładziemy $v_p(0) = \infty$.

Uwaga 1.3. Niech $x, y \in \mathbf{Q}$. Łatwo jest zauważyć następujące własności waluacji p-adycznej (ćwiczenie):

(1) $v_p(x) = \infty$ wtedy i tylko wtedy, gdy $x = 0$.
(2) $v_p(xy) = v_p(x) + v_p(y)$.
(3) $v_p(x + y) \geqslant \min(v_p(x), v_p(y))$.
(4) Jeśli $v_p(x) \neq v_p(y)$, to $v_p(x + y) = \min(v_p(x), v_p(y))$.

Wszystkie te własności należy interpretować w odpowiedni sposób, gdy waluacja przyjmuje wartość ∞. Własność 1.3.(4) jest szczególnie istotna – pozwala nam ona liczyć waluację sumy w przypadku, gdy wszystkie wyrazy (dwa lub więcej) mają parami różną waluację.

Twierdzenie 1.4. Niech p będzie liczbą pierwszą, $n \geqslant 1$ liczbą naturalną, $a, b \in \mathbf{Z}$ liczbami całkowitymi nie podzielnymi przez p i 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 $p = 2$ i dodatkowo bądź $4 \mid a - b$, bądź $2 \nmid n$, to
$$v_2(a^n - b^n) = v_2(a - b) + v_2(n).$$

Uwaga 1.5. Twierdzenie nie jest prawdziwe dla $p = 2$ bez dodatkowego założenia. Dla przykładu przyjmijmy $n = 2, a = 3, b = 1$. Wówczas $v_2(a - b) = 1$ oraz $v_2(a^2 - b^2) = 3$.

Dowód Twierdzenia 1.4: Zauważmy najpierw, że jeśli twierdzenie jest prawdziwe dla $n = n_1$ oraz $n = n_2$, to jest prawdziwe także dla $n = n_1 n_2$; faktycznie, stosując twierdzenie dla odpowiednich wartości (i sprawdzając, że założenia są spełnione), otrzymujemy

$$v_p(a^{n_1 n_2} - b^{n_1 n_2}) = v_p((a^{n_1})^{n_2} - (b^{n_1})^{n_2}) = v_p(a^{n_1} - b^{n_1}) + v_p(n_2) = v_p(a-b) + v_p(n_1) + v_p(n_2) = v_p(a-b) + v_p(n_1 n_2).$$

Pozwala nam to zredukować dowód twierdzenia do przypadku, gdy n jest liczbą pierwszą. W dalszym ciągu będziemy zakładali, że tak jest.

Na mocy założenia możemy napisać $a = b + p^s m$ dla $s = v_p(a - b) \geqslant 1$ i $m \in \mathbf{Z}$ nie podzielnego przez p. (Jeśli $p = 2$ i $2 \mid n$, to mamy także $s \geqslant 2$.) Podnosząc tę równość do n-tej potęgi i korzystając ze wzoru dwumianowego otrzymujemy

$$a^n = (b + p^s m)^n = \sum_{i=0}^{n} \binom{n}{i} b^{n-i} p^{si} m^i.$$

Mówiąc nieprecyzyjnie, możemy policzyć waluację $a^n - b^n$, ponieważ wyrazy występujące w powyższej sumie mają zazwyczaj różną waluację. Mówiąc dokładniej, wyrazy odpowiadające $i \geqslant 2$ są podzielne przez p^{2s}, co pozwala nam napisać

$$a^n = b^n + nb^{n-1} p^s m + p^{2s} m' \qquad \text{dla pewnego } m' \in \mathbf{Z}$$

i zatem $a^n - b^n = p^s(nb^{n-1} m + p^s m')$. Jeśli n jest liczbą pierwszą różną od p, to nb^{n-1} nie jest podzielne przez p i zatem $v_p(a^n - b^n) = s = v_p(a - b)$, $v_p(n) = 0$, i szukana równość zachodzi. Jeśli $n = p$ oraz $s \geqslant 2$, rozumujemy podobnie: wyraz nb^{n-1} jest podzielny przez p, ale nie przez p^2, i zatem to samo ma miejsce dla $nb^{n-1} + p^s m'$. Co za tym idzie $v_p(a^n - b^n) = s + 1 = v_p(a - b) + v_p(n)$. W przypadku, gdy $n = p$ i $s = 1$ (i zatem z naszego założenia $p > 2$) musimy rozumować uważniej: w równości (1) wyodrębnijmy *trzy* pierwsze wyrazy. Otrzymujemy

$$a^p - b^p = p^2 b^{n-1} m + \frac{p(p-1)}{2} b^{n-2} p^2 m^2 + p^3 m'' \qquad \text{dla pewnego } m'' \in \mathbf{Z}\,.$$

Dwa ostatnie wyrazy są podzielne przez p^3 (korzystamy tutaj z tego, że $p \neq 2$), więc $v_p(a^p - b^p) = 2 = v_p(a - b) + v_p(n)$.

□

Uwaga 1.6. Można zadać pytanie dla jakich liczb n liczba $a^n - b^n$ jest podzielna przez p. Na mocy małego twierdzenie Fermata jest tak dla $n = p - 1$ (przypomnijmy, że $p \nmid a, b$). Można łatwo pokazać, że zbiór wszystkich takich n jest zbiorem wielokrotności pewnej liczby całkowitej m dzielącej $p - 1$. Wynik, który implikuje ten jako swój szczególny przypadek, udowodnimy w poniższym stwierdzeniu.

Stwierdzenie 1.7. Niech $a > b \geqslant 1$ będą liczbami całkowitymi i niech $n \geqslant m \geqslant 1$ będą liczbami naturalnymi. Zachodzi wówczas równość

$$\operatorname{nwd}(a^n - b^n, a^m - b^m) = a^{\operatorname{nwd}(n,m)} - b^{\operatorname{nwd}(n,m)}.$$

Dowód. Dla uproszczenia notacji połóżmy $x_n = a^n - b^n$. Jest jasne, że jeśli $n \mid m$, to $x_n \mid x_m$, i zatem $\operatorname{nwd}(x_n, x_m)$ jest podzielny przez $x_{\operatorname{nwd}(n,m)}$. Dla dowodu implikacji przeciwnej, pokażemy, że dowolny wspólny dzielnik x_n i x_m dzieli także x_{n-m}. Wynika to z równości

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

oraz faktu, że dowolny dzielnik x_n jest względnie pierwszy z a.

Aby wywnioskować stąd tezę, wystarczy zastosować algorytm Euklidesa; faktycznie, zastępując sukcesywnie parę $\{n, m\}$ przez $\{n - m, m\}$ otrzymamy ostatecznie parę $\{\operatorname{nwd}(n, m), 0\}$, i co za tym idzie pokażemy, że każdy wspólny dzielnik x_n i x_m dzieli $x_{\operatorname{nwd}(n,m)}$. □

2. Twierdzenie Zsigmondy'ego

Twierdzenie 2.1 (Twierdzenie Zsigmondy'ego)**.** Niech $a > b \geqslant 1$ będą względnie pierwszymi liczbami całkowitymi. Rozpatrzmy ciąg liczb całkowitych $(x_n)_{n \geqslant 1}$ zdefiniowany wzorem $x_n = a^n - b^n$. Wówczas dla każdego $n \geqslant 2$ istnieje dzielnik pierwszy p wyrazu x_n, który nie dzieli x_k dla żadnego $1 \leqslant k < n$ chyba, że zachodzi jeden z następujących dwóch warunków:

(1) $n = 2$, a i b są nieparzyste, a $a + b$ jest potęgą dwójki;
(2) $n = 6$, $a = 2$, $b = 1$.

Łatwo widać, że wymienione w wypowiedzi twierdzenia wyjątki są nimi faktycznie. Dla $a = 2$, $b = 1$ pierwsze wyrazy ciągu (x_n) to $1, 3, 7, 15, 31, 63$; dzielniki pierwsze $63 = 3^2 \cdot 7$ to $3 = x_2$ i $7 = x_3$. Każdy dzielnik pierwszy p wyrazu x_n, który nie dzieli x_k dla $1 \leqslant k < n$ nazywamy *pierwotnym* dzielnikiem pierwszym.

Dowód twierdzenia Zsigmondy'ego może się na pierwszy rzut oka wydać nieumotywowany. Aby temu zapobiec, wykażemy najpierw twierdzenie dla szczególnych wartości n, tj. gdy

(1) $n = 2$;
(2) n jest liczbą pierwszą nieparzystą;
(3) n jest potęgą liczby pierwszej;
(4) n jest iloczynem dwóch różnych liczb pierwszych (nieparzystych).

Dowód twierdzenia Zsigmondy'ego dla $n = 2$. Naszym celem jest znalezienie liczby pierwszej p dzielącej $a^2 - b^2$, ale nie $a - b$. Dowolny dzielnik pierwszy wspólny dla $a - b$ i $a + b$ dzieli także $2a$ i $2b$, a zatem jest równy 2, ponieważ a i b są względnie pierwsze. Jeśli zatem $a + b$ nie jest potęgą dwójki, to posiada dzielnik pierwszy nieparzysty p, i dzielnik ten ma żądane własności. Z drugiej strony, jeśli $a + b$ jest potęgą dwójki, dzielnik taki nie istnieje. □

Dowód twierdzenia Zsigmondy'ego dla $n = \ell$ będącego liczbą pierwszą nieparzystą. Przypuśćmy, że liczba pierwsza p dzieli $a^\ell - b^\ell$ oraz $a^k - b^k$ dla pewnego $1 \leqslant k < \ell$. Ze stwierdzenia 1.7 wynika, że p dzieli także $a - b$.

Oznacza to, że dowolny wspólny dzielnik pierwszy x_ℓ i x_k dla $1 \leqslant k < \ell$ dzieli również x_1. Musimy zatem znaleźć liczbę pierwszą p dzielącą $a^\ell - b^\ell$, ale nie $a - b$. Dowód istnienia takiego p będzie niekonstruktywny; przypuśćmy, że takie p nie istnieje. Jeśli q jest dowolnym dzielnikiem $a - b$, to na mocy lematu o podnoszeniu wykładnika mamy $v_q(a^\ell - b^\ell) = v_q(a - b) + v_q(\ell)$ (korzystamy tu z względnej pierwszości a i b) i zatem

$$v_q(a^\ell - b^\ell) = \begin{cases} v_q(a-b) + 1, & \text{jeśli } q = \ell, \\ v_q(a-b), & \text{jeśli } q \neq \ell. \end{cases}$$

Ponieważ przypuściliśmy, że dowolny dzielnik pierwszy $a^\ell - b^\ell$ jest również dzielnikiem pierwszym $a - b$, otrzymujemy stąd, że

$$a^\ell - b^\ell = \begin{cases} \ell(a-b), & \text{jeśli } \ell \mid a - b, \\ (a-b), & \text{jeśli } \ell \nmid a - b. \end{cases}$$

Dzieląc przez $a - b$ otrzymujemy

$$a^{\ell-1} + a^{\ell-2}b + \cdots + b^{\ell-1} = \ell,$$

co nie jest możliwe, albowiem po lewej stronie mamy sumę ℓ liczb całkowitych dodatnich, z których wszystkie poza ostatnią są > 1. Sprzeczność.

□

Dla uproszczenia kolejnych dowodów sformułujemy łatwy fakt o dzielnikach pierwotnych będący natychmiastowym wnioskiem ze stwierdzenia 1.7.

Wniosek 2.2. Niech $n \geqslant 2$ będzie liczbą całkowitą. Na to, by wyraz x_n posiadał czynnik pierwotny ℓ potrzeba i wystarcza, by ℓ nie dzieliło żadnego z wyrazów $x_{n/p}$ dla wszystkich liczb pierwszych p dzielących n.

Dowód twierdzenia Zsigmondy'ego dla n będącego potęgą liczby pierwszej. Ten wynik można otrzymać albo powtarzając rozumowanie z przypadku, gdy n jest liczbą pierwszą, albo też stosując bezpośrednio ten wynik do odpowiednio wybranych wartości a i b. Zapewne konieczne będzie rozważenie osobno przypadku, gdy n jest potęgą liczby pierwszej nieparzystej oraz gdy jest potęgą dwójki. Pozostawiamy go czytelnikom jako ćwiczenie. □

Dowód twierdzenia Zsigmondy'ego dla $n = \ell_1 \cdot \ell_2$, gdzie $\ell_1 \neq \ell_2$ są nieparzystymi liczbami pierwszymi. Na mocy wniosku 2.2 dowolny czynnik pierwszy q wyrazu x_n, który dzieli również x_k dla pewnego $1 \leqslant k < n$ musi dzielić również x_{ℓ_1} lub x_{ℓ_2}. Przypuśćmy dla ustalenia uwagi, że $q \mid x_{\ell_1}$. Stosując podobnie jak poprzednio lemat o podnoszeniu wykładnika, otrzymujemy

$$v_q(a^n - b^n) = \begin{cases} v_q(a^{\ell_1} - b^{\ell_1}) + 1, & q = \ell_2, \\ v_q(a^{\ell_1} - b^{\ell_1}), & q \neq \ell_2. \end{cases}$$

Jeśli $q \mid x_{\ell_2}$ otrzymujemy podobną zależność

$$v_q(a^n - b^n) = \begin{cases} v_q(a^{\ell_1} - b^{\ell_1}) + 1, & q = \ell_2, \\ v_q(a^{\ell_1} - b^{\ell_1}), & q \neq \ell_2. \end{cases}$$

Przypuśćmy dla dowodu nie wprost, że x_n nie ma żadnych pierwotnych dzielników pierwszych, tj. że każdy czynnik pierwszy x_n dzieli również x_{ℓ_1} lub x_{ℓ_2}. Na mocy powyższej analizy otrzymujemy wówczas nierówność

$$x_n \leqslant x_{\ell_1} x_{\ell_2} \ell_1 \ell_2.$$

(Dokładniejsza analiza pokazałaby, że x_n jest równe jednej z liczb

$$\frac{x_{\ell_1}x_{\ell_2}}{x_1}, \frac{x_{\ell_1}x_{\ell_2}}{x_1}\ell_1, \frac{x_{\ell_1}x_{\ell_2}}{x_1}\ell_2, \frac{x_{\ell_1}x_{\ell_2}}{x_1}\ell_1\ell_2,$$

ale nie będzie nam to potrzebne.)

Aby dokończyć dowód, konieczne będzie napisanie pewnych nierówności. Jeden z możliwych sposobów, by kontynuować jest następujący. Bez straty ogólności możemy przyjąć, że $\ell_1 < \ell_2$. Mamy wówczas

$$a^{(\ell_1-1)\ell_2} \leqslant a^{(\ell_1-1)\ell_2} + a^{(\ell_1-2)\ell_2}b^{\ell_2} + \cdots + b^{(\ell_1-1)\ell_2} = \frac{x_n}{x_{\ell_2}} \leqslant x_{\ell_1}\ell_1\ell_2 \leqslant a^{\ell_1}\ell_1\ell_2$$

i zatem

$$a^{(\ell_1\ell_2-1)/2} \leqslant a^{\ell_1\ell_2-\ell_1-\ell_2} \leqslant \ell_1\ell_2.$$

Ponieważ $a \geqslant 2$ oraz $2^n \geqslant 4n$ dla $n \geqslant 4$ (łatwo to pokazać np. przez indukcję), otrzymujemy stąd, że

$$4\frac{\ell_1\ell_2 - 1}{2} \leqslant \ell_1\ell_2$$

i zatem $\ell_1\ell_2 \leqslant 2$. Sprzeczność. □

Powyższe rozumowania można by kontynuować (warto np. by czytelnik/czytelniczka rozważyli przypadek $n = 6$), ale staje się to coraz bardziej pracochłonne wraz z arytmetyczną złożonością (w szczególności, liczbą czynników pierwszych) liczby n. W ogólnym przypadku konieczne jest wprowadzenie nowego narzędzia. Są to wielomiany cyklotomiczne, które zdefiniujemy w kolejnym rozdziale.

3. Wielomiany cyklotomiczne

W niniejszym rozdziale będziemy używali liczb zespolonych (tak naprawdę istotne dla nas będzie pojęcie pierwiastków z jedności). W wielu przypadkach można sobie poradzić bez użycia liczb zespolonych definiując wielomiany cyklotomiczne przy pomocy wzoru inwersyjnego Möbiusa. Nie wiem jednak, w jaki sposób bez pomocy liczb zespolonych wykazać nierówności z lematu 5, które odgrywają kluczową rolę w dowodzie.

Dla liczby naturalnej $n \geqslant 1$ oznaczamy przez ζ_n liczbę zespoloną

$$\zeta_n = \cos(2\pi/n) + i\sin(2\pi/n).$$

Jest to pierwiastek pierwotny n-tego stopnia z jedności, tzn. $\zeta_n^n = 1$, podczas gdy $\zeta_n^k \neq 1$ dla $1 \leqslant k \leqslant n-1$. Faktycznie, wzór de Moivre'a pokazuje, że

$$\zeta_n^k = \cos(2\pi k/n) + i\sin(2\pi k/n), \qquad k \in \mathbf{Z}\,.$$

Wielomian $X^n - 1$ ma w liczbach zespolonych dokładnie n pierwiastków, mianowicie liczby ζ_n^k dla $0 \leqslant k \leqslant n-1$. Można to zapisać wzorem

$$X^n - 1 = \prod_{k=0}^{n-1}(X - \zeta_n^k).$$

Rozpatrzmy teraz wielomian Φ_n zmiennej X zdefiniowany wzorem

$$\Phi_n = \prod_{\substack{0\leqslant k\leqslant n-1\\ \mathrm{nwd}(k,n)=1}} (X - \zeta_n^k),$$

którego pierwiastami są dokładnie liczby zespolone postaci ζ_n^k, tzn. wszystkie pierwiastki **pierwotne** z jedności stopnia n. (Zauważmy, że jeśli k jest względnie pierwsze z n, to ζ_n^k jest pierwiastkiem pierwotnym z jedności; w sytuacji ogólnej, przyjmując $d := \mathrm{nwd}(k,n)$, otrzymujemy, że liczba ζ_n^k jest pierwiastkiem pierwotnym z jedności stopnia n/d.) Bezpośrednio z definicji wynika, że stopień wielomianu Φ_n to $\varphi(n)$, gdzie φ to funkcja Eulera, tzn. $\varphi(n)$ oznacza liczbę liczb $1 \leqslant k \leqslant n$ względnie pierwszych z n.

Wielomiany $X^n - 1$ i Φ_n są ze sobą związane. Pogrupujmy pierwiastki ζ_n^k, $0 \leqslant k \leqslant n-1$, wielomianu $X^n - 1$ w zależności od stopnia tych pierwiastków lub – równoważnie – największego wspólnego dzielnika $\mathrm{nwd}(k,n)$ liczb k i n. Każdy z pierwiastków ζ_n^k, $0 \leqslant k \leqslant n-1$, wielomianu $X^n - 1$ jest pierwiastkiem pewnego wielomianu Φ_d dla $d = n/\mathrm{nwd}(k,n)$ i wszystkie te pierwiastki występują. Otrzymujemy stąd równość

$$X^n - 1 = \prod_{d|n} \Phi_{n/d} = \prod_{d|n} \Phi_d. \tag{1}$$

Powyższa zależność jest analogiczna (a właściwie jest szczególnym przypadkiem) tej, która pojawia się we wzorze inwersyjnym Möbiusa, który zostanie omówiony w następnym rozdziale.

Policzmy kilka pierwszych wielomianów cyklotomicznych. Dla $n = 1$ otrzymujemy $\Phi_1 = X - 1$. Dla $n = 2$ otrzymujemy $\Phi_2 = X + 1$. W ogólności, gdy $n = p$ jest liczbą pierwszą, wzór (1) daje $X^p - 1 = \Phi_1\Phi_p$, i co za tym idzie

$$\Phi_p = \frac{X^p - 1}{\Phi_1} = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \cdots + X + 1.$$

Podobne rozumowanie dla $n = 4, 6, 8, 9, 10$ daje

$$\begin{aligned}
\Phi_4 &= \frac{X^4 - 1}{\Phi_2\Phi_1} = \frac{X^4 - 1}{(X+1)(X-1)} = X^2 + 1,\\
\Phi_6 &= \frac{X^6 - 1}{\Phi_3\Phi_2\Phi_1} = \frac{X^6 - 1}{(X^2+X+1)(X+1)(X-1)} = X^2 - X + 1,\\
\Phi_8 &= \frac{X^8 - 1}{\Phi_4\Phi_2\Phi_1} = \frac{X^8 - 1}{(X^2+1)(X+1)(X-1)} = X^4 + 1,\\
\Phi_9 &= \frac{X^9 - 1}{\Phi_3\Phi_1} = \frac{X^9 - 1}{(X^2+X+1)(X-1)} = X^6 + X^3 + 1,\\
\Phi_{10} &= \frac{X^{10} - 1}{\Phi_5\Phi_2\Phi_1} = \frac{X^{10} - 1}{(X^5+X^4+X^3+X^2+1)(X+1)(X-1)} = X^4 - X^3 + X^2 - X + 1.
\end{aligned}$$

Stąd można uzyskać wzór ogólny (więcej o tym w kolejnym rozdziale). Bezpośrednio przez indukcję wnioskujemy także następujący fakt (korzystamy tu z tego, że iloraz wielomianu o współczynnikach całkowitych przez wielomian o współczynnikach całkowitych i **współczynniku wiodącym jeden** ma współczynniki całkowite).

Stwierdzenie 3.1. Dla każdego $n \geqslant 1$ wielomian Φ_n ma współczynniki całkowite.

Można pokazać, ale jest to trudniejsze, że wielomian Φ_n jest nierozkładalny (nad $\mathbf{Z}$). Dla $n = p$ jest to znany fakt, dowodzony zazwyczaj przy pomocy lematu Eisensteina. Podobne rozumowanie działa, gdy n jest potęgą liczby pierwszej. W ogólnej sytuacji trzeba się nieco bardziej napracować; nie będzie nam to potrzebne.

Obserwacja wielomianów Φ_n dla małych wartości n pozwala przypuszczać, że mają one zawsze współczynniki ze zbioru $\{-1, 0, 1\}$. Tak jednak nie jest, a najmniejsza wartość n dla której nie jest to prawdą to $n = 105$.

Dla naszych potrzeb konieczne będą wzory pozwalające na rekurencyjne wyznaczanie wielomianów cyklotomicznych. Pokażemy dowód tego faktu wykorzystujący definicję wielomianów cyklotomicznych przy pomocy ich pierwiastków zespolonych. W kolejnym rozdziale omówimy inny dowód wykorzystujący wzór inwersyjny Möbiusa.

Stwierdzenie 3.2. Niech n będzie liczbą naturalną, a p jej dzielnikiem pierwszym.

(1) Jeśli $p^2 \mid n$, to
$$\Phi_n(X) = \Phi_{n/p}(X^p).$$

(2) Jeśli $p^2 \nmid n$, to
$$\Phi_n(X) = \frac{\Phi_{n/p}(X^p)}{\Phi_{n/p}(X)}.$$

Dowód. Przypuśćmy najpierw, że $p^2 \mid n$. Jeśli ζ_n^k, $\mathrm{nwd}(k, n) = 1$, jest jednym z pierwiastków wielomianu Φ_n, to $\zeta_n^{pk} = \zeta_{n/p}^k$ jest pierwiastkiem wielomianu $\Phi_{n/p}$, i wszystkie jego pierwiastki otrzymujemy w ten sposób. Co więcej, przyporządkowanie $\zeta_n^k \mapsto \zeta_{n/p}^k$ skleja ze sobą dokładnie p pierwiastków, a mianowicie $\zeta_n^{k+in/p}$ dla $0 \leqslant i \leqslant p-1$. Dla ustalonego k produkt $\prod_{i=0}^{p-1}(X - \zeta_n^{k+in/p})$ przyjmuje postać

$$\prod_{i=0}^{p-1}(X - \zeta_n^{k+in/p}) = \zeta_n^{kp}\prod_{i=0}^{p-1}(\zeta_n^{-k}X - \zeta_n^{in/p}) = \zeta_n^{kp}\prod_{i=0}^{p-1}(\zeta_n^{-k}X - \zeta_p^i) = X^p - \zeta_n^{kp} = X^p - \zeta_{n/p}^k.$$

Pozwala nam to napisać równość

$$\begin{aligned}
\Phi_n(X) &= \prod_{\substack{0\leqslant k\leqslant n-1\\ \mathrm{nwd}(k,n)=1}}(X - \zeta_n^k) = \prod_{\substack{0\leqslant k\leqslant n/p-1\\ \mathrm{nwd}(k,n/p)=1}}\prod_{i=0}^{p-1}(X - \zeta_n^{k+in/p})\\
&= \prod_{\substack{0\leqslant k\leqslant n/p-1\\ \mathrm{nwd}(k,n/p)=1}}(X^p - \zeta_{n/p}^k) = \Phi_{n/p}(X^p).
\end{aligned}$$

Rozumowanie w przypadku, gdy $p^2 \nmid n$ jest podobne, tyle że wówczas spośród liczb $\zeta_n^{k+in/p}$, $\mathrm{nwd}(k, n/p) = 1$, $0 \leqslant k \leqslant n/p - 1$, $0 \leqslant i \leqslant p - 1$, tylko $p - 1$ jest pierwiastkami wielomianu Φ_n, a pozostała jest pierwiastkiem wielomianu $\Phi_{n/p}$ (pierwiastek ten odpowiada wartości i dla której $k+in/p \equiv 0 \bmod p$). Z tego powodu wielomian

$\Phi_{n/p}(X^p)$, którego pierwiastkami są wszystkie liczby $\zeta_n^{k+in/p}$, $0 \leqslant k \leqslant n/p-1$, $\mathrm{nwd}(k, n/p) = 1$, $0 \leqslant i \leqslant p-1$, jest produktem wielomianów $\Phi_n(X)$ oraz $\Phi_{n/p}(X)$. □

Czytelnikom, których wielomiany cyklotomiczne zainteresowały poleca się następujące zadania.

Zadania 3.3.

(1) Pokazać, że jeśli $n = p^s$ jest potęgą liczby pierwszej p, to $\Phi_n = X^{p^{s-1}} + X^{p^{s-2}} + \cdots + X^p + 1$.
(2) Pokazać, że jeśli $n \equiv 2 \bmod 4$, to $\Phi_n(X) = \Phi_{n/2}(-X)$.
(3) (Trudniejsze) Pokazać, że jeśli n ma tylko 2 czynniki pierwsze, to Φ_n ma współczynniki w zbiorze $\{-1, 0, 1\}$.
(4) Obliczyć Φ_{105} (najlepiej przy pomocy jednego z programów do algebry komputerowej, np. `SageMath`) i zauważyć, że ma on współczynnik różny od $-1, 0, 1$.
(5) Pokazać, że Φ_n ma współczynniki w zbiorze $\{-1, 0, 1\}$ dla $n < 105$.

Dla nas najistotniejsze będzie to, że wielomiany cyklotomiczne można wykorzystać do uzyskania faktoryzacji liczb postaci $a^n - 1$ oraz $a^n - b^n$ na czynniki.

Stwierdzenie 3.4. Niech $a, b \in \mathbf{Z}$ będą liczbami całkowitymi, $b \neq 0$. Wówczas

(1) $a^n - 1 = \prod_{d|n} \Phi_d(a)$;
(2) $a^n - b^n = \prod_{d|n} b^{\varphi(d)} \Phi_d(a/b)$.

Występujące w powyższych faktoryzacjach liczby $\Phi_d(a)$ oraz $b^{\varphi(d)}\Phi_d(a/b)$ są liczbami całkowitymi.

Dowód. Żądane faktoryzacje uzyskujemy natychmiast podstawiając $X = a$ oraz $X = a/b$ w równaniu (1). Fakt, że wartości $b^{\varphi(d)}\Phi_d(a/b)$ są liczbami całkowitymi wynika z tego, że Φ_d jest wielomianem stopnia $\varphi(d)$ o współczynnikach całkowitych (p. stwierdzenie 3.1). □

Notacja 3.5. Piszemy $\Phi_n(x, y) = y^{\varphi(n)}\Phi_n(x/y)$. Możemy traktować Φ_n jako wielomian jednorodny stopnia $\varphi(n)$ zmiennych x i y.

W dalszym ciągu musimy oszacować wartości wielomianów cyklotomicznych w liczbach rzeczywistych. Jest to jedyne miejsce w tej pracy, które faktycznie wydaje się wymagać w istotny sposób wykorzystania liczb zespolonych.

Lemat 3.6. Niech $n \geqslant 1$ będzie liczbą całkowitą, a $x \geqslant y \geqslant 1$ liczbami rzeczywistymi. Wówczas zachodzą nierówności

$$(x-1)^{\varphi(n)} \leqslant \Phi_n(x) \leqslant (x+1)^{\varphi(n)}, \qquad (x-y)^{\varphi(n)} \leqslant \Phi_n(x, y) \leqslant (x+y)^{\varphi(n)}.$$

Nierówności te są ostre dla $n \geqslant 3$.

Dowód. W przypadku $n = 1, 2$ mamy $\Phi_n(x) = x \mp 1$ oraz $\Phi_n(x, y) = x \mp y$ i zatem teza jest spełniona. Dla $n \geqslant 3$ piszemy $\Phi_n(x)$ jako produkt $\varphi(n)$ wyrazów $\Phi_n(x) = \prod_{\mathrm{nwd}(k,n)=1}(x - \zeta_n^k)$ i grupujemy w tym produkcie czynniki $(x - \zeta_n^k)$ oraz $(x - \zeta_n^{n-k})$. Produkt tych dwóch czynników wynosi

$$(x - \zeta_n^k)(x - \zeta_n^{n-k}) = x^2 - 2\cos(\frac{2\pi k}{n})x + 1$$

i leży ściśle pomiędzy $(x-1)^2$ oraz $(x+1)^2$ (korzystamy tu z tego, że $n > 2$). Par takich jest $\varphi(n)/2$, i stąd wynika teza dla $\Phi_n(x)$. Nierówności dla $\Phi_n(x, y)$ wynikają bezpośrednio z tych dla $\Phi_n(x)$. □

4. Wzór inwersyjny Möbiusa

Przy rozpatrywaniu pewnych problemów z teorii liczb zdarza się, że dwie funkcje f i g, określone na zbiorze liczb naturalnych dodatnich i o wartościach – powiedzmy – zespolonych, związane są wzorem

$$g(n) = \sum_{d|n} f(d), \tag{2}$$

gdzie suma przebiega po wszystkich dzielnikach naturalnych d liczby n. Wzór ten wyraża wartości funkcji g w terminach wartości funkcji f, ale jest jasne, że także na odwrót wartości funkcji g wyznaczają jednoznacznie wartości funkcji f; faktycznie, $f(n) = g(n) - \sum_{d|n, d<n} g(d)$, co rekurencyjnie prowadzi do wyznaczenia wartości $f(n)$ w terminach $g(k)$ dla $1 \leqslant k \leqslant n$. Naszym celem będzie wyprowadzenie bezpośredniego wzoru na funkcję f w terminach funkcji g. W tym celu definiujemy funkcję Möbiusa.

Definicja 4.1. Funkcja Möbiusa $\mu\colon \mathbf{N}_+ \to \{-1, 0, 1\}$ zdefiniowana jest wzorem

$$\mu(n) = \begin{cases} (-1)^s, & \text{gdy } n \text{ jest iloczynem } s \textbf{ różnych} \text{ liczb pierwszych;} \\ 0, & \text{gdy } n \text{ jest podzielne przez kwadrat pewnej liczby pierwszej.} \end{cases}$$

W powyższej definicji przyjmujemy, że 1 jest iloczynem zerowej liczby (parami różnych) liczb pierwszych (produkt pusty), i zatem $\mu(1) = 1$. Tak zdefiniowana funkcja Möbiusa ma szczególną własność, a mianowicie wpisuje się w kontekst opisany w równaniu (2) dla $f = \mu$ oraz funkcji g zdefiniowanej wzorem

$$g(n) = \begin{cases} 1, & \text{gdy } n = 1; \\ 0, & \text{gdy } n > 1. \end{cases}$$

Stwierdzenie 4.2.

$$\sum_{d|n} \mu(n) = \begin{cases} 1, & \text{gdy } n = 1; \\ 0, & \text{gdy } n > 1. \end{cases}$$

Dowód. Rozłóżmy n na czynniki pierwsze

$$n = p_1^{k_1} \cdots p_s^{k_s},$$

gdzie p_i są parami różnymi liczbami pierwszymi, a k_i liczbami naturalnymi dodatnimi. Wartości $\mu(d)$ dla $d \mid n$ są niezerowe jedynie dla wartości d postaci $d = \prod_{i \in I} p_i$ dla pewnego zbioru $I \subset \{1, \ldots, s\}$; ponadto, jeśli I zawiera k elementów, to $\mu(d) = (-1)^k$. Liczba k-elementowych podzbiorów zbioru $\{1, \ldots, s\}$ to $\binom{s}{k}$, i zatem na mocy wzoru dwumianowego mamy

$$\sum_{d|n} \mu(n) = \sum_{k=0}^{s} \binom{s}{k} (-1)^k = (1-1)^s = \begin{cases} 1, & \text{gdy } s = 0; \\ 0, & \text{gdy } s \geqslant 1. \end{cases}$$

(Ściśle rzecz biorąc, wyprowadzenie to wymaga być może dodatkowego komentarza, gdy $s = 0$, jeśli czytelnik/czytelniczka obawia się symbolu 0^0; przy odpowiedniej interpretacji jest jednak poprawne, a w każdym razie przypadek $s = 0$ jest trywialny.) To kończy dowód. □

Możemy teraz sformułować wzór inwersyjny Möbiusa, który precyzuje postać „odwrotnej" zależności funkcji g od funkcji f, o której istnieniu już się przekonaliśmy.

Twierdzenie 4.3 (Wzór inwersyjny Möbiusa)**.** Funkcje $f, g\colon \mathbf{N}_+ \to \mathbf{C}$ spełniają zależność

$$g(n) = \sum_{d|n} f(d), \qquad n \geqslant 1$$

wtedy i tylko wtedy, gdy

$$f(n) = \sum_{d|n} \mu(n/d) g(d), \qquad n \geqslant 1.$$

Dowód. Przypuśćmy najpierw, że $g(n) = \sum_{d|n} f(d)$ dla $n \geqslant 1$ i policzmy:

$$\sum_{d|n} \mu(n/d) g(d) = \sum_{e|d} \sum_{d|n} \mu(n/d) f(e) = \sum_{e|n} \sum_{k|(n/e)} \mu(n/ke) f(e) = f(n),$$

gdzie ostatnia równość wynika z tożsamości $\sum_{k|(n/e)} \mu(n/ke) = 0$ dla $e < n$ (stwierdzenie 4.2). To kończy dowód jednej z implikacji. Dowód drugiej może zostać przeprowadzony analogicznie; można też skorzystać z uprzedniej obserwacji mówiącej, że wartości $(f(n))_{n \geqslant 1}$ i $(g(n))_{n \geqslant 1}$ są wyznaczone jednoznacznie przez siebie nawzajem. □

Uwaga 4.4. W dowodzie nie jest ważne, że funkcje przyjmują wartości w liczbach zespolonych. Wypowiedź i dowód twierdzenia można wypowiedzieć bez znaczących zmian dla funkcji przyjmujących wartości w dowolnej grupie abelowej. Dla wielomianów cyklotomicznych ważne będzie zastosowanie tego wzoru dla funkcji przyjmujących wartości w grupie multyplikatywnej funkcji wymiernych. Wypowiemy poniżej odpowiednie stwierdzenie w tym przypadku, pozostawiając konieczne niewielkie modyfikacje dowodu czytelnikom. (Aby udowodnić poniższe twierdzenie nie trzeba wiedzieć, czym jest grupa abelowa.)

Twierdzenie 4.5 (Wzór inwersyjny Möbiusa)**.** Funkcje f, g określone są na zbiorze $\mathbf{N}_+$ i przyjmują wartości w zbiorze $\mathbf{C}(X)^*$ funkcji wymiernych różnych od zera. Wówczas zależność

$$g(n) = \prod_{d|n} f(d), \qquad n \geqslant 1$$

zachodzi wtedy i tylko wtedy, gdy

$$f(n) = \prod_{d|n} g(d)^{\mu(n/d)}, \qquad n \geqslant 1.$$

Wniosek 4.6. Zachodzi równość $\Phi_n = \prod_{d|n} (X^d - 1)^{\mu(n/d)}$.

Dowód. Równość ta wynika ze wzoru inwersyjnego Möbiusa oraz z równości (1). □

Korzystając z wniosku 4.6 oraz najprostszych własności funkcji Möbiusa można uzyskać dużo prostszy dowód stwierdzenia 3.2. Szczegóły pozostawiamy czytelnikom.

5. Dowód twierdzenia Zsigmondy'ego

Lemat 5.1. Niech $a > b \geqslant 1$ będą względnie pierwszymi liczbami całkowitymi. Rozpatrzymy ciag (x_n) zadany wzorem $x_n = a^n - b^n$. Jeśli dla danego $n \geqslant 2$ wyraz x_n nie posiada pierwotnych czynników pierwszych, to bądź $n = 2$, bądź wyraz $\Phi_n(a, b)$ jest liczbą pierwszą dzielącą n.

Dowód. Załóżmy, że $n \geqslant 3$ oraz że wyraz x_n nie posiada pierwotnych czynników pierwszych. Pokażemy, że $\Phi(a, b)$ jest liczbą pierwszą dzielącą n.

Krok I: $\Phi_n(a, b)$ jest iloczynem różnych liczb pierwszych, z których każda dzieli n.

Jeśli ℓ jest liczbą pierwszą dzielącą $\Phi_n(a, b)$, to ℓ dzieli x_n i na mocy wniosku 2.2 ℓ dzieli $x_{n/p}$ dla pewnego $p \mid n$. Na mocy stwierdzenia 3.4 liczba $\Phi_n(a, b)$ dzieli $x_n/x_{n/q}$ dla dowolnego dzielnika pierwszego q liczby n i zatem $v_\ell(x_n) > v_\ell(x_{n/q})$. Stosując to do $q = p$ i korzystając z twierdzenia 1.4 wnioskujemy, że $\ell = p$ oraz że (przynajmniej dla $\ell \neq 2$) $v_\ell(x_n) = v_\ell(x_{n/\ell}) + 1$. Oznacza to, że ℓ dzieli n oraz że $v_\ell(\Phi_n(a, b)) = 1$ dla $\ell \neq 2$.

Musimy jeszcze uporać się z trudnościami występującymi w przypadku, gdy $\ell = 2$. Jeśli 2 dzieli $\Phi_n(a, b)$, to 2 dzieli x_n i, jako że a i b są względnie pierwsze, muszą być obie nieparzyste. Wówczas jednak każda z liczb x_m, $m \geqslant 1$, jest parzysta. Jeśli tylko n nie jest potęgą dwójki, to posiada czynnik pierwszy $q \neq 2$ oraz (ponownie na mocy twierdzenia 1.4) $v_\ell(x_n) = v_\ell(x_{n/q})$, co stoi w sprzeczności z parzystością $\Phi_n(a, b)$. Jeśli jednak n jest potęgą dwójki, to $n \geqslant 4$ i $4 \mid a^2 - b^2$. Wynika stąd, że $v_\ell(x_n) = v_\ell(x_{n/2}) + 1$. Pokazaliśmy zatem, że w każdym razie $4 \nmid \Phi_n(a, b)$.

Krok II: $\Phi_n(a, b)$ ma co najwyżej jeden czynnik pierwszy.

Przypuśćmy nie wprost, że $\Phi_n(a, b)$ jest podzielne przez dwie liczby pierwsze $\ell_1 > \ell_2$, z których każda dzieli n. Rozumując jak w Kroku I otrzymujemy, że

$$\ell_1 \mid x_{n/\ell_1} \qquad \text{oraz} \qquad \ell_2 \mid x_{n/\ell_2}.$$

Jest jasne, że a i b nie są podzielne przez ℓ_1 i ℓ_2. Twierdzimy, że $\ell_2 \nmid x_{n/\ell_1}$. Faktycznie, ponownie stosując twierdzenie 1.4, otrzymujemy, że jeśli $\ell_2 \mid x_{n/\ell_1}$, to (ponieważ $\ell_1 \neq \ell_2$) mamy $v_{\ell_2}(x_n) = v_{\ell_2}(x_{n/\ell_1})$, a zatem $\ell_2 \nmid \Phi_n(a, b)$. Mamy zatem kongruencje

$$a^{n/\ell_1} \not\equiv b^{n/\ell_1} \bmod \ell_2 \qquad \text{and} \qquad a^n \equiv b^n \bmod \ell_2.$$

Niech k będzie taką liczbą całkowitą, że $kb^{n/\ell_1} \equiv a^{n/\ell_1} \bmod \ell_2$. Mamy zatem $k \not\equiv 1 \bmod \ell_2$ oraz $k^{\ell_1} \equiv 1 \bmod \ell_2$. Z drugiej strony, z małego twierdzenia Fermata dostajemy kongruencje $k^{\ell_2 - 1} \equiv 1 \bmod \ell_2$. Ponieważ ℓ_1 i $\ell_2 - 1$ są względnie pierwsze, otrzymujemy stąd, że $k \equiv 1 \bmod \ell_2$. Sprzeczność.

Z kroków I i II wynika, że $\Phi_n(a, b)$ jest bądź liczbą pierwszą dzielącą n, bądź jest równa 1. Ta druga możliwość jest jednak sprzeczna z lematem 5. □

Podobnie jak w szczególnych przypadkach rozważanych wcześniej, dla zakończenia dowodu twierdzenia Zsigmondy'ego musimy oszacować $\Phi_n(a, b)$ od dołu, by pokazać, że $\Phi_n(a, b)$ jest większe niż jakikolwiek czynnik pierwszy n. To da nam poszukiwaną sprzeczność. Niestety, w tym celu musimy przeanalizować kilka przypadków. Zanim przystąpimy do tego, zauważmy, że dowód jest bardzo prosty w przypadku, gdy $b = 1$, $a \geqslant 3$. Faktycznie, mamy wówczas $\varphi(n) \geqslant \varphi(p) = p - 1$, i lemat daje natychmiast nierówność

$$\Phi_n(a) = \Phi_n(a, 1) > (a - 1)^{\varphi(n)} \geqslant (a - 1)^{p-1} \geqslant 2^{p-1} \geqslant p,$$

gdyż ostra nierówność $\Phi_n(a, b) > (a - b)^{\varphi(n)}$ zachodzi dla wszystkich $n \geqslant 2$, a w ostatnim przejściu korzystamy z nierówności $2^{m-1} \geqslant m$ dla $m \geqslant 2$, która jest łatwa do pokazania np. przez indukcję po m.

Lemat 5.2. Niech $n \geqslant 2$ będzie liczbą naturalną, p liczbą pierwszą dzielącą n, zaś $a > b \geqslant 1$ liczbami całkowitymi. Wówczas zachodzi nierówność $\Phi_n(a, b) > p$, chyba że $n = 6$, $a = 2$, $b = 1$.

Dowód. Bez straty ogólności możemy założyć, że p jest największym dzielnikiem pierwszym n. Jeśli tylko $a - b \geqslant 2$, dowód przedstawiony powyżej w szczególnym przypadku wciąż działa:

$$\Phi_n(a, b) > (a - b)^{\varphi(n)} \geqslant (a - b)^{p-1} \geqslant 2^{p-1} \geqslant p.$$

Pozostaje nam rozpatrzyć przypadek $a - b = 1$. Jeśli n jest podzielne przez p^2, to na mocy stwierdzenia 3.2 mamy $\Phi_n(a, b) = \Phi_{n/p}(a^p, b^p)$, i poprzednie rozumowanie może zostać zastosowane, albowiem $a^p - b^p > a - b = 1$.

Pozostaje nam rozpatrzeć przypadek $a - b = 1$ oraz n będącego iloczynem różnych liczb pierwszych. Mamy wówczas

$$\Phi_n(a, b) = \frac{\Phi_{n/p}(a^p, b^p)}{\Phi_{n/p}(a, b)}.$$

Używając nierówności z lematu uzyskujemy

$$\Phi_n(a,b) \geqslant \left(\frac{a^p-b^p}{a+b}\right)^{\varphi(n/p)} = \left(\frac{(b+1)^p-b^p}{2b+1}\right)^{\varphi(n/p)} \geqslant \frac{(b+1)^p-b^p}{2b+1}.$$

Gdy $b \geqslant 3$ i $p \geqslant 3$ lub $b = 2$ i $p \geqslant 5$, wyrażenie to możemy przeszacować przez

$$\frac{(b+1)^p-b^p}{2b+1} \geqslant p\frac{b^{p-1}}{2b+1} > p,$$

bowiem w tym przypadku $b^{p-1} > 2b+1$. Gdy $b = 1$, wyrażenie to jest równe $\frac{2^p-1}{3}$, co jest ściśle większe od p dla $p \geqslant 5$.

Przypadek, gdy $p \leqslant 3$ oznacza, że $n \in \{2,3,6\}$. Dla $n \in \{2,3\}$ mamy $\Phi_2(a,b) = a+b > 2$ oraz $\Phi_3(a,b) = a^2+ab+b^2 > 3$. W ostatnim przypadku $n = 6$ mamy $\Phi_6(a,b) = a^2-ab+b^2 = b^2+b+1 > 3$ dla $(a,b) \neq (2,1)$. Pozostaje przypadek $n = 6$, $a = 2$, $b = 1$, gdy zachodzi równość $\Phi_6(2,1) = 3$. □

Dowód twierdzenia Zsigmondy'ego. Twierdzenie wynika natychmiast z lematów 5.1 i 5.2. □

Literatura

1. Evans Chen, *The OTIS excerpts. A collection of 192 problems and solutions*, `https://web.evanchen.cc/excerpts.html`, 2019.
2. Santiago Cuellar and Samper Jose Alexandro, *A nice and tricky lemma*, Mathematical Reflections **3** (2007), `http://reflections.awesomemath.org/2007_3/Lifting_the_exponent.pdf`.
3. Bart Michels, *Zsigmondy's theorem*, `https://www.math.univ-paris13.fr/~michels/files/zsigmondy_en.pdf`, 2014.
4. Amir Hossein Parvardi, *Lifting The Exponent Lemma (LTE)*, `https://imosuisse.ch/smo/skripte/unused/Lifting_the_exponent_EN.pdf`, 2011.
5. M. Teleuca, *Zsigmondy's theorem and its applications in contest problems*, Internat. J. Math. Ed. Sci. Tech. **44** (2013), no. 3, 443–451, `https://doi.org/10.1080/0020739X.2012.714493`. MR 3172590
6. Karl Zsigmondy, *Zur Theorie der Potenzreste*, Monatsh. Math. Phys. **3** (1892), no. 1, 265–284. MR 1546236