Podróże po Imperium Liczb

Część 12. Wielomiany

Rozdział 12

12. Wielomiany cyklotomiczne

Andrzej Nowicki 31 maja 2013, http://www.mat.uni.torun.pl/~anow

Spis treści

12 Wielomiany cyklotomiczne **143**
12.1 Definicja i przykłady 143
12.2 Początkowe własności wielomianów cyklotomicznych 144
12.3 Nierozkładalność wielomianów cyklotomicznych 146
12.4 Następne własności wielomianów cyklotomicznych 147
12.5 Wielomiany cyklotomiczne i nierówności 151
12.6 Wielomiany cyklotomiczne nad ciałami 152
12.7 Wielomiany $\Psi_n(x, y)$ 153
12.8 Wielomiany cyklotomiczne i ich numery 154
12.9 Współczynniki wielomianów cyklotomicznych 158
12.10 Współczynniki wielomianu $\Phi_{pq}(x)$ 159
12.11 Współczynniki wielomianów $\Phi_{pqr}(x)$ i $\Phi_{pqrs}(x)$ 162
12.12 Liczby naturalne postaci $\Phi_n(a)$ 164
12.13 Podzielność liczb $\Phi_n(a)$ przez liczby pierwsze 166
12.14 Twierdzenie Hurwitza 169
12.15 Twierdzenie Banga o rzędach 169
12.16 Liczby pierwsze w postępach arytmetycznych 172
12.17 Wielomiany podzielne przez $x^2 + x + 1$ 172
12.18 Inne zastosowania wielomianów cyklotomicznych 176

Wszystkie książki z serii "Podróże po Imperium Liczb" napisano w edytorze LaTeX. Spisy treści tych książek oraz pewne wybrane rozdziały moża znaleźć na internetowej stronie autora: http://www-users.mat.uni.torun.pl/~anow.

12 Wielomiany cyklotomiczne

12.1 Definicja i przykłady

Niech $n \geqslant 1$ będzie ustaloną liczbą naturalną. Wiadomo, że istnieje dokładnie $\varphi(n)$ pierwiastków pierwotnych n-tego stopnia z jedynki. Oznaczmy te pierwiastki przez $\omega_1, \ldots, \omega_{\varphi(n)}$ i niech

$$\boxed{\Phi_n(x) = \prod_{k=1}^{\varphi(n)} (x - \omega_k)}\,.$$

$\Phi_n(x)$ nazywamy *n-tym wielomianem cyklotomicznym* lub *n-tym wielomianem podziału koła*. Jest to wielomian moniczny stopnia $\varphi(n)$ i jego pierwiastkami są wszystkie pierwiastki pierwotne n-tego stopnia z jedynki. Udowodnimy w następnych podrozdziałach, że każde takie $\Phi_n(x)$ jest nieprzywiedlnym wielomianem o współczynnikach całkowitych (patrz 12.3.1 oraz 12.2.8).

Przykłady:

$$\begin{aligned}
\Phi_1(x) &= x - 1, & \Phi_{11}(x) &= x^{10} + x^9 + x^8 + \cdots + x + 1,\\
\Phi_2(x) &= x + 1, & \Phi_{12}(x) &= x^4 - x^2 + 1,\\
\Phi_3(x) &= x^2 + x + 1, & \Phi_{13}(x) &= x^{12} + x^{11} + x^{10} + \cdots + x + 1,\\
\Phi_4(x) &= x^2 + 1, & \Phi_{14}(x) &= x^6 - x^5 + x^4 - x^3 + x^2 - x + 1,\\
\Phi_5(x) &= x^4 + x^3 + x^2 + x + 1, & \Phi_{15}(x) &= x^8 - x^7 + x^5 - x^4 + x^3 - x + 1,\\
\Phi_6(x) &= x^2 - x + 1, & \Phi_{16}(x) &= x^8 + 1,\\
\Phi_7(x) &= x^6 + x^5 + \cdots + x + 1, & \Phi_{17}(x) &= x^{16} + x^{15} + x^{14} + \cdots + x + 1,\\
\Phi_8(x) &= x^4 + 1, & \Phi_{18}(x) &= x^6 - x^3 + 1,\\
\Phi_9(x) &= x^6 + x^3 + 1, & \Phi_{19}(x) &= x^{18} + x^{17} + x^{16} + \cdots + x + 1,\\
\Phi_{10}(x) &= x^4 - x^3 + x^2 - x + 1, & \Phi_{20}(x) &= x^8 - x^6 + x^4 - x^2 + 1,
\end{aligned}$$

$$\begin{aligned}
\Phi_{21}(x) &= x^{12} - x^{11} + x^9 - x^8 + x^6 - x^4 + x^3 - x + 1,\\
\Phi_{22}(x) &= x^{10} - x^9 + x^8 - x^7 + x^6 - x^5 + x^4 - x^3 + x^2 - x + 1,\\
\Phi_{23}(x) &= x^{22} + x^{21} + x^{20} + \cdots + x^2 + x + 1,\\
\Phi_{24}(x) &= x^8 - x^4 + 1,\\
\Phi_{25}(x) &= x^{20} + x^{15} + x^{10} + x^5 + 1,\\
\Phi_{26}(x) &= x^{12} - x^{11} + x^{10} - x^9 + x^8 - x^7 + x^6 - x^5 + x^4 - x^3 + x^2 - x + 1,\\
\Phi_{27}(x) &= x^{18} + x^9 + 1,\\
\Phi_{28}(x) &= x^{12} - x^{10} + x^8 - x^6 + x^4 - x^2 + 1,\\
\Phi_{29}(x) &= x^{28} + x^{27} + x^{26} + \cdots + x^2 + x + 1,\\
\Phi_{30}(x) &= x^8 + x^7 - x^5 - x^4 - x^3 + x + 1,\\
\Phi_{50}(x) &= x^{20} - x^{15} + x^{10} - x^5 + 1,\\
\Phi_{100}(x) &= x^{40} - x^{30} + x^{20} - x^{10} + 1,\\
\Phi_{1000}(x) &= x^{400} - x^{300} + x^{200} - x^{100} + 1.
\end{aligned}$$

12.2 Początkowe własności wielomianów cyklotomicznych

12.2.1. *Z definicji wielomianów cyklotomicznych wynika, że*

$$\boxed{\Phi_n(x) = \prod_{k \in A_n} (x - \xi^k)},$$

gdzie $\xi = \cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n}$ *oraz* A_n *jest zbiorem wszystkich liczb naturalnych zbioru* $\{1, \ldots, n\}$ *względnie pierwszych z* n.

12.2.2. *Dla* $n \geqslant 3$ *zachodzi równość*

$$\Phi_n(x) = \prod_{k \in B_n} \left(x^2 - 2x \cos\left(\frac{2k\pi}{n}\right) + 1 \right),$$

gdzie B_n *jest zbiorem wszystkich liczb naturalnych mniejszych od* $\frac{n}{2}$ *i względnie pierwszych z liczbą* n.

D. Wynika to z równości 12.2.1 oraz tego, że ξ^{n-k} jest sprzężeniem liczby ξ^k. ⊠

12.2.3. *Jeżeli* $n \neq m$, *to* $\Phi_n(x) \neq \Phi_m(x)$.

D. Niech U_n i U_m będą zbiorami pierwiastków pierwotnych odpowiednio stopni n i m z jedynki. Wiadomo, że jeśli $n \neq m$, to $U_n \neq U_m$ (a nawet $U_n \cap U_m = \emptyset$). Zatem jeśli $n \neq m$, to $\Phi_n(x) \neq \Phi_m(x)$, gdyż są to wielomiany moniczne mające różne zbiory pierwiastków. ⊠

Niech $n \geqslant 2$ będzie ustaloną liczbą naturalną. Przez $F_n(x)$ oznaczać będziemy wielomian należący do $\mathbb{Z}[x]$, będący najmniejszą wspólną wielokrotnością wszystkich wielomianów postaci $x^d - 1$, gdzie $d < n$ oraz $d \mid n$. Dodatkowo przyjmujemy, że $F_1(x) = 1$. Zapamiętajmy:

$$\boxed{F_n(x) = \mathrm{nww}\Big\{x^d - 1;\ d < n,\ d \mid n,\ d \in \mathbb{N}\Big\}}.$$

Z tej definicji wynika, że $F_n(x)$ jest monicznym wielomianem o współczynnikach całkowitych, podzielnym przez wielomian $x - 1$. Ponadto, $x^d - 1$ dzieli $F_n(x)$ dla wszystkich $1 \leqslant d < n$ takich, że $d \mid n$.

12.2.4. *Niech* e *będzie pierwiastkiem pierwotnym* n*-tego stopnia z jedynki. Wówczas:*

$$F_n(x) = \prod_{\substack{r \in \{1,2,\ldots,n\} \\ (r,n)>1}} (x - e^r).$$

12.2.5. *Dla każdego* $n \in \mathbb{N}$ *zachodzi równość* $x^n - 1 = F_n(x) \cdot \Phi_n(x)$. ([Br77], [La84]).

12.2.6. *Jeżeli* p *jest liczbą pierwszą, to*

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \ldots + x + 1.$$

D. Jedyną liczbą naturalną mniejszą niż p i dzielącą p jest $d = 1$. Wobec tego $F_p = (x-1)$. Z równości 12.2.5 wynika zatem, że $\Phi_p(x) = \frac{x^p-1}{x-1} = x^{p-1} + x^{p-2} + \ldots + x + 1$. ⊠

12.2.7. *Niech $A \subset B$ będą pierścieniami (przemiennymi z 1). Rozważmy trzy wielomiany: $f(x), g(x), h(x)$ należące do $B[x]$. Załóżmy, że:*

(a) $f(x) = g(x)h(x)$,

(b) *$f(x)$ i $g(x)$ są moniczne,*

(c) $f(x), g(x) \in A[x]$.

Wtedy wielomian $h(x)$ jest moniczny i należy do $A[x]$.

D. Moniczność wielomianu $h(x)$ jest oczywista. Niech:

$$\begin{aligned} f(x) &= x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0, \\ g(x) &= x^m + b_{m-1}x^{m-1} + \ldots + b_1x + b_0, \\ h(x) &= x^s + c_{s-1}x^{s-1} + \ldots + c_1x + c_0, \end{aligned}$$

Współczynniki postaci a_i, b_j należą do A, natomiast współczynniki postaci c_i należą do B. Ponieważ $f(x) = g(x)h(x)$, więc porównując współczynniki przy x^{n-1} mamy $a_{n-1} = c_{s-1} + b_{m-1}$. Stąd $c_{s-1} = a_{n-1} - b_{m-1} \in A$. Wiemy więc, że $c_{s-1} \in A$. Załóżmy, że wiemy już, że wszystkie współczynniki

$$c_{s-1},\ c_{s-2},\ \ldots,\ c_{k+2},\ c_{k+1}$$

należą do A. Pokażemy, że wówczas współczynnik c_k również należy do A. W tym celu porównajmy w równości $f(x) = g(x)h(x)$ współczynniki przy x^{k+s}. Wtedy $a_{k+s} = c_k + c_{k+1}b_{s-1} + c_{k+2}b_{s-2} + \ldots$ i wobec tegoże

$$c_k = a_{k+s} - (c_{k+1}b_{s+1} + c_{k+2}b_{s-2} + \ldots).$$

Prawa strona należy do A. Zatem $c_k \in A$ i to kończy nasz indukcyjny dowód. ⊠

12.2.8. *Każdy wielomian $\Phi_n(x)$ należy do pierścienia $\mathbb{Z}[x]$. Innymi słowy, wszystkie współczynniki dowolnego wielomianu cyklotomicznego są liczbami całkowitymi.* ([Br77], [La84]).

D. Wiemy, że $x^n - 1 = F_n(x)\Phi_n(x)$ (patrz 12.2.5). Wielomiany $x^n - 1$ i $F_n(x)$ są moniczne i należą do $\mathbb{Z}[x]$. Z 12.2.7 wynika więc, że wielomian $\Phi_n(x)$ również należy do $\mathbb{Z}[x]$. ⊠

★ T. Nagell, *The cyclotomic polynomial*, [Nagl] 158-160.

12.3 Nierozkładalność wielomianów cyklotomicznych

12.3.1 (Kronecker)**.** *Każdy wielomian $\Phi_n(x)$ jest nierozkładalny w $\mathbb{Z}[x]$.* ([Br77], [Fila] s.86).

D. ([Br77]). Przypuśćmy, że wielomian $\Phi_n(x)$ jest rozkładalny w $\mathbb{Z}[x]$. Istnieją wtedy dwa wielomiany $g(x)$ i $h(x)$ należące do $\mathbb{Z}[x]$ (dodatniego stopnia) takie, że:

$$\Phi_n(x) = g(x) \cdot h(x).$$

Możemy założyć, że wielomian $g(x)$ jest nierozkładalny w $\mathbb{Z}[x]$. Załóżmy ponadto, że są to wielomiany moniczne. Ponieważ $\Phi_n(\omega_1) = \Phi_n(\omega_2) = \ldots = \Phi_n(\omega_{\varphi(n)}) = 0$, gdzie $\omega_1, \omega_2, \ldots, \omega_{\varphi(n)}$ są wszystkimi pierwiastkami pierwotnymi n-tego stopnia z jedynki, więc istnieje co najmniej jeden z tych pierwiastków pierwotnych, oznaczmy go przez e, spełniający równość $g(e) = 0$.

Niech p będzie taką liczbą pierwszą, że $p \nmid n$. Udowodnimy, że $g(e^p) = 0$. W tym celu zauważmy najpierw, że e^p jest również pierwiastkiem pierwotnym n-tego stopnia z jedynki (ponieważ liczby p, n są względnie pierwsze). Zatem $\Phi_n(e^p) = 0$, więc $g(e^p) = 0$ lub $h(e^p) = 0$. Pokażemy, że $g(e^p) = 0$.

Przypuśćmy, że $h(e^p) = 0$. Wówczas liczba e jest pierwiastkiem jednocześnie wielomianów $g(x)$ oraz $h(x^p)$. Ponieważ wielomian $g(x)$ jest jest nierozkładalny w $\mathbb{Z}[x]$, więc stąd wynika, że $g(x)$ dzieli $h(x^p)$ w $\mathbb{Z}[x]$. Zatem

$$h(x^p) = g(x) \cdot v(x),$$

gdzie $v(x) \in \mathbb{Z}[x]$. Rozpatrzmy homomorfizm pierścieni $\alpha : \mathbb{Z}[x] \longrightarrow \mathbb{Z}_p[x]$ indukowany przez naturalny homomorfizm: $\mathbb{Z} \to \mathbb{Z}_p$ (liczbie całkowitej a przyporządkowana jest reszta z dzielenia a przez p). Mamy wówczas w pierścieniu $\mathbb{Z}_p[x]$ następujące dwie równości:

$$\alpha(\Phi_n(x)) = \alpha(g(x)) \cdot \alpha(h(x)), \qquad \alpha(h(x^p)) = \alpha(g(x)) \cdot \alpha(v(x)).$$

Ale $\alpha(h(x^p)) = (\alpha(h(x)))^p$, więc $\alpha(h(x))^p = \alpha(g(x)) \cdot \alpha(v(x))$. Wielomian $\alpha(v[x])$ ma stopień $\geqslant 1$ (bo jest moniczny). Niech $u(x) \in \mathbb{Z}_p[x]$ będzie wielomianem nierozkładalnym w $\mathbb{Z}_p[x]$ dzielącym $\alpha(v(x))$. Wtedy wielomian $u(x)$ dzieli wielomian

$$(\alpha(h(x)))^p = \underbrace{\alpha(h(x)) \cdot \alpha(h(x)) \cdots \alpha(h(x))}_{p},$$

dzieli więc $\alpha(h(x))$. Wielomian $u(x)$ dzieli więc jednocześnie wielomiany $\alpha(g(x))$ i $\alpha(h(x))$. Oznacza to, że wielomiany $\alpha(g(x))$ i $\alpha(h(x))$ mają wspólny czynnik w $\mathbb{Z}_p[x]$. Stąd wynika dalej, że wielomian

$$\alpha(\Phi_n(x)) = \alpha(g(x)) \cdot \alpha(h(x))$$

ma czynnik wielokrotny w $\mathbb{Z}_p[x]$. Ale $x^n - 1 = F_n(x) \cdot \Phi_n(x)$ (patrz 12.2.5), więc w pierścieniu $\mathbb{Z}_p[x]$ mamy równość

$$x^n - 1 = \alpha(x^n - 1) = \alpha(f_n(x)) \cdot \alpha(\Phi_n(x)),$$

z której wynika, że wielomian $x^n - 1$ ma czynnik wielokrotny w $\mathbb{Z}_p[x]$. Zatem w pewnym rozszerzeniu ciała $\mathbb{Z}_p$ wielomian $x^n - 1$ ma pierwiastek podwójny. To jest oczywiście niemożliwe. Doszliśmy zatem do sprzeczności.

W ten sposób wykazaliśmy, że $g(e) = 0$ oraz $g(e^p) = 0$ dla wszystkich takich liczb pierwszych p, że $p \nmid n$. Stąd wynika, że $g(\omega) = 0$ dla każdego ω będącego pierwotnym pierwiastkiem n-tego stopnia z jedynki.

Niech ω będzie pierwiastkiem pierwotnym n-tego stopnia z jedynki. Ponieważ e jest też takim pierwotnym pierwiastkiem, więc $\omega = e^k$ dla pewnego k. Zatem $\operatorname{nwd}(k, n) = 1$. Jeżeli $k = 1$, to $\omega = e$, więc $g(\omega) = g(e) = 0$. Niech teraz $k \geqslant 2$. Niech $k = p_1 p_2 \cdots p_s$, gdzie $p_1, p_2, \ldots, p_s$ są liczbami pierwszymi (niekoniecznie różnymi). Każda z tych liczb pierwszych jest oczywiście względnie pierwsza z liczą n. Zatem $p_1 \nmid n,\ p_2 \nmid n,\ \ldots,\ p_s \nmid n$. Z tego co już udowodniliśmy wynika, że $g(e^{p_1}) = 0$. Przyrównując $e_1 = e^{p_1}$ mamy $g(e_1) = 0$, więc $g(e^{p_2}) = 0$, więc $g(e^{p_1 p_2}) = 0$ i tak dalej aż do równości

$g(e^{p_1p_2\cdots p_s}) = 0$. Zatem $g(e^k) = 0$ czyli $g(\omega) = 0$. Każdy zatem pierwiastek pierwotny n-tego stopnia z jedynki jest zerem wielomianu $g(x)$. Zatem:

$$g(x) = \prod_{k=1}^{\varphi(n)} (x - \omega_k) = \Phi_n(x).$$

Ale $g(x)$ jest nierozkładalne w $\mathbb{Z}[x]$, więc $\Phi_n(x)$ jest wielomianem nierozkładalnym w $\mathbb{Z}[x]$. ⊠

12.3.2. *Jeżeli $n \neq m$, to wielomiany cyklotomiczne $\Phi_n(x)$ i $\Phi_m(x)$ są względnie pierwsze.*

D. Wynika to z tego, że wielomiany $\Phi_n(x)$ oraz $\Phi_m(x)$ są nierozkładalne, moniczne i różne. ⊠

12.3.3 (Kronecker)**.** *Jeśli $f \in \mathbb{Z}[x] \setminus \mathbb{Z}$ jest nierozkładalnym wielomianem monicznym i wszystkie jego pierwiastki (zespolone) leżą na kole*

$$\{z;\ |z| = 1\},$$

to $f(x)$ jest wielomianem cyklotomicznym. ([Fila] s.86).

★ T. Nagell, *Irreducibility of the cyclotomic polynomial*, [Nagl] 160-164.

12.4 Następne własności wielomianów cyklotomicznych

12.4.1. *Jeżeli $d \mid n$, to wielomian $\Phi_d(x)$ dzieli wielomian x^n-1 w $\mathbb{Z}[x]$, tzn. istnieje wielomian $H(x) \in \mathbb{Z}[x]$ taki, że $x^n - 1 = H(x)\Phi_d(x)$.*

D. Niech $n = dm$. Wtedy

$$x^n - 1 = x^{dm} - 1 = (x^d)^m - 1^m = (x^d - 1)(x^{d(m-1)} + x^{d(m-2)} + \ldots + 1),$$

a zatem wielomian $x^d - 1$ dzieli w $\mathbb{Z}[x]$ wielomian $x^n - 1$. Wiemy , że $x^d - 1 = F_d(x) \cdot \Phi_d(x)$ (patrz 12.2.5). Zatem $\Phi_d(x)$ dzieli $x^d - 1$ oraz $x^d - 1$ dzieli $x^n - 1$, a więc $\Phi_d(x)$ dzieli $x^n - 1$. ⊠

12.4.2.
$$\boxed{x^n - 1 = \prod_{d|n} \Phi_d(x)}\,.$$

D. Oznaczmy: $H(x) = \prod_{d|n} \Phi_d(x)$. Ponieważ wielomiany postaci $\Phi_d(x)$ są parami względnie pierwsze (patrz 12.3.2) oraz każdy z nich (gdy $d \mid n$) dzieli wielomian $x^n - 1$ (patrz 12.4.1), więc $H(x)$ dzieli $x^n - 1$. Wielomian $H(x)$ jest moniczny i jego stopień jest równy n, gdyż dobrze wiadomo, że $\sum_{d|n} \varphi(d) = n$. Zatem $H(x) = x^n - 1$. ⊠

12.4.3. *Jeśli $m < n$, to wielomiany $x^m - 1$ i $\Phi_n(x)$ są względnie pierwsze.*

D. Wynika to z 12.4.2 i 12.3.2. ⊠

12.4.4. $x^{15} - 1 = \Phi_1(x)\Phi_3(x)\Phi_5(x)\Phi_{15}(x)$. (Wynika z 12.4.2).

12.4.5 (T. M. Apostol, 1970)**.** *Niech $d < n$ będą liczbami naturalnymi i niech k będzie liczbą naturalną zdefiniowaną następująco:*

$$k = \begin{cases} p, & \text{gdy } \frac{n}{d} \text{ jest potęgą liczby pierwszej } p, \\ 1, & \text{w przeciwnym przypadku.} \end{cases}$$

Istnieją wtedy wielomiany o współczynnikach całkowitych $F(x), G(x)$ takie, że

$$\boxed{k = F(x)\Phi_d(x) + G(x)\Phi_n(x)}.$$

W literaturze matematycznej znajdziemy sporo różnych dowodów tego twierdzenia. W 1970 roku udowodnił to Tom M. Apostol [Apl]. Dwa dowody, w tym jeden Andrzeja Schinzla, opublikował później Michael Filaseta [Fil]. Ostatnio prosty dowód opublikował Gregory Dresden [Drn]. Jego dowód podaje jawnie postać wielomianów $F(x)$ i $G(x)$.

W pierwszym wydaniu tej książki powyższe twierdzenie się nie pojawiło. Autor dziękuje profesorom Władysławowi Narkiewiczowi oraz Andrzejowi Schinzlowi za cenne informacje o tym twierdzeniu i jego dowodach.

W jednym z następnych podrozdziałów (patrz 12.12.6) wykorzystamy pewien szczególny przypadek omawianego twierdzenia. Teraz przedstawimy ten przypadek wraz z dowodem.

Załóżmy, że $m > n$ są liczbami naturalnymi i niech $m = kn + r$, gdzie $k \in \mathbb{N}$, $r \in \mathbb{Z}$, $0 \leqslant r < n$. Mamy wtedy równość

$$x^m - 1 = (x^{m-n} + x^{m-2n} + x^{m-3n} + \cdots + x^{m-kn})(x^n - 1) + x^r - 1.$$

Stosując tego typu równości i postępując tak jak w algorytmie Euklidesa, otrzymujemy:

12.4.6. *Niech $n, m \in \mathbb{N}$ oraz $d = \operatorname{nwd}(n, m)$. Istnieją wtedy wielomiany o współczynnikach całkowitych $A(x), B(x)$ takie, że $x^d - 1 = A(x)(x^n - 1) + B(x)(x^m - 1)$.*

Z powyższych obserwacji wynika, wspomniany wcześniej, następujący szczególny przypadek twierdzenia 12.4.5.

12.4.7. *Jeśli d, n są liczbami naturalnymi takimi, że $d < n$ oraz $d \nmid n$, to istnieją wielomiany o współczynnikach całkowitych $F(x), G(x)$ takie, że*

$$\boxed{1 = F(x)\Phi_d(x) + G(x)\Phi_n(x)}.$$

D. Oznaczmy: $H_k(x) = x^k - 1$ dla wszystkich $k \in \mathbb{N}$.

Niech $r = \operatorname{nwd}(d, n)$ i niech $A(x), B(x) \in \mathbb{Z}[x]$ takie, że

$$(*) \qquad H_r(x) = A(x)H_d(x) + B(x)H_n(x).$$

Takie wielomiany $A(x), B(x)$ istnieją na mocy 12.4.6. Wprowadźmy zbiory:

$$U = \{m \in \mathbb{N};\ m \mid r\}, \quad V_1 = \{m \in \mathbb{N};\ m \mid d,\ m \nmid r\}, \quad V_2 = \{m \in \mathbb{N};\ m \mid n,\ m \nmid r\}$$

U jest zbiorem wszystkich dzielników naturalnych liczby r; każdy taki dzielnik jest oczywiście dzielnikiem liczby d i jest dzielnikiem liczby n. V_1 jest zbiorem tych wszystkich dzielników liczby d, które

nie są dzielnikami liczby r. Natomiast V_2 jest zbiorem tych wszystkich dzielników liczby n, które nie są dzielnikami liczby r.

Zauważmy, że d nie należy do zbioru U. Gdyby bowiem było przeciwnie, to mielibyśmy równości $d = r = \mathrm{nwd}(d, n)$, z których wynikałoby, że d dzieli n; sprzeczność z założeniem, że $d \nmid n$. W podobny sposób uzasadniamy, że n nie należy do zbioru U.

Zatem $d \in V_1$ oraz $n \in V_2$. Oznaczmy:

$$F(x) = \prod_{m \in V_1 \setminus \{d\}} \Phi_m(x), \qquad G(x) = \prod_{m \in V_2 \setminus \{n\}} \Phi_m(x).$$

Jest jasne, że $F(x), G(x)$ są wielomianami o współczynnikach całkowitych. Korzystamy teraz z twierdzenia 12.4.2 i mamy:

$$H_d(x) = \prod_{m|d} \Phi_m(x) = \prod_{m \in U} \Phi_m(x) \cdot \prod_{m \in V_1} \Phi_m(x) = H_r(x) \prod_{m \in V_1} \Phi_m(x) = H_r(x)F(x)\Phi_d(x).$$

W ten sam sposób wykazujemy, że $H_n(x) = H_r(x)G(x)\Phi_n(x)$. Wstawiamy to do równości $(*)$ i po podzieleniu przez $H_r(x)$ otrzymujemy tezę. ⊠

12.4.8. *Dla każdego $n \in \mathbb{N}$ zachodzi równość:*

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

w której μ oznacza funkcję Möbiusa. ([Fila] s.87).

D. Wynika z równości 12.4.2 i własności splotowych funkcji Möbiusa (patrz [N-5]). ⊠

12.4.9. *W ciele $\mathbb{Q}(x)$ dla każdej liczby naturalnej $n \geqslant 2$ zachodzi równość*

$$\Phi_n(x) = x^{\varphi(n)} \Phi_n\left(\frac{1}{x}\right).$$

D. Wynika to z równości 12.4.8 i ze znanych równości $\sum_{d|n} \mu(d)\frac{n}{d} = \varphi(n)$ oraz $\sum_{d|n} \mu(d) = 0$ (dla $n \geqslant 2$). ⊠

12.4.10. *Niech $f(x) \in \mathbb{Z}[x]$ będzie wielomianem z nieparzystymi współczynnikami stopnia $d - 1$. Jeśli $\Phi_n(x)$ dzieli wielomian $f(x)$, to n dzieli $2d$.* ([BoC]).

12.4.11 (Gauss)**.** *Jeśli $n > 1$ jest nieparzystą liczbą bezkwadratową, to istnieją takie wielomiany $A(x), B(x) \in \mathbb{Z}[x]$, że $4\Phi_n(x) = A(x)^2 - n(-1)^{(n-1)/2}B(x)^2$.* (Brent).

12.4.12 (Aurifeuille, Le Lasseur, Lucas)**.** *Jeśli $n > 1$ jest nieparzystą liczbą bezkwadratową, to istnieją takie wielomiany $C(x), D(x) \in \mathbb{Z}[x]$, że $\Phi_n\left((-1)^{(n-1)/2}x\right) = C(x)^2 - nxD(x)^2$.* (Brent).

12.4.13 (Aurifeuille, Le Lasseur, Lucas)**.** *Jeśli n jest parzystą liczbą bezkwadratową, to istnieją takie wielomiany $C(x), D(x) \in \mathbb{Z}[x]$, że $\pm\Phi_{n/2}(-x^2) = C(x)^2 - nxD(x)^2$.* (Brent).

12.4.14. *Przykłady:*

(1) $4\Phi_3(x) = (2x+1)^2 + 3\cdot 1^2$;

(2) $4\Phi_5(x) = (2x^2+x+2)^2 - 5x^2$, $\Phi_5(x) = (x^2+3x+1)^2 - 5x(x+1)^2$;

(3) $4\Phi_{15}(x) = A^2 + 15B^2$, *gdzie* $A = 2x^2 - x^3 - 4x^2 - x + 2$, $B = x^3 - x$;

(4) $\Phi_{15}(-x) = C^2 - 15xD^2$, *gdzie* $C = x^4 + 8x^3 + 13x^2 + 8x + 1$, $D = x^3 + 3x^2 + 3x + 1$.

(Brent).

12.4.15 ([BoC])**.** *Niech $p \in \mathbb{P}$ i niech T_p będzie funkcją przyporządkującą każdemu monicznemu wielomianowi $f(x) = \prod(x - \alpha_i)$ (gdzie każde α_i jest liczbą zespoloną) wielomian*

$$\prod(x - \alpha_i^p).$$

Jeśli n jest liczbą naturalną niepodzielną przez p, to

(1) $T_p\left(\Phi_n(x)\right) = \Phi_n(x)$;

(2) $T_p\left(\Phi_{pn}(x)\right) = \Phi_n(x)^{p-1}$;

(3) $T_p\left(\Phi_{p^s n}(x)\right) = \Phi_{p^{s-1}n}(x)^p$, *dla* $s \geqslant 2$.

Zdefiniowaliśmy wielomiany cyklotomiczne za pomocą pierwiastków pierwotnych z jedynki. Pan Tomasz Ordowski przesłał mi (w maju 2013 roku) następujące zadanie do rozwiązania. Z tezy tego zadania wynika, że wielomiany cyklotomiczne można definiować bez wspominania o pierwiastkach z jedynki.

12.4.16. *Niech $(E_n(x))$ będzie ciągiem wielomianów takim, że*

$$E_1(x) = 1 \quad \textit{oraz} \quad E_{n+1}(x) = \mathrm{nww}\Big(E_n(x),\ x^n - 1\Big) \quad \textit{dla } n \in \mathbb{N}.$$

Wówczas dla każdej liczby naturalnej n, zachodzi równość

$$\frac{E_{n+1}(x)}{E_n(x)} = \Phi_n(x).$$

D. (Sposób I). Udowodnimy indukcyjnie, że dla każdej liczby naturalnej n zachodzi równość

$$(*) \qquad E_{n+1}(x) = \prod_{k=1}^{n} \Phi_k(x).$$

Dla $n = 1$ jest to oczywiste. Jeśli $f(x), g(x)$ są wielomianami, to przez $[f(x), g(x)]$ oznaczać będziemy najmniejszą wspólną wielokrotność tych wielomianów. Krok indukcyjny:

$$E_{n+1}(x) = \Big[E_n(x),\ x^n - 1\Big] = \left[\prod_{k=1}^{n-1} \Phi_k(x),\ \prod_{d|n} \Phi_d(b)\right] = \Big[A(x)B(x),\ A(x)\Phi_n(x)\Big].$$

Wykorzystaliśmy twierdzenie 12.4.2. Tutaj $A(x)$ jest iloczynem wszystkich wielomianów postaci $\Phi_d(x)$, gdzie $d < n$ oraz $d \mid n$. Natomiast $B(x)$ jest iloczynem wszystkich wielomianów postaci $\Phi_d(x)$, gdzie $d < n$ oraz $d \nmid n$. Wiemy, że wielomiany cyklotomiczne są nieprzywiedlne i są parami różne. Zatem,

wielomiany $B(x)$ oraz $\Phi_n(x)$ są względnie pierwsze, a zatem $[B(x),\ \Phi_n)(x)] = B(x)\cdot\Phi_n(x)$. Mamy więc:

$$\begin{aligned} E_{n+1}(x) &= \Big[A(x)B(x),\ A(x)\Phi_n(x)\Big] = A(x)\Big[B(x),\ \Phi_n(x)\Big] \\ &= A(x)B(x)\Phi_n(x) = \Big(\textstyle\prod_{k=1}^{n-1}\Phi_k(x)\Big)\cdot\Phi_n(x) \\ &= \textstyle\prod_{k=1}^{n}\Phi_k(x) \end{aligned}$$

i to kończy nasz indukcyjny dowód równości $(*)$. Zatem $E_{n+1}(x)/E_n(x) = \Phi_n(x)$. ⊠

D. (Sposób II). (Władysław Narkiewicz). Niech $A_n(x) = E_{n+1}(x)/E_n(x)$. Jeśli liczba (zespolona) z jest pierwiastkiem wielomianu $A_n(x)$, to $E_{n+1}(z) = 0$ oraz $E_n(z)$ jest niezerowe, gdyż wielomiany $E_n(x)$ nie mają pierwiastków wielokrotnych. Zatem z musi być pierwiastkiem wielomianu $x^n - 1$, wiec jest pierwiastkiem n-tego stopnia z jedynki. Zauważmy, że ten pierwiastek jest pierwotny. Gdyby nie był, to mielibyśmy równość $E_n(z) = 0$, a to jest niemożliwe. Zatem każdy pierwiastek wielomianu $A_n(x)$ jest pierwiastkiem n-tego wielomianu cyklotomicznego $\Phi_n(x)$ i z nieprzywiedlności tego ostatniego wynika, że $A_n(x) = \Phi_n(x)$. ⊠

★ R. P. Brent, *On computing factors of cyclotomic polynomials*, preprint, 1993.
L. Carlitz, *Note on the cyclotomic polynomials*, [Mon] 61(2)(1954) 106-108.
M. Isaacs, *Cyclotomy and geometric constructions*. [Isaa], rozdział 20.
D. R. Kohel, *Cyclotomic polynomials and base b representations of integers*, preprint.
J. MacDougall, *Mersenne composities and cyclotomic primes*, [MG] 87(508)(2003) 71-75.
D. G. C. McKeon, T. N. Sherry, *Exploring cyclotomic polynomials*, [MG] 502(2001) 59-65.
K. F. McLean, *Cyclotomic and double angle polynomials*, [MG] 88(512)(2004) 208-214.
L. Mirsky, *A note on cyclotomic polynomials*, [Mon] 69(8)(1962) 772-775.
K. Motose, *Ramanujan's sums and cyclotomic polynomials*, Hirosaki 2004.
K. Motose, *On Euclidean algorithm*, Hirosaki, 2005.
P. Ribenboim, *Wielomiany podziału koła*, [Ri01] 93-108.
M. Sawczuk, *Wielomiany cyklotomiczne*, [Pmgr] 2001.
W. Sengerov, A. Spivak, *Wielomiany podziału okręgu*, [Kw] 1/1998 11-18, 2/1998 63-64.

12.5 Wielomiany cyklotomiczne i nierówności

12.5.1. *Dla każdego $n \in \mathbb{N}$ funkcja $\Phi_n(x)$ jest ściśle rosnąca w przedziale $[1,\infty)$.* ([Mot1]).

D. To jest oczywiste dla $n = 1$ i $n = 2$, gdyż $\Phi_1(x) = x-1$, $\Phi_2(x) = x+1$. Jeśli $n \geqslant 3$, to fakt ten łatwo wynika z równości $\Phi_n(x) = \prod_{k\in B_n}\left(x^2 - 2x\cos\left(\frac{2k\pi}{n}\right) + 1\right)$, gdzie B_n jest zbiorem wszystkich liczb naturalnych mniejszych od $\frac{n}{2}$ i względnie pierwszych z n (patrz 12.2.2). Każda bowiem funkcja postaci $f(x) = x^2 - 2x\cos\left(\frac{2k\pi}{n}\right) + 1$ (dla $n \geqslant 3$) jest ściśle rosnąca w przedziale $[1,\infty)$. ⊠

12.5.2. *Jeśli $n \geqslant 2$, to $\Phi_n(a) \geqslant 1$ dla wszystkich liczb rzeczywistych $a \geqslant 1$.*

D. Z dowodu faktu 12.5.1 wynika, że $\Phi_n(1) > 0$. Zatem $\Phi_n(1) \geqslant 1$ (gdyż $\Phi_n(1) \in \mathbb{Z}$). To, że $\Phi_n(1) \geqslant 1$ wynika również z 12.9.3. Jeśli więc $a \geqslant 1$, to $\Phi_n(a) \geqslant \Phi_n(1) \geqslant 1$ (na mocy 12.5.1). ⊠

12.5.3. *Jeśli $n \geqslant 2$, to dla każdej liczby naturalnej a zachodzi nierówność*

$$|\Phi_n(a)| > a - 1.$$

D. ([Br68]). Niech e będzie pierwiastkiem n-tego stopnia z jedynki. Dla $a = 1$ oczywiście $\Phi_n(a) \neq 0$, a zatem $|\Phi_n(q)| \geqslant 1 > q-1 = 0$. Przypuśćmy więc, że $a > 1$. Wówczas dla dowolnej liczby całkowitej k mamy: $|a - e^k| \geqslant |a| - |e^k| = a - 1 \geqslant 1$. Wobec tego:

$$\Phi_n(a) = \prod_{\substack{r\in\{1,2,\ldots,n\}\\(r,n)=1}} |a - e^r| \geqslant |a - e|.$$

Ponieważ e nie jest liczbą rzeczywistą dodatnią dla $n > 1$, więc $|a - e| > |a| - |e| = a - 1$. ⊠

U. Powyższy fakt wykorzystuje się w dowodzie Twierdzenia Wedderburna o przemienności ciał skończonych (patrz np. [Br68]). ⊠

12.5.4. *Jeśli $n \geqslant 2$, to dla każdej liczby naturalnej a zachodzi nierówność*

$$\Phi_n(a) \geqslant a.$$

D. Już wiemy z 12.5.2, że $\Phi_n(1) \geqslant 1$. Zatem rozważana nierówność jest prawdziwa dla $a = 1$. Niech teraz a będzie liczbą naturalną większą od 1 i przypuśćmy, że $\Phi_n(a) < a$. Ponieważ $1 < 2 < \cdots < a - 1 < a$, więc na mocy 12.5.1 otrzymujemy:

$$1 \leqslant \Phi_n(1) < \Phi_n(2) < \cdots < \Phi_n(a-1) < \Phi_n(a) < a,$$

przy czym wszystkie liczby $\Phi_n(1), \Phi_n(2), \ldots, \Phi_n(a)$ są naturalne (gdyż $\Phi_n(x) \in \mathbb{Z}[x]$). Otrzymaliśmy sprzeczność: pomiędzy 1 i a jest $a + 1$ liczb naturalnych. ⊠

12.5.5. *Niech $n \geqslant 2$ będzie liczbą naturalną. Niech $r = \omega(n)$ będzie liczbą wszystkich liczb pierwszych dzielących n. Niech $n' = r(n)$ będzie iloczynem wszystkich liczb pierwszych dzielących n i niech $m = n/n'$. Wtedy:*

(1) *jeśli r jest liczbą parzystą, to $\dfrac{a^m - 1}{a^m} a^{\varphi(n)} < \Phi_n(a) < a^{\varphi(n)}$, dla wszystkich liczb rzeczywistych $a \geqslant 2$;*

(2) *jeśli r jest liczbą nieparzystą, to $a^{\varphi(n)} < \Phi_n(a) < \dfrac{a^m}{a^m - 1} a^{\varphi(n)}$, dla wszystkich liczb rzeczywistych $a \geqslant 2$.* ([Mot1]).

12.5.6. *$(a-1)^{\varphi(n)} < \Phi_n(a) \leqslant (a+1)^{\varphi(n)}$, dla $n \geqslant 2$, $a \geqslant 2$.* ([Mot5]).

12.5.7. *$\dfrac{1}{2} a^{\varphi(n)} < \Phi_n(a) \leqslant 2a^{\varphi(n)}$, dla $n \geqslant 2$, $a \geqslant 2$.* (R.Thangadurai, A.Vatwani, [Mon] 118(8)(2011)).

oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

12.6 Wielomiany cyklotomiczne nad ciałami

oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

12.6.1. *Niech $p \in \mathbb{P}$, $n, m \in \mathbb{N}$, $n \neq m$, $p \nmid n$, $p \nmid m$. Wtedy wielomiany $\Phi_n(x)$ i $\Phi_m(x)$ są względnie pierwsze w $\mathbb{Z}_p[x]$.* ([BoC]).

12.6.2. *Jeśli $p \in \mathbb{P}$, to $\Phi_p(x) = (x-1)^{p-1}$ w $\mathbb{Z}_p[x]$.*

12.6.3. *Niech $p \in \mathbb{P}$, $n \in \mathbb{N}$, $p \nmid n$. Niech $m = \delta_n(p)$ będzie rzędem liczby p modulo n. Wtedy wielomian $\Phi_n(x)$, traktowany jako wielomian należący do $\mathbb{Z}_p[x]$, jest iloczynem $\varphi(n)/m$ parami różnych wielomianów nierozkładalnych w $\mathbb{Z}_p[x]$, z których każdy jest stopnia m.* ([Mon] 75(1)(1968) 46).

12.6.4. *Niech k będzie $q = p^s$ elementowym ciałem. Niech $n \in \mathbb{N}$, $p \nmid n$ i niech $m = \delta_n(q)$ będzie rzędem liczby q modulo n. Wtedy wielomian $\Phi_n(x)$, traktowany jako wielomian należący do $k[x]$, jest iloczynem $\varphi(n)/m$ parami różnych wielomianów nierozkładalnych w $k[x]$, z których każdy jest stopnia m.* ([Mot5], [Mot7]).

12.6.5. *Niech $n, s \in \mathbb{N}$. Wielomian $\Phi_n(x^s)$ jest nierozkładalny w $\mathbb{Q}[x]$ wtedy i tylko wtedy, gdy każdy dzielnik pierwszy liczby s jest dzielnikiem pierwszym liczby n.* ([Golo]).

★ W. J. Guerrier, *The factorization of the cyclotomic polynomials mod p*, [Mon] 75(1)(1968) 46.

oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

12.7 Wielomiany $\Psi_n(x, y)$

oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

Oznaczmy:

$$\boxed{\Psi_n(x,y) = y^{\varphi(n)}\Phi_n\left(\frac{x}{y}\right)}.$$

Przykłady:

$$\begin{aligned}
\Psi_1(x,y) &= x - y,\\
\Psi_2(x,y) &= x + y,\\
\Psi_3(x,y) &= x^2 + xy + y^2,\\
\Psi_4(x,y) &= x^2 + y^2,\\
\Psi_5(x,y) &= x^4 + x^3y + x^2y^2 + xy^3 + y^4,\\
\Psi_6(x,y) &= x^2 - xy + y^2,\\
\Psi_7(x,y) &= x^6 + x^5y + x^4y^2 + x^3y^3 + x^2y^4 + xy^5 + y^6,\\
\Psi_8(x,y) &= x^4 + y^4,\\
\Psi_9(x,y) &= x^6 + x^3y^3 + y^6.
\end{aligned}$$

12.7.1. *Z własności wielomianów cyklotomicznych wynikają następujące własności wielomianów postaci $\Psi_n(x, y)$.*

(1) *Każde $\Psi_n(x, y)$ jest jednorodnym wielomianem stopnia $\varphi(n)$ zmiennych x i y o współczynnikach całkowitych.*

(2) *Każdy wielomian $\Psi_n(x, y)$ jest nierozkładalny w $\mathbb{Z}[x, y]$.*

(3) $\Phi_n(x) = \Psi_n(x, 1)$.

(4) $\Psi_n(x,y) = \prod_{d|n}\left(x^{n/d} - y^{n/d}\right)^{\mu(d)}$.

(5) $x^n - y^n = \prod_{d|n}\Psi_d(x, y)$.

12.7.2. $\Psi_n(x, y) = \Psi_n(y, x)$, *dla $n \geqslant 2$.* ([Mot7]).

D. Wynika to z równości

$$\Psi_n(x,y) = \prod_{d|n} \left(x^{n/d} - y^{n/d}\right)^{\mu(d)} \quad \text{oraz} \quad \sum_{d|n} \mu(d) = 0$$

(dla $n \geqslant 2$). ⊠

oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

12.8 Wielomiany cyklotomiczne i ich numery

oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

Najpierw zajmować się będziemy wielomianami cyklotomicznymi, których numery są potęgami liczb pierwszych. Wiemy (patrz 12.2.6), że jeżeli p jest liczbą pierwszą, to

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \ldots + x + 1.$$

12.8.1. $\Phi_{p^2}(x) = x^{p(p-1)} + x^{p(p-2)} + \ldots + x^p + 1.$

12.8.2. *Jeżeli p jest liczbą pierwszą i k jest liczbą naturalną to*

$$\Phi_{p^k}(x) = x^{p^{k-1}(p-1)} + x^{p^{k-1}(p-2)} + \ldots + x^{p^{k-1}\cdot 1} + 1.$$

D. Indukcja ze względu na k. Dla k=1,2 już wiemy, że tak jest. Załóżmy, że to jest prawdą dla pewnego $k \geqslant 1$. Wtedy dla $k+1$ mamy

$$x^{p^{k+1}} - 1 = (x^{p^k})^p - 1 = (x^{p^k} - 1)(x^{p^k(p-1)} + x^{p^k(p-2)} + \ldots + x^{p^k} + 1).$$

Z drugiej strony (ma mocy 12.4.2) mamy:

$$x^{p^{k+1}} - 1 = (x^{p^k})^p - 1 = \underbrace{\Phi_1(x)\Phi_p(x)\Phi_{p^2}(x)\ldots\Phi_{p^k}(x)}_{x^{p^k}-1}\Phi_{p^{k+1}}(x) = (x^{p^k} - 1)\Phi_{p^{k+1}}(x).$$

Zatem $\Phi_{p^{k+1}}(x) = x^{p^k(p-1)} + x^{p^k(p-2)} + \ldots + x^{p^k} + 1$. ⊠

12.8.3. *Jeżeli p jest liczbą pierwszą i $k \geqslant 0$, to*

$$\Phi_{p^{k+1}}(x) = \Phi_p(x^{p^k}). \qquad \text{(Wynika z 12.8.2).}$$

12.8.4. $\Phi_{2^{k+1}} = x^{2^k} + 1.$ (Jest to szczególny przypadek faktu 12.8.3).

12.8.5. *Jeśli $s = i + j$, to $\Phi_{p^s}(x) = \Phi_{p^i}(x^{p^j})$.*

D. $\Phi_{p^s}(x) = \sum_{k=0}^{p-1} x^{kp^{s-1}} = \sum_{k=0}^{p-1} (x^{p^j})^{kp^{i-1}} = \Phi_{p^i}(x^{p^j})$. ⊠

12.8.6. *Jeżeli p i q są różnymi liczbami pierwszymi, to*

$$\Phi_{p^iq^j}(x) = \Phi_{pq}(x^{p^{i-1}q^{j-1}}),$$

dla $i \geqslant 1$, $j \geqslant 1$.

12.8.7. *Jeżeli $p_1, p_2, \ldots, p_s$ są parami różnymi liczbami pierwszymi, to*

$$\Phi_{p_1^{r_1}p_2^{r_2}\cdots p_s^{r_s}}(x) = \Phi_{p_1p_2\cdots p_s}\left(x^{p_1^{r_1-1}p_2^{r_2-1}\cdots p_s^{r_s-1}}\right).$$

12.8.8. *Niech $r(n)$ oznacza iloczyn wszystkich liczb pierwszych dzielących liczbę naturalną n. Zachodzi zawsze równość:*

$$\Phi_n(x) = \Phi_{r(n)}(x^{n/r(n)}).$$

Jest to inne wysłowienie faktu 12.8.7.

12.8.9. *Jeżeli liczby m i n są względnie pierwsze, to*

$$\Phi_m(x^n) = \prod_{d|n} \Phi_{md}(x). \quad \text{([ArB]).}$$

D. $\Phi_m(x) = \prod\limits_{\alpha\in U_m}(x-\alpha^n)$. Wobec tego:

$$\begin{aligned}\Phi_m(x^n) &= \prod_{\alpha\in U_m}(x^n-\alpha^n) = \prod_{\alpha\in U_m}\prod_{\gamma\in G_n}(x-\alpha\cdot\gamma) = \prod_{d|n}\prod_{\alpha\in U_m}\prod_{\beta\in U_d}(x-\alpha\beta)\\ &= \prod_{d|n}\prod_{(\alpha,\beta)\in U_m\times U_d}(x-\alpha\beta) = \prod_{d|n}\prod_{\delta\in U_{md}}(x-\delta) = \prod_{d|n}\Phi_{md}(x). \ \boxtimes\end{aligned}$$

12.8.10. *Jeżeli p jest liczbą pierwszą i m liczbą naturalną taką, że $p \nmid m$, to*

$$\Phi_{mp}(x) = \frac{\Phi_m(x^p)}{\Phi_m(x)}. \quad \text{([ArB]).}$$

D. Korzystając z 12.8.9 dla $n = p$ mamy: $\Phi_m(x^p) = \Phi_{m\cdot 1}(x)\cdot\Phi_{mp}(x)$ i stąd wynika teza. $\boxtimes$

Następne stwierdzenia dotyczą wielomianów cyklotomicznych o numerach parzystych.

12.8.11. *Jeżeli $n \geqslant 3$ jest liczbą nieparzystą, to $\Phi_{2n}(x) = \Phi_n(-x)$.* ([ArB]).

D. Indukcja ze względu na n. Dla $n = 3$ mamy: $\Phi_6(x) = x^2 - x + 1 = \Phi_3(-x)$. Załóżmy, że to jest prawdą dla wszystkich liczb nieparzystych (większych od 1) mniejszych od n. Wtedy

$$x^{2n}-1 = \prod_{e|2n}\Phi_e(x) = \prod_{d|n}\Phi_d(x)\cdot\prod_{d|n}\Phi_{2d}(x) = \prod_{d|n}\Phi_d(x)\cdot\prod_{\substack{d|n\\1<d<n}}\Phi_{2d}(x)\cdot\Phi_{2n}(x)\cdot\Phi_2(x).$$

Z drugiej strony:

$$\begin{aligned}x^{2n}-1 &= (x^n-1)(x^n+1) = -(x^n-1)\Big((-x)^n-1\Big)\\ &= -\prod_{d|n}\Phi_d(x)\cdot\prod_{\substack{d|n\\1<d<n}}\Phi_d(-x)\cdot\Phi_n(-x)\cdot\Phi_1(-x).\end{aligned}$$

Porównajmy teraz powyższe dwie równości. Z założenia indukcyjnego dla nieparzystych d takich, że $3 \leqslant d < n$, $d \mid n$, mamy $\Phi_{2d}(x) = \Phi_d(-x)$ oraz

$$\Phi_2(x) = x + 1 = -\big((-x) - 1\big) = -\Phi_1(-x).$$

Porównując mamy: $\Phi_{2n}(x) = \Phi_n(-x)$. $\boxtimes$

12.8.12. *Jeżeli $p \geqslant 3$ jest liczbą pierwszą, to* $\Phi_{4p}(x) = \Phi_p(-x^2)$. ([ArB]).

D. Na mocy twierdzenia 12.4.2 mamy: że

$$x^{4p} - 1 = \Phi_1(x) \cdot \Phi_2(x) \cdot \Phi_4(x) \cdot \Phi_p(x) \cdot \Phi_{2p}(x) \cdot \Phi_{4p}(x).$$

Z drugiej strony wiemy, że:

$$\begin{aligned} x^{4p} - 1 &= \Big((x^p)^2 - 1\Big)\Big((x^p)^2 + 1\Big) \\ &= (x^p - 1)(x^p + 1)\Big((x^2)^p + 1\Big) \\ &= \Phi_1(x) \cdot \Phi_p(x) \cdot \Phi_2(x) \cdot \Phi_p(-x) \cdot \Phi_2(x^2) \cdot \Phi_p(-x^2). \end{aligned}$$

Z 12.8.11 wiemy, że zachodzi równość $\Phi_{2p}(x) = \Phi_p(-x)$. Ponadto wiemy, że $\Phi_2(x^2) = x^2 + 1 = \Phi_4(x)$. Porównując strony napisanych powyżej równości otrzymujemy tezę. ☒

12.8.13. *Jeżeli $p \geqslant 3$ jest liczbą pierwszą, to*

$$\Phi_{8p}(x) = \Phi_p(-x^4). \qquad \text{([ArB]).}$$

D. Wiemy z 12.4.2, że

$$x^{8p} - 1 = \Phi_1(x) \cdot \Phi_2(x) \cdot \Phi_4(x) \cdot \Phi_8(x) \cdot \Phi_p(x) \cdot \Phi_{2p}(x) \cdot \Phi_{4p}(x) \cdot \Phi_{8p}(x).$$

Z drugiej strony wiemy, że:

$$\begin{aligned} x^{8p} - 1 &= (x^{4p} - 1)\Big((x^4)^p + 1\Big) \\ &= \Phi_1(x) \cdot \Phi_2(x) \cdot \Phi_4(x) \cdot \Phi_p(x) \cdot \Phi_{2p}(x) \cdot \Phi_{4p}(x) \cdot \Phi_2(x^4) \cdot \Phi_p(-x^4). \end{aligned}$$

Z 12.8.3 wiemy, że $\Phi_8(x) = \Phi_2(x^4)$. Zatem $\Phi_{8p}(x) = \Phi_p(-x^4)$. ☒

12.8.14. *Jeżeli $p \geqslant 3$ jest liczbą pierwszą, to*

$$\Phi_{2^k p}(x) = \Phi_p(-x^{2^{k-1}}).$$

12.8.15. *Jeżeli p i q są różnymi liczbami pierwszymi nieparzystymi, to*

$$\Phi_{4pq}(x) = \Phi_{pq}(-x^2).$$

D. Wiemy z 12.4.2, że

$$x^{4pq} - 1 = \Phi_1(x) \cdot \Phi_2(x) \cdot \Phi_4(x) \cdot \Phi_p(x) \cdot \Phi_{2p}(x) \cdot \Phi_{4p}(x) \cdot \Phi_q(x) \cdot \Phi_{2q}(x) \cdot \Phi_{4q}(x) \cdot \Phi_{pq}(x) \cdot \Phi_{2pq}(x) \cdot \Phi_{4pq}(x).$$

Z drugiej strony wiemy, że:

$$\begin{aligned} x^{4pq} - 1 &= (x^{2pq} - 1)(x^{2pq} + 1) \\ &= \Phi_1(x) \cdot \Phi_2(x) \cdot \Phi_p(x) \cdot \Phi_{2p}(x) \cdot \Phi_q(x) \cdot \Phi_{2q}(x) \cdot \Phi_{pq}(x) \cdot \Phi_{2pq}(x) \cdot (x^{2pq} + 1). \end{aligned}$$

Porównując stronami powyższe równości otrzymujemy równość:

$$\Phi_4(x) \cdot \Phi_{4p}(x) \cdot \Phi_{4q}(x) \cdot \Phi_{4pq}(x) = x^{2pq} + 1.$$

Następnie korzystając z 12.8.12 otrzymujemy, że:

$$\begin{aligned} (x^2 + 1) \cdot \Phi_p(-x^2) \cdot \Phi_q(-x^2) \cdot \Phi_{4pq}(x) &= x^{2pq} + 1 \\ &= -\Big((-x^2)^{pq} - 1\Big) \\ &= -\Phi_1(-x^2) \cdot \Phi_p(-x^2) \cdot \Phi_q(-x^2) \cdot \Phi_{pq}(-x^2). \end{aligned}$$

Wiemy jednak, że

$$-\Phi_1(-x^2) = -(-x^2 - 1) = x^2 + 1.$$

Zatem $\Phi_{4pq}(x) = \Phi_{pq}(-x^2)$. ☒

Teraz przedstawiamy wielomiany cyklotomiczne o numerach podzielnych przez 3.

12.8.16. *Jeżeli p i q są takimi liczbami pierwszymi, że $p > q > 3$, to*

$$\Phi_{3p}(x) - \Phi_{3q}(x) = (x^p - x^q)\frac{x^p + x^q + 1}{x^2 + x + 1}.$$

D.
$$\begin{aligned}\Phi_{3p}(x) - \Phi_{3q}(x) &= \frac{\Phi_3(x^p)}{\Phi_3(x)} - \frac{\Phi_3(x^q)}{\Phi_3(x)} \\ &= \frac{1}{x^2+x+1}\Big[(x^{2p} + x^p + 1) - (x^{2q} + x^q + 1)\Big] \\ &= \frac{1}{x^2+x+1}(x^{2p} - x^{2q} + x^p - x^q) \\ &= \frac{1}{x^2+x+1}\Big[(x^p - x^q)(x^p + x^q) + (x^p - x^q)\Big] \\ &= \frac{1}{x^2+x+1}(x^p - x^q)(x^p + x^q + 1). \boxtimes\end{aligned}$$

12.8.17. *Jeżeli p i q są takimi liczbami pierwszymi, że $p > q > 3$, to wielomian*

$$(x^p - x^q)(x^p + x^q + 1)$$

jest podzielny w $\mathbb{Z}[x]$ przez wielomian $x^2 + x + 1$.

D. Wynika z 12.8.17, gdyż wiemy, że

$$\Phi_{3p} - \Phi_{3q}$$

jest wielomianem należącym do pierścienia $\mathbb{Z}[x]$. Mamy zatem w $\mathbb{Z}[x]$ równość

$$(x^2 + x + 1)(\Phi_{3p}(x) - \Phi_{3q}(x)) = (x^p - x^q)(x^p + x^q + 1). \boxtimes$$

U. Wielomiany postaci $x^p - x^q$ (gdzie p i q są liczbami pierwszymi takimi, że $p > q > 3$) i $x^2 + x + 1$ nie muszą być względnie pierwsze. Dla przykładu

$$x^{29} - x^{23} = x^{23}(x^6 - 1) = x^{23}(x^3 - 1)(x^3 + 1) = x^{23}(x - 1)(x^3 + 1)(x^2 + x + 1),$$

czyli tutaj $x^2 + x + 1$ dzieli $x^{29} - x^{23}$. $\boxtimes$

12.8.18. *Jeżeli p i q są takimi liczbami pierwszymi, że $p > q > 3$, to wielomian*

$$\Phi_{3p}(x) - \Phi_{3q}(x)$$

jest podzielny przez x^q.

12.8.19. *Jeżeli p i q są takimi liczbami pierwszymi, że $p > q > 3$, to wielomian*

$$\Phi_{3p}(x) - \Phi_{3q}(x)$$

jest podzielny przez wielomian $x^q(x - 1)(x + 1)$.

12.8.20. *Jeżeli p i q są takimi liczbami pierwszymi, że $p > q > 3$ oraz $p - q = 6$, to*

$$\Phi_{3p}(x) - \Phi_{3q}(x) = (x - 1)(x + 1)(x^2 - x + 1)(x^p + x^q + 1)x^q.$$

12.8.21. *Jeżeli p i q są takimi liczbami pierwszymi, że $p > q > 3$ oraz $p - q = 4$, to wielomian*

$$\Phi_{3p}(x) - \Phi_{3q}(x)$$

jest podzielny przez wielomian $x^q(x^4 - 1) = x^q(x - 1)(x + 1)(x^2 + 1)$.

oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

12.9 Współczynniki wielomianów cyklotomicznych

oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

Niech

$$\Phi_n(x) = c_{\varphi(n)}x^{\varphi(n)} + c_{\varphi(n)-1}x^{\varphi(n)-1} + \cdots + c_2x^2 + c_1x^1 + c_0.$$

Wiemy, że liczby $c_0, c_1, \ldots, c_{\varphi(n)}$ są całkowite.

12.9.1. *Jeśli $n \geqslant 2$, to $c_k = c_{\varphi(n)-k}$ dla wszystkich $k \in \{0, 1, \ldots, \varphi(n)\}$.*

D. Wynika to z równości $\Psi_n(x, y) = \Psi_n(y, x)$ (patrz 12.7.2). ⊠

12.9.2. *Wyrazem wolnym wielomianu $\Phi_1(x)$ jest -1. Wyraz wolny każdego wielomianu $\Phi_n(x)$, gdzie $n \geqslant 2$, jest równy 1.*

D. (Sposób I). Jest to szczególny przypadek faktu 12.9.1, gdyż dla $n \geqslant 2$ mamy: $c_0 = c_{\varphi(n)-0} = c_{\varphi(n)} = 1$.

(Sposób II). Wyrazem wolnym wielomianu $\Phi_2(x) = x + 1$ jest oczywiście 1. Załóżmy, że $n \geqslant 3$ i niech $\omega_1, \ldots, \omega_{\varphi(n)}$ będą wszystkimi pierwotnymi pierwiastkami n-tego stopnia z jedynki. Niech a oznacza wyraz wolny wielomianu $\Phi_n(x)$. Mamy wtedy

$$a = (-1)^{\varphi(n)}\omega_1 \cdots \omega_{\varphi(n)}.$$

Wiadomo, że jeśli $n \geqslant 3$, to $\varphi(n)$ jest liczbą parzystą. Zatem $a = \omega_1 \cdots \omega_{\varphi(n)}$.

Jeśli ε jest pierwotnym pierwiastkiem n-tego stopnia z jedynki, to liczba $\frac{1}{\varepsilon}$ również jest pierwotnym pierwiastkiem n-tego stopnia z jedynki. Ponadto, jeśli $n > 2$, to $\varepsilon \neq \frac{1}{\varepsilon}$. Zatem zbiór wszystkich pierwotnych pierwiastków n-tego stopnia z jedynki można rozbić na parami rozłączne dwuelementowe zbiory postaci $\{\varepsilon, \frac{1}{\varepsilon}\}$. Iloczyn wszystkich takich pierwiastków jest więc równy 1, tzn. $a = 1$. ⊠

12.9.3. *Niech $n \geqslant 2$. Rozpatrzmy sumę wszystkich współczynników wielomianu $\Phi_n(x)$. Suma ta jest oczywiście równa $\Phi_n(1)$. Jeśli n nie jest potęgą liczby pierwszej, to*

$$\Phi_n(1) = 1.$$

W przeciwnym przypadku, jeśli $n = p^s$, $p \in \mathbb{P}$, $s \geqslant 1$, to

$$\Phi_n(1) = p.$$

D. (K. Motose). Dla $n = p^s$ fakt ten wynika z równości

$$\Phi_{p^s} = x^{p^{s-1}(p-1)} + x^{p^{s-1}(p-2)} + \cdots + 1$$

(patrz 12.8.2). Załóżmy, że $n \geqslant 2$ nie jest potegą liczby pierwszej. Wtedy $n = p^s m$, gdzie p jest pewną liczbą pierwszą i $m \geqslant 2$, $p \nmid m$. Ponieważ

$$\Phi_{mp^s}(x) = \frac{\Phi_m(x^{p^s})}{\Phi_m(x^{p^{s-1}})}$$

oraz $\Phi_m(1) \neq 0$ (gdyż $m \neq 1$), więc $\Phi_n(1) = \dfrac{\Phi_m(1)}{\Phi_m(1)} = 1$. ⊠

12.9.4. *Jeśli $n \geqslant 3$ jest liczbą nieparzystą, to $\Phi_n(-1) = 1$.* ([Mon] 6(111)(2004) 531-533).

12.9.5. *Jeżeli $n \in \mathbb{N}$ jest dowolną potęgą liczby pierwszej, wówczas wszystkie współczynniki n-tego wielomianu cyklotomicznego są nieujemne.*

D. Wynika to z równości $\Phi_{p^s} = x^{p^{s-1}(p-1)} + x^{p^{s-1}(p-2)} + \cdots + 1$ (patrz 12.8.2). ⊠

12.9.6. *Wszystkie współczynniki wielomianu $\Phi_n(x)$ są nieujemne wtedy i tylko wtedy, gdy n jest potęgą liczby pierwszej.* ([Mon] 73(5)(1966) E1769).

12.9.7. *Niech $q > p$ będą liczbami pierwszymi i niech r, s będą nieujemnymi liczbami całkowitymi takimi jak w* 12.10.3. *Wówczas środkowy współczynnik wielomianu $\Phi_{pq}(x)$ jest równy $(-1)^r$.* ([Mon] 103(7)(1996) 562-564, wynika z 12.10.4).

12.9.8 (Dresden 2004)**.** *Dla $n \geqslant 3$ środkowy współczynnik wielomianu $\Phi_n(x)$ jest albo równy zero (kiedy n jest potęgą dwójki) albo jest liczbą nieparzystą.* ([Mon] 6(111)(2004)).

12.9.9. *Niech $m(n)$ oznacza środkowy współczynnik wielomianu $\Phi_n(x)$. Kilka przykładów:*

$$m(385 = 5 \cdot 7 \cdot 11) = -3,$$
$$m(4785 = 3 \cdot 5 \cdot 11 \cdot 29) = 5,$$
$$m(7735 = 5 \cdot 7 \cdot 13 \cdot 17) = -7,$$
$$m(11305 = 5 \cdot 7 \cdot 17 \cdot 19) = 19.$$ (J. Suzuki 1987).

12.9.10 (I. Schur)**.** *Niech $b \in \mathbb{N}$. Istnieje wielomian cyklotomiczny, którego co najmniej jeden współczynnik ma wartość bezwzględną większą od b.* ([Fila] s.103).

★ G. P. Dresden, *On the middle coefficient of a cyclotomic polynomial*, [Mon] 6(111)(2004) 531 - 533.

E. Lehmer, *On the magnitude of coefficients of the cyclotomic polynomials*, [Bams] 42(1936) 389-392.

J. Suzuki, *On coefficients of cyclotomic polynomials*, [Pjap] 63(1987) 279-280.

12.10 Współczynniki wielomianu $\Phi_{pq}(x)$

Jeśli p i q są różnymi liczbami pierwszymi, to (patrz 12.4.8)

$$\Phi_{pq}(x) = \frac{(1 - x^{pq})(1 - x)}{(1 - x^p)(1 - x^q)}.$$

Jest to wielomian stopnia $\varphi(pq) = (p - 1)(q - 1)$.

12.10.1 (Migotti 1883, Bang 1895)**.** *Wszystkie współczynniki wielomianu*

$$\Phi_{pq}(x),$$

gdzie p i q są liczbami pierwszymi, należą do zbioru $\{-1, 0, 1\}$.

([Bang], [Mon] 73(9)(1966), 103(7)(1996)).

Przedstawimy teraz dokładniejsze opisy współczynników wielomianów postaci Φ_{pq}. Opisy te pochodzą głównie z artykułów z czasopisma [Mon].

12.10.2 (Sister Marion Beiter 1964)**.** *Niech $q > p$ będą liczbami pierwszymi i niech*

$$\Phi_{pq}(x) = \sum c_k x^k.$$

Wtedy dla każdego $k = 0, 1, \ldots, \varphi(pq)$ zachodzi równość

$$c_k = \begin{cases} (-1)^\delta, & \text{jeśli } k \text{ można jednoznacznie przedstawić w postaci } k = \alpha q + \beta p + \delta, \\ 0, & \text{w przeciwnym wypadku,} \end{cases}$$

gdzie α, β są nieujemnymi liczbami całkowitymi oraz $\delta = 0$ lub 1. ([Mon] 71(1964) 769-770).

Do przedstawienia następnych charakteryzacji współczynników wielomianu $\Phi_{pq}(x)$ potrzebny będzie następujący fakt. Jeśli a i b są względnie pierwszymi liczbami naturalnymi, to każdą liczbę naturalną n, większą od $ab - a - b$, można przedstawić w postaci $n = xa + yb$, gdzie x i y są nieujemnymi liczbami całkowitymi. Dowód tego faktu można znaleźć np. w [Nar03] s.34 (jest również w [N-6]). Korzystając z tego, łatwo dowodzi się następujący lemat.

12.10.3. *Jeśli $q \neq p$ są liczbami pierwszymi, to istnieją jednoznacznie wyznaczone takie nieujemne liczby całkowite r, s, że $(p-1)(q-1) = rp + sq$. Ponadto:*

(1) $0 \leqslant r \leqslant q-2$, $0 \leqslant s \leqslant p-2$;

(2) $r = u - 1$, $s = v - 1$, *gdzie* $u \in \{1, 2, \ldots, q-1\}$, $v \in \{1, 2, \ldots, p-1\}$ *są takimi liczbami naturalnymi, że* $up \equiv 1 \pmod{q}$ *oraz* $vq \equiv 1 \pmod{p}$.

12.10.4 (Lam, Leung 1996)**.** *Niech $q > p$ będą liczbami pierwszymi i niech r, s będą nieujemnymi liczbami całkowitymi takimi jak w* 12.10.3. *Wówczas wszystkie współczynniki wielomianu $\Phi_{pq}(x) = \sum c_k x^k$ należą do zbioru $\{-1, 0, 1\}$. Dokładniej:*

(1) $c_k = 1$ *wtedy i tylko wtedy, gdy $k = ip + jq$, gdzie $i \in \{0, 1, \ldots, r\}$, $j \in \{0, 1, \ldots, s\}$;*

(2) $c_k = -1$ *wtedy i tylko wtedy, gdy $k = ip + jq - pq$, gdzie $i \in \{r+1, r+2, \ldots, q-1\}$, $j \in \{s+1, s+2, \ldots, p-1\}$;*

(3) $c_k = 0$ *w pozostałych przypadkach.* ([Mon] 103(7)(1996) 562-564).

Wprowadzamy następujące oznaczenia. Przez $a(p, q)$ oznaczać będziemy liczbę wszystkich współczynników równych 1 wielomianu $\Phi_{pq}(x)$. Podobnie przez $b(p, q)$ i $c(p, q)$ oznaczać będziemy liczby współczynników równych odpowiednio -1 i 0 wielomianu $\Phi_{pq}(x)$. Dla przykładu, jeśli $p = 3$ i $q = 5$, to

$$\Phi_{15} = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$$

i mamy: $a(3, 5) = 4$, $b(3, 5) = 3$ oraz $c(3, 5) = 2$.

12.10.5. $b(p, q) = a(p, q) - 1$. ([Mon] 73(9)(1966), 103(7)(1996)).

D. Wynika to natychmiast z tego, że wszystkie współczynniki wielomianu $\Phi_{pq}(x)$ należą do zbioru $\{-1, 0, 1\}$ oraz z tego, że

$$\Phi_{pq}(1) = 1$$

(patrz 12.10.1 i 12.9.3). Łatwo to również wywnioskować z faktu 12.10.7. ⊠

12.10.6 (Carlitz 1966)**.** *Niech $q > p$ będą liczbami pierwszymi i niech $w \in \{1, 2, \ldots, p-1\}$ będzie jedyną liczbą naturalną taką, że $wq \equiv -1 \pmod{p}$. Wtedy*

$$a(p, q) = \frac{1}{p}(p - w)(wq + 1).$$

([Mon] 73(9)(1966)).

12.10.7 (Lam, Leung 1996)**.** *Niech $q > p$ będą liczbami pierwszymi i niech r, s będą nieujemnymi liczbami całkowitymi takimi jak w* 12.10.3*. Zachodzą równości:*

(1) $a(p, q) = (r + 1)(s + 1)$,

(2) $b(p, q) = (p - s - 1)(q - r - 1)$,

(3) $c(p, q) = 2 + (p - 1)(q - 1) - 2(r + 1)(s + 1)$. ([Mon] 103(7)(1996), wynika to z 12.10.4).

12.10.8 (Lenstra 1978)**.** *Niech $q > p$ będą liczbami pierwszymi.*
Niech $u \in \{1, 2, \ldots, q-1\}$, $v \in \{1, 2, \ldots, p-1\}$ będą jedynymi takimi liczbami naturalnymi, że $up \equiv 1 \pmod{q}$ i $vq \equiv 1 \pmod{p}$. Wtedy

$$a(p, q) = uv, \qquad b(p, q) = uv - 1.$$

([Mon] 103(7)(1996)).

12.10.9 (Carlitz 1966)**.** *Z faktu* 12.10.6 *łatwo wywnioskować następujące równości.*

(1) $a(3, 3k + 1) = 2k + 1$, $a(3, 3k + 2) = 2k + 2$.

(2) $a(5, 5k+1) = 4k+1$, $a(5, 5k+2) = 6k+3$, $a(5, 5k+3) = 6k+4$, $a(5, 5k+4) = 4k+4$.

(3) $a(p, kp + 1) = k(p - 1) + 1$, $a(p, pk + p - 1) = k(p - 1) + p - 1$. ([Mon] 73(9)(1966)).

12.10.10 (Zeitlin 1968)**.** *Niech $q > p$ bądą liczbami pierwszymi i niech*

$$\Phi_{pq}(x) = \sum_{k=0}^{N} c_k x^k,$$

gdzie $N = \varphi(pq) = (p - 1)(q - 1)$. Przyjmujemy, że $c_k = 0$ dla $k > N$. Zachodzą wówczas następujące równości.

(1) $c_k = \sum_{i=0}^{2k} (-1)^i c_i c_{2k-i}$, *dla* $k = 0, 1, \ldots, N$;

(2) $\sum_{i=0}^{N-1} (-1)^i c_i c_{i+1} = 0$;

(3) $\sum_{i=0}^{N/2} c_{2i} = 1$; $\sum_{i=1}^{N/2} c_{2i-1} = 0$;

(4) $\sum_{i=1}^{N} ic_i = \frac{1}{2}N = \sum_{i=1}^{N}(-1)^i ic_i$;

(5) $\sum_{i=1}^{N}(-1)^i ic_i^2 = \frac{1}{2}Nc_{N/2}$;

(6) $\sum_{i=1}^{N} i^2c_i = \frac{1}{6}N(N+pq+1)$, $\sum_{i=1}^{N}(-1)^i i^2c_i = \frac{1}{2}N(pq+1)$;

(7) $\sum_{i=1}^{N} i^3c_i = \frac{1}{4}N^2(pq+1)$, $\sum_{i=1}^{N}(-1)^i i^3c_i = \frac{1}{4}N^2(3pq+3-N)$. ([Zeit]).

★ M. Beiter, *The midterm coefficient of the cyclotomic polynomial $F_{pq}(x)$*, [Mon] 71(1964) 769-770.

M. Beiter, *Magnitude of the coefficients of the cyclotomic polynomial $F_{pq}(x)$*, [Mon] 75(1968) 370-372.

L. Carlitz, *The number of terms in the cyclotomic polyn. $F_{pq}(x)$*, [Mon] 73(9)(1966) 979-981.

T. Y. Lam, K. H. Leung, *On the cyclotomic polynomial $\Phi_{pq}(x)$*, [Mon] 103(7)(1996) 562-564.

H. Lenstra, *Vanishing sums of roots of unity*, Proc. Bicentennial Congress Wiskunding Genootschap, Vrije Univ. Amsterdam, 1978, 249-268.

A. Migotti, *Zur Theorie der Kreisteilungsgleichung*, S.-B. der Math.-Naturwiss. Classe der Kaiser. Akad. der Wiss., Wien 87(1983) 7-14.

12.11 Współczynniki wielomianów $\Phi_{pqr}(x)$ i $\Phi_{pqrs}(x)$

12.11.1. *Patrząc na tablice wielomianów cyklotomicznych mogłoby się wydawać, że wszystkie niezerowe współczynniki wielomianów cyklotomicznych są równe ± 1. Nie jest to jednak prawdą bowiem:*

$$\begin{aligned}\Phi_{105}(x) \;=\; & 1+x+x^2-x^5-x^6\underline{-2}x^7-x^8-x^9+x^{12}+x^{13}+x^{14}+x^{15}+x^{16}+x^{17}\\ & -x^{20}-x^{22}-x^{24}-x^{28}+x^{31}+x^{32}+x^{33}+x^{34}+x^{35}\\ & +x^{36}-x^{39}-x^{40}\underline{-2}x^{41}-x^{42}-x^{43}+x^{46}+x^{47}+x^{48}.\end{aligned}$$

12.11.2. *Niech $r > q > p$ będą liczbami pierwszymi i niech*

$$\Phi_{pqr}(x) = \sum_{k=0}^{N} c_k x^k,$$

gdzie $N = \varphi(pqr) = (p-1)(q-1)(r-1)$.
Oznaczmy przez m największą z liczb $|c_0|,\ |c_1|,\ \ldots,\ |c_N|$. Wtedy:

(1) $m \leqslant p-1$, ([Bang] 1895);

(2) *jeśli $p = 5$, to $m \leqslant 3$;*

(3) *jeśli $p = 7$ i $m = 6$, to $q \equiv \pm 3 \pmod 7$ oraz $r \equiv \pm 3 \pmod 7$;*

(4) *jeśli $p \geqslant 5$ i $m = p-1$, to liczby r i s nie przystają do ± 1 modulo p.*

([Bloo]).

12.11.3 (Zeitlin 1968)**.** *Niech $r > q > p$ będą liczbami pierwszymi i niech*

$$\Phi_{pqr}(x) = \sum_{k=0}^{N} c_k x^k,$$

gdzie $N = \varphi(pqr) = (p-1)(q-1)(r-1)$. Oznaczmy $M = pqr + p + q + r$. Zachodzą wówczas następujące równości.

(1) $\displaystyle\sum_{i=1}^{N} ic_i = \frac{1}{2}N = \sum_{i=1}^{N}(-1)^i ic_i;$

(2) $\displaystyle\sum_{i=1}^{N}(-1)^i ic_i^2 = \frac{1}{2}Nc_{N/2};$

(3) $\displaystyle\sum_{i=1}^{N} i^2c_i = \frac{1}{6}N(N+M),\ \sum_{i=1}^{N}(-1)^i i^2c_i = \frac{1}{2}NM;$

(4) $\displaystyle\sum_{i=1}^{N} i^3c_i = \frac{1}{4}N^2M,\ \sum_{i=1}^{N}(-1)^i i^3c_i = \frac{1}{4}N^2(3M-N).$ ([Zeit]).

12.11.4 (Bloom 1968)**.** *Niech $s > r > q > p$ będą liczbami pierwszymi i niech*

$$\Phi_{pqrs}(x) = \sum_{k=0}^{N} c_k x^k,$$

gdzie $N = \varphi(pqrs) = (p-1)(q-1)(r-1)(s-1)$.
Oznaczmy przez m największą z liczb $|c_0|,\ |c_1|,\ \ldots,\ |c_N|$. Wtedy

$$m \leqslant p(p-1)(pq-1).$$

([Bloo]).

12.11.5 (Zeitlin 1968)**.** *Niech $s > r > q > p$ będą liczbami pierwszymi i niech*

$$\Phi_{pqr}(x) = \sum_{k=0}^{N} c_k x^k,$$

gdzie $N = \varphi(pqrs) = (p-1)(q-1)(r-1)(s-1)$. Zachodzą wówczas następujące równości.

(1) $\displaystyle\sum_{i=1}^{N} ic_i = \frac{1}{2}N = \sum_{i=1}^{N}(-1)^i ic_i;$

(2) $\displaystyle\sum_{i=1}^{N}(-1)^i ic_i^2 = \frac{1}{2}Nc_{N/2}.$ ([Zeit]).

★ M. Beiter, *Magnitude of the coefficients of the cyclotomic polynomial $F_{pq}(x)$*, [Mon] 75(1968) 370-372.

12.12 Liczby naturalne postaci $\Phi_n(a)$

W tym podrozdziale zajmować się będziemy liczbami postaci $\Phi_n(a)$, gdzie a jest liczbą naturalną. Przypomnijmy (patrz 12.5.4), że jeśli $n \geqslant 2$, to dla każdej liczby naturalnej a zachodzi nierówność $\Phi_n(a) \geqslant a$. Stąd w szczególności wynika, że każde takie $\Phi_n(a)$ (dla $n \geqslant 2$ oraz $a \in \mathbb{N}$) jest liczbą naturalną.

Przypadek $a = 1$ jest już nam dobrze znany. Przypomnijmy (patrz 12.9.3), że jeśli $n \geqslant 2$ nie jest potęgą liczby pierwszej, to $\Phi_n(1) = 1$. W przeciwnym przypadku, jeśli $n = p^s$, $p \in \mathbb{P}$, $s \geqslant 1$, to $\Phi_n(1) = p$. W dalszym ciągu zakładać będziemy często, że a jest liczbą naturalną większą od 1.

Spójrzmy na kilka przykładów.

12.12.1. *Liczby postaci* $\Phi_n(2)$ *dla* $1 \leqslant n \leqslant 40$.

n	$\Phi_n(2)$	n	$\Phi_n(2)$	n	$\Phi_n(2)$	n	$\Phi_n(2)$
1	1	11	2047	21	2359	31	2147483647
2	3	12	13	22	683	32	65537
3	7	13	8191	23	8388607	33	599479
4	5	14	43	24	241	34	43691
5	31	15	151	25	1082401	35	8727391
6	3	16	257	26	2731	36	4033
7	127	17	131071	27	262657	37	137438953471
8	17	18	57	28	3277	38	174763
9	73	19	524287	29	536870911	39	9588151
10	11	20	205	30	331	40	61681

W prawych kolumnach mamy dokładnie 27 *liczb pierwszych. W pierwszej tabelce oprócz* $\Phi_1(2) = 1$ *występują same liczby pierwsze. Następna liczba,* $\Phi_{11}(2) = 2047 = 23 \cdot 89$*, już nie jest liczbą pierwszą. Istnieją dokładnie* 44 *liczby pierwsze postaci* $\Phi_n(2)$*, gdzie* $1 \leqslant n \leqslant 100$*. Jeśli natomiast* $1 \leqslant n \leqslant 1000$*, to takich liczb pierwszych jest dokładnie* 99. (Maple).

12.12.2. *Liczby postaci* $\Phi_n(3)$ *dla* $1 \leqslant n \leqslant 40$.

n	$\Phi_n(3)$	n	$\Phi_n(3)$	n	$\Phi_n(3)$	n	$\Phi_n(3)$
1	2	11	88573	21	368089	31	308836698141973
2	4	12	73	22	44287	32	43046722
3	13	13	797161	23	47071589413	33	2413941289
4	10	14	547	24	6481	34	32285041
5	121	15	4561	25	3501192601	35	189150889201
6	7	16	6562	26	398581	36	530713
7	1093	17	64570081	27	387440173	37	225141952945498681
8	82	18	703	28	478297	38	290565367
9	757	19	581130733	29	34315188682441	39	195528263281
10	61	20	5905	30	8401	40	42521761

W prawych kolumnach mamy dokładnie 16 *liczb pierwszych. Istnieją dokładnie* 23 *liczby pierwsze postaci* $\Phi_n(3)$*, gdzie* $1 \leqslant n \leqslant 100$*. Jeśli natomiast* $1 \leqslant n \leqslant 200$*, to takich liczb pierwszych jest dokładnie* 31. (Maple).

Przypomnijmy, że jeśli $n \neq m$, to wielomiany cyklotomiczne $\Phi_n(x)$, $\Phi_m(x)$ są względnie pierwsze (patrz 12.9.3) w pierścieniu $\mathbb{Z}[x]$. Stąd jednak nie wynika, że jeśli $n \neq m$ oraz $2 \leqslant a \in \mathbb{N}$, to liczby naturalne $\Phi_n(a)$, $\Phi_m(a)$ są również względnie pierwsze. Mamy na przykład $6 \neq 18$ oraz $\operatorname{nwd}(\Phi_6(2),\ \Phi_{18}(2)) = \operatorname{nwd}(6, 57) = 3$. Inny przykład: $2 \neq 4$ oraz $\operatorname{nwd}(\Phi_2(3),\ \Phi_4(3)) = \operatorname{nwd}(4, 10) = 2$

W pewnych jednak przypadkach tę względną pierwszość można uzyskać. Udowodniliśmy (patrz 12.4.7), że jeśli d, n są liczbami naturalnymi takimi, że $d < n$ oraz $d \nmid n$, to istnieją wielomiany o współczynnikach całkowitych $F(x), G(x)$ takie, że

$$1 = F(x)\Phi_d(x) + G(x)\Phi_n(x).$$

Podobnego typu równość zachodzi zachodzi nawet przy słabszym założeniu; wystarczy założyć, że n/d nie jest potęgą liczby pierwszej (patrz twierdzenie 12.4.5). Z tych faktów wynikają natychmiast następujące trzy stwierdzenia zachodzące dla dowolnej liczby naturalnej a (a nawet dla $a \in \mathbb{Z}$).

12.12.3. *Jeśli d, n są liczbami naturalnymi takimi, że $d < n$ oraz $d \nmid n$, to dla dowolnej liczby całkowitej a, liczby $\Phi_d(a),\ \Phi_n(a)$ są względnie pierwsze.*

12.12.4. *Jeśli m, m są względnie pierwszymi liczbami naturalnymi większymi od 1, to to dla dowolnej liczby całkowitej a, liczby $\Phi_n(a),\ \Phi_m(a)$ są względnie pierwsze.*

12.12.5. *Niech $1 < d < m$ będą liczbami naturalnymi. Jeśli istnieje taka liczba całkowita a, że $\operatorname{nwd}(\Phi_d(a),\ \Phi_n(a)) > 1$, to d jest dzielnikiem liczby n.*

Pan Tomasz Ordowski przesłał mi (w maju 2013 roku) dwa interesujące zadania do rozwiązania, dotyczące wielomianów cyklotomicznych. O pierwszym jego zadaniu napisaliśmy na stronie 150 (patrz 12.4.16). Oto drugie zadanie wraz z dowodem.

12.12.6. *Niech $a \geqslant 2$ będzie liczbą naturalną i niech (b_n) będzie ciągiem liczb naturalnych takim, że*

$$b_1 = 1 \quad \textit{oraz} \quad b_{n+1} = \operatorname{nww}\Big(b_n,\ a^n - 1\Big) \quad \textit{dla} \quad n \in \mathbb{N}.$$

Wówczas dla dowolnej liczby naturalnej n zachodzi równość

$$\frac{b_{n+1}}{b_n} = \Phi_n(a).$$

D. Udowodnimy, że dla każdej liczby naturalnej n zachodzi równość

$$(*) \qquad b_n = \prod_{k=1}^{n-1} \Phi_k(a).$$

Indukcja ze względu na n. Dla $n = 1$ jest to oczywiste. Krok indukcyjny:

$$b_{n+1} = [b_n,\ a^n - 1] = \left[\prod_{k=1}^{n-1} \Phi_k(a),\ \prod_{d|n} \Phi_d(a)\right] = [AB,\ A\Phi_n(a)]\,.$$

Wykorzystaliśmy twierdzenie 12.4.2. Tutaj A jest iloczynem wszystkich liczb postaci $\Phi_d(a)$, gdzie $d < n$ oraz $d \mid n$. Natomiast B jest iloczynem wszystkich liczb postaci $\Phi_d(a)$, gdzie $d < n$ oraz $d \nmid n$. Nawiasami kwadratowymi oznaczono najmniejszą wspólną wielokrotność.

Ze stwierdzenia 12.12.3 wynika, że liczby B oraz $\Phi_n(b)$ są względnie pierwsze. Mamy zatem:

$$b_{n+1} = [AB,\ A\Phi_n(a)] = A\,[B,\ \Phi_n(a)] = AB\Phi_n(a) = \left(\prod_{k=1}^{n-1}\Phi_k(a)\right)\cdot\Phi_n(a) = \prod_{k=1}^{n}\Phi_k(a)$$

i to kończy nasz indukcyjny dowód równości $(*)$. Zatem $b_{n+1}/b_n = \Phi_n(a)$. ⊠

oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

12.13 Podzielność liczb $\Phi_n(a)$ przez liczby pierwsze

oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

Jeśli $a, m \in \mathbb{Z}$, $m \geqslant 2$ oraz $\mathrm{nwd}(a, m) = 1$, to przez $\delta_m(a)$ oznaczamy rząd liczby a modulo m, tzn. $\delta_m(a)$ jest najmniejszą liczbą naturalną n taką, że

$$a^n \equiv 1 \pmod{m}.$$

Podstawowe własności liczby $\delta_m(a)$ znajdują się np. w [N-4].

12.13.1. *Niech $p \in \mathbb{P}$, $a \in \mathbb{Z}$, $n \in \mathbb{N}$. Jeśli $p \mid \Phi_n(a)$, to $p \nmid a$.*

D. Wiadomo, że wielomian $\Phi_n(x)$ jest podzielnikiem (w $\mathbb{Z}[x]$) wielomianu $x^n - 1$. Załóżmy, że $p \mid \Phi_n(a)$. Wtedy $p \mid a^n - 1$. Gdyby p dzieliło a, to otrzymalibyśmy sprzeczność: $p \mid 1$. ⊠

12.13.2. *Niech $a \geqslant 2$, $n \geqslant 2$ będą liczbami naturalnymi i niech p będzie liczbą pierwszą. Jeśli $p \mid \Phi_n(a)$, to*

$$n = p^s\delta_p(a),$$

gdzie $s \geqslant 0$ jest pewną liczbą całkowitą. ([Mot1], [Mot5]).

D. Załóżmy, że $p \mid \Phi_n(a)$. Wtedy $p \nmid a$ (patrz 12.13.1), więc można mówić o rzędzie $\delta_p(a)$. Ponieważ $a^n \equiv 1 \pmod{p}$, więc rząd $\delta_p(a)$ jest podzielnikiem liczby n. Zatem $n = p^s t\delta_p(a)$, gdzie $s \geqslant 0$, $t \in \mathbb{N}$, $p \nmid t$. Pokażemy, że $t = 1$.

Przypuśćmy, że $t > 1$. Oznaczmy: $m = p^s\delta_p(a)$. Wtedy $n = mt$, $p \nmid t$. Ponieważ $m \mid n$, więc

$$a^n - 1 = \prod_{d\mid n}\Phi_d(a) = \prod_{d\mid m}\Phi_d(a)\cdot\prod_{d\in A}\Phi_d(a) = (a^m - 1)\prod_{d\in A}\Phi_d(a),$$

gdzie A jest zbiorem tych wszystkich naturalnych podzielników liczby n które nie są podzielnikami liczby m. Zauważmy, że $n \in A$ (gdyż $t > 1$). W iloczynie $\prod\limits_{d\in A}\Phi_d(a)$ występuje więc czynnik $\Phi_n(a)$, który jest podzielny przez p. Oznacza to, że liczba całkowita $\frac{a^n-1}{a^m-1}$ jest podzielna przez p. Przypomnijmy, że $a^m \equiv 1 \pmod{p}$. Modulo p mamy więc:

$$0 \equiv \frac{a^n-1}{a^m-1} = \frac{a^{mt}-1}{a^m-1} = a^{m(t-1)} + a^{m(t-2)} + \cdots + a^m + 1 \equiv \underbrace{1+1\cdots+1}_{t} = t,$$

czyli otrzymaliśmy sprzeczność: $p \mid t$. Zatem $t = 1$ i stąd $n = p^s\delta_p(a)$. ⊠

Zmierzamy teraz do udowodnienia twierdzenia odwrotnego do twierdzenia 12.13.2.

12.13.3. *Niech $p \in \mathbb{P}$, $a \geqslant 2$, $a \in \mathbb{N}$, $p \nmid a$. Wtedy $p \mid \Phi_\delta(a)$, gdzie $\delta = \delta_p(a)$.*

D. Wiemy, że δ jest najmniejszą liczbą naturalną taką, że $p \mid a^\delta - 1$. Wiemy również, że

$$a^\delta - 1 = \prod_{d|\delta} \Phi_d(a).$$

Wśród czynników postaci $\Phi_d(a)$, gdzie $d \mid \delta$, występuje więc czynnik podzielny przez p. Przypuśćmy, że $p \mid \Phi_d(a)$, gdzie $d < \delta$. Wtedy p dzieli $a^d - 1$, gdyż

$$a^d - 1 = \prod_{e|d} \Phi_e(a).$$

Jeśli więc $d < \delta$, to mamy sprzeczność z własnością minimalności liczby δ. Zatem $p \mid \Phi_\delta(a)$. ⊠

12.13.4. *Niech $a \in \mathbb{Z}$, $2 \nmid a$, $s \in \mathbb{N}$. Wtedy $2 \mid \Phi_{2^s}(a)$.*

D. To jest oczywiste, gdyż $\Phi_{2^s}(a) = a^{2^{s-1}} + 1$. ⊠

Zanotujmy następujący dobrze znany fakt (patrz np. [N-8]), który w dalszym ciągu będzie przydatny.

12.13.5. *Niecg $p \geqslant 3$ będzie liczbą pierwszą i niech $b \geqslant 2$ będzie liczbą naturalną taką, że $b \equiv 1 \pmod p$. Niech $w = \dfrac{b^p - 1}{b - 1}$. Wtedy*

$$w \in \mathbb{N}, \quad p \mid w \quad \textit{oraz} \quad p^2 \nmid w.$$

12.13.6. *Niech $a \geqslant 2$, $n \geqslant 2$ będą liczbami naturalnymi i niech p będzie liczbą pierwszą taką, że $p \nmid a$. Jeśli $n = p^s\delta_p(a)$, gdzie $s \geqslant 0$, to $p \mid \Phi_n(a)$.* ([Mot1], [Mot5]).

D. Wykazaliśmy to już w przypadkach, gdy $s = 0$ (patrz 12.13.3) i $p = 2$ (patrz 12.13.4). Zakładamy więc, że $n = p^s\delta_p(a)$, $s \geqslant 1$, $p \geqslant 3$. Oznaczmy:

$$m = p^{s-1}\delta_p(a), \quad b = a^m.$$

Wtedy oczywiście $b \equiv 1 \pmod p$, $b \geqslant 2$ oraz $n = pm$. Z faktu 12.13.5 wynika więc, że liczba $\frac{b^p-1}{b-1}$ jest całkowita i podzielna przez p. Ale

$$\frac{b^p - 1}{b - 1} = \frac{a^n - 1}{a^m - 1},$$

więc liczba $\dfrac{a^n - 1}{a^m - 1}$ jest całkowita i podzielna przez p. Z własności wielomianów cyklotomicznych otrzymujemy:

$$a^n - 1 = \prod_{d|n} \Phi_d(a) = \prod_{d|m} \Phi_d(a) \cdot \prod_{d \in A} \Phi_d(a) = (a^m - 1) \prod_{d \in A} \Phi_d(a),$$

gdzie A jest zbiorem tych wszystkich naturalnych podzielników liczby n, które nie są podzielnikami liczby m. Zatem liczba

$$\prod_{d \in A} \Phi_d(a) = \frac{a^n - 1}{a^m - 1}$$

jest podzielna przez p. Istnieje więc $d_0 \in A$ takie, że $p \mid \Phi_{d_0}(a)$. Jest jasne, że $d_0 = p^s e$, gdzie $s \mid \delta_p(a)$.

Przypuśćmy, że $e < \delta_p(a)$. Ponieważ $p \mid \Phi_{d_0}(a)$ oraz $\Phi_{d_0}(a) \mid a^{d_0} - 1$, więc $a^{d_0} \equiv 1 \pmod p$. Ponadto, z małego twierdzenia Fermata mamy: $a^{p^s} \equiv a^{p^{s-1}} \equiv \cdots \equiv a \pmod p$. Zatem,

$$a^e \equiv a^{p^s e} = a^{d_0} \equiv 1 \pmod p.$$

Jeśli więc $e < \delta_p(a)$, to mamy sprzeczność z minimalnością liczby $\delta_p(a)$. Zatem $e = \delta_p(a)$. Stąd $d_0 = p^s\delta_p(a) = n$ oraz $p \mid \Phi_{d_0}(a) = \Phi_n(a)$. ⊠

12.13.7. *Niech $a \geqslant 2$, $n \geqslant 2$ będą liczbami naturalnymi i niech p będzie liczbą pierwszą. Następujące dwa warunki są równoważne.*

(1) $p \mid \Phi_n(a)$;

(2) $p \nmid a$ *i* $n = p^s\delta_p(a)$, *gdzie* $s \geqslant 0$. ([Mot1], wynika z 12.13.2 i 12.13.6).

12.13.8. *Niech $p \geqslant 3$ będzie liczbą pierwszą i $a \geqslant 2$ liczbą naturalną.*
Jeśli $p \mid n$ i $p \mid \Phi_n(a)$, to $p^2 \nmid \Phi_n(a)$. ([Mot1]).

D. Skoro $p \mid n$, więc $n \geqslant 3$. Ponieważ $p \mid \Phi_n(a)$, więc

$$n = p^s\delta_p(a)$$

(patrz 12.13.2), gdzie $s \geqslant 0$. W naszym przypadku $s \geqslant 1$, gdyż $p \mid n$ i $\delta_p(a) < p$. Niech

$$m = p^{s-1}\delta_p(a) \quad \text{i} \quad b = a^m.$$

Wtedy $n = pm$, $\delta_p(a) \mid m$, $b \geqslant 2$ oraz

$$b \equiv 1 \pmod{p}.$$

Z dowodu twierdzenia 12.13.6 wiemy, że $\Phi_n(a)$ jest podzielnikiem liczby całkowitej

$$\frac{a^n - 1}{a^m - 1},$$

czyli liczby $\dfrac{b^p - 1}{b - 1}$. Liczba $\dfrac{b^p - 1}{b - 1}$ nie jest podzielna przez p^2 (patrz 12.13.5). Zatem $p^2 \nmid \Phi_n(a)$. ⊠

12.13.9. *Niech $p \geqslant 3$ będzie liczbą pierwszą i $a \geqslant 2$ liczbą naturalną. Załóżmy, że $p \mid \Phi_n(a)$. Wtedy $n = p^s\delta_p(a)$, dla pewnej nieujemnej liczby całkowitej s. Jeśli $s \geqslant 1$, to $p^2 \nmid \Phi_n(a)$.* (Wynika z 12.13.2 i 12.13.8).

12.13.10. *Niech $p \geqslant 3$ będzie liczbą pierwszą i $a \geqslant 2$ liczbą naturalną. Jeśli $p^2 \mid \Phi_n(a)$, to $n = \delta_p(a)$.* (Wynika z 12.13.9).

★ Y. Gallot, *Cyclotomic polynomials and prime numbers*, preprint.
J. MacDougall, *Mersenne composities and cyclotomic primes*, preprint.
K. Motose, [Mot2], [Mot3].

12.14 Twierdzenie Hurwitza

12.14.1. *Niech $a \geqslant 1$ i $n \geqslant 2$ będą liczbami naturalnymi. Następujące dwa warunki są równoważne.*

(1) *Liczba $\Phi_{n-1}(a)$ jest podzielna przez n.*

(2) *Liczba n jest pierwsza oraz $\delta_n(a) = n-1$ (tzn. a jest pierwiastkiem pierwotnym modulo n).* ([Mot1]).

D. Dla $a = 1$ jest to oczywiste. Zakładamy, że $a \geqslant 2$.

(1) $\Rightarrow$ (2). Załóżmy, że $n \mid \Phi_{n-1}(a)$ i niech p będzie liczbą pierwszą dzielącą n. Wtedy $p \mid \Phi_{n-1}(a)$ i stąd (patrz 12.13.2) $n-1 = p^s\delta_p(a)$ dla pewnego $s \geqslant 0$. Gdyby s było większe od zera otrzymalibyśmy sprzeczność: $p \mid 1$. Zatem $s = 0$, czyli $n - 1 = \delta_p(a)$. Ponieważ $\delta_p(a) \mid p - 1$, więc $n - 1 \mid p - 1$ i stąd $n \leqslant p \leqslant n$. Zatem $n = p$ jest liczbą pierwszą i $n - 1 = \delta_n(a)$.

(2) $\Rightarrow$ (1) Załóżmy, że $n = p$ jest liczbą pierwszą i $\delta_p(a) = p-1$. Wtedy (patrz 12.13.3) $p \mid \Phi_{p-1}(a)$, czyli $n \mid \Phi_{n-1}(a)$. $\boxtimes$

Z powyższych faktów otrzymujemy następujące twierdzenie Hurwitza.

12.14.2 (Hurwitz)**.** *Niech $n \geqslant 2$. Wtedy n jest liczbą pierwszą wtedy i tylko wtedy, gdy istnieje liczba naturalna a taka, że $n \mid \Phi_{n-1}(a)$.* ([Mon] 61(8)(1954) s.564, wynika z 12.14.1).

★ M. Ward, *Cyclotomy and the converse of Fermat's theorem*, [Mon] 61(8)(1954) 564.

12.15 Twierdzenie Banga o rzędach

W tym i w następnych podrozdziałach przedstawiamy kilka zastosowań wielomianów cyklotomicznych.

Przez $\delta_m(a)$ oznaczamy rząd liczby a modulo m, tzn. $\delta_m(a)$ najmniejszą liczbę naturalną n taką, że

$$a^n \equiv 1 \pmod{m}.$$

To ma sens tylko w przypadku, gdy $\mathrm{nwd}(a, m) = 1$.

12.15.1. *Rozpatrzmy liczbę Mersenne'a $M_s = 2^s - 1$, gdzie $s \geqslant 2$.*
Nie istnieje żadna liczba pierwsza p taka, że $\delta_p(M_s) = 2$. ([Mot1]).

D. Przypuśćmy, że taka liczba pierwsza p istnieje. Wtedy $2 = \delta_p(M_s) \leqslant p - 1$, więc $p \geqslant 3$. Korzystając z 12.13.3 stwierdzamy, że

$$p \mid \Phi_2(M_s) = M_s + 1 = 2^s$$

(gdyż $\Phi_2(x) = x + 1$). Mamy więc sprzeczność: $3 \leqslant p = 2$. $\boxtimes$

12.15.2. *Niech $a \geqslant 2$ będzie liczbą naturalną. Następujące dwa warunki są równoważne.*

(1) *Istnieje liczba pierwsza p taka, że $\delta_p(a) = 2$.*

(2) *Liczba a nie jest liczbą Mersenne'a.*

D. Implikację (1) $\Rightarrow$ (2) już wykazaliśmy (12.15.1). Wykażemy implikację (2) $\Rightarrow$ (1). Załóżmy, że a nie jest liczbą Mersenne'a. Wtedy $a+1$ nie jest potęgą dwójki. Istnieje więc nieparzysta liczba pierwsza p dzieląca $a+1$. Wtedy $a \equiv -1 \pmod p$ i stąd $a^2 \equiv 1 \pmod p$, czyli $\delta_p(a) = 2$. $\boxtimes$

12.15.3. *Nie istnieje żadna liczba pierwsza p taka, że $\delta_p(2) = 6$.* ([Mot1], [Mot5]).

D. Przypuśćmy, że taka liczba pierwsza p istnieje. Wtedy $6 = \delta_p(2) \leqslant p-1$, więc $p \geqslant 7$. Oczywiście $p \nmid 2$. Korzystając z 12.13.3 stwierdzamy, że

$$p \mid \Phi_6(2) = 2^2 - 2 + 1 = 3$$

(gdyż $\Phi_6(x) = x^2 - x + 1$). Mamy więc sprzeczność: $7 \leqslant p \leqslant 3$. $\boxtimes$

12.15.4. *Niech $a \geqslant 2$, $n \geqslant 2$ będą liczbami naturalnymi. Załóżmy, że $p = \Phi_n(a)$ jest liczbą pierwszą i przy tym $p \mid n$. Wtedy*

$$n = 6 \quad \textit{oraz} \quad a = 2$$

(i wtedy $p = 3$). ([Mot5]).

D. Przypuśćmy, że $a \geqslant 3$. Wtedy $p = \Phi_n(a) > (a-1)^{\varphi(n)} \geqslant 2^{\varphi(n)} \geqslant 2^{p-1}$ (skorzystaliśmy z nierówności 12.5.6), czyli $p > 2^{p-1}$, co jest oczywiście sprzecznością.

Zatem $a = 2$. Mamy więc $p = \Phi_n(2)$. Ponieważ $\Phi_n(2)$ dzieli $2^n - 1$, więc p jest nieparzyste, czyli $p \geqslant 3$. Wiemy, na mocy 12.13.2, że $n = p^s\delta$, gdzie $\delta = \delta_p(2)$ oraz $s \geqslant 0$, Ale $p \mid n$, więc $s \geqslant 1$.

Przypuśćmy, że $s \geqslant 2$. Wtedy $p = \Phi_n(2) = \Phi_{p^s\delta}(2) = \Phi_{p\delta}\left(2^{p^{s-1}}\right)$ i mamy sytuację taką samą jak na początku tego dowodu dla

$$a = 2^{p^{s-1}} > 3;$$

otrzymujemy znowu sprzeczność. Zatem $s = 1$.

Mamy więc $n = p\delta$, $p = \Phi_n(2)$. Korzystając jeszcze raz z nierówności 12.5.6 otrzymujemy:

$$p = \Phi_{pm}(2) = \frac{\Phi_m(2^p)}{\Phi_m(2)} > \frac{(2^p-1)^{\varphi(m)}}{(2+1)^{\varphi(m)}} = \left(\frac{2^p-1}{3}\right)^{\varphi(m)} \geqslant \frac{2^p-1}{3},$$

czyli $3p + 1 > 2^p$. Stąd jedynie $p = 3$. Zatem $n = 3\delta_3(2) = 3 \cdot 2 = 6$. $\boxtimes$

12.15.5. *Niech $n \geqslant 3$, $a \geqslant 2$ będą liczbami naturalnymi. Jeśli $\Phi_n(a)$ dzieli n, to $(n, a) = (6, 2)$.* ([Rtk], [Mot5]).

D. Załóżmy, że $\Phi_n(a) \mid n$. Ponieważ $\Phi_n(a) \geqslant a$, więc $\Phi_n(a) \geqslant 2$. Niech p będzie liczbą pierwszą dzielącą $\Phi_n(a)$. Wtedy $n = p^s\delta_p(a)$, $s \geqslant 0$ (patrz 12.13.2). W naszym przypadku $s \geqslant 1$, gdyż $p \mid \Phi_n(a) \mid n$. Oczywiście $\delta_p(a) < p$. Zatem p jest największą liczbą pierwszą dzielącą n. Gdyby jakaś inna liczba pierwsza q dzieliła również $\Phi_n(a)$, to w ten sam sposób pokazalibyśmy, że q jest również największą liczbą pierwszą dzielącą n, czyli $q = p$. Oznacza to, że $\Phi_n(a)$ jest potęgą liczby pierwszej p. Wiemy jednak (patrz 12.13.10), że

$$p^2 \nmid \Phi_n(a).$$

Zatem $\Phi_n(a) = p$ jest liczbą pierwszą i teza wynika z 12.15.4. $\boxtimes$

12.15.6 (Bang 1886)**.** *Niech $n \geqslant 3$, $a \geqslant 2$ będą takimi liczbami naturalnymi, że*

$$(n, a) \neq (6, 2).$$

Istnieje wtedy liczba pierwsza p taka, że $n = \delta_p(a)$. ([BirV], [Rtk], [Mot1], [Mot5]).

D. Przypuśćmy, że taka liczba pierwsza p nie istnieje. Oczywiście $\Phi_n(a) \geqslant a \geqslant 2$. Istnieje zatem liczba pierwsza p dzieląca liczbę $\Phi_n(a)$. Wtedy, na mocy 12.13.2, $n = p^s\delta_p(a)$ gdzie $s \geqslant 0$. Jeśli $s = 0$, to $n = \delta_p(a)$ wbrew temu co założyliśmy. Zatem $s \geqslant 1$. Ale $\delta_p(a) \leqslant p-1$, więc p jest największą liczbą pierwszą dzielącą n. Biorąc inną liczbę pierwszą q dzielącą $\Phi_n(a)$, stwierdzamy w ten sam sposób, że q jest największą liczbą pierwszą dzielącą n. Zatem $\Phi_n(a)$ jest potęgą liczby pierwszej p i przy tym $p \mid n$. Wiemy (patrz 12.13.10), że $p^2 \nmid \Phi_n(a)$. Zatem $\Phi_n(a) = p$ jest liczbą pierwszą dzielącą n. Korzystając z 12.15.4 stwierdzamy, że $(n, a) = (6, 2)$ wbrew temu, że $(n, a) \neq (6, 2)$. ⊠

Z powyższych faktów wynika następujące ogólne twierdzenie.

12.15.7 (Bang 1886)**.** *Niech $n \geqslant 2$, $a \geqslant 2$ będą liczbami naturalnymi. Następujące warunki są równoważne.*

(1) *Istnieje liczba pierwsza p taka, że $n = \delta_p(a)$.*

(2) *Para (n, a) nie jest postaci $(2, 2^s - 1)$ i nie jest równa $(6, 2)$.* ([Mot1]).

12.15.8 (Maple)**.** *Przykłady najmniejszych liczb pierwszych p spełniających równość*

$$n = \delta_p(a),$$

dla danych n, a.

(13) $a = 2$:

$$\begin{array}{lll} 2 = \delta_3(2), & 9 = \delta_{73}(2), & 15 = \delta_{151}(2), \\ 3 = \delta_7(2), & 10 = \delta_{11}(2), & 16 = \delta_{257}(2), \\ 4 = \delta_5(2), & 11 = \delta_{23}(2), & 17 = \delta_{131071}(2), \\ 5 = \delta_{31}(2), & 12 = \delta_{13}(2), & 18 = \delta_{19}(2), \\ 7 = \delta_{127}(2), & 13 = \delta_{8197}(2), & 19 = \delta_{524287}(2), \\ 8 = \delta_{17}(2), & 14 = \delta_{43}(2), & 20 = \delta_{41}(2). \end{array}$$

(14) $a = 3$:

$$\begin{array}{lll} 3 = \delta_{13}(3), & 6 = \delta_7(3), & 10 = \delta_{61}(3), \\ 4 = \delta_5(3), & 7 = \delta_{1093}(3), & 11 = \delta_{23}(3), \\ 5 = \delta_{11}(3), & 8 = \delta_{41}(3), & 12 = \delta_{73}(3). \\ & 9 = \delta_{757}(3), & \end{array}$$

(15) $a = 5$:

$$\begin{array}{lll} 2 = \delta_3(5), & 5 = \delta_{11}(5), & 8 = \delta_{313}(5), \\ 3 = \delta_{31}(5), & 6 = \delta_7(5), & 9 = \delta_{19}(5), \\ 4 = \delta_{13}(5), & 7 = \delta_{19531}(5), & 10 = \delta_{521}(5). \end{array}$$

12.15.9. *Niech $a \geqslant 3$, $n \geqslant 3$, $m \geqslant 3$. Jeśli $\Phi_n(a) = \Phi_m(a)$, to $n = m$.* ([Mot1]).

D. Przypuśćmy, że $n < m$. Z twierdzenia Banga istnieje liczba pierwsza p taka, że $m = \delta_p(a)$. Wtedy oczywiście $p \nmid a$ oraz $p \mid \Phi_m(a)$ (na mocy 12.13.3 lub 12.13.7). Ale $\Phi_m(a) = \Phi_n(a)$, więc $p \mid \Phi_n(a)$. Zatem (na mocy 12.13.2) $n = p^s\delta_p(a)$, gdzie $s \geqslant 0$. Stąd $n = p^s\delta_p(a) \geqslant \delta_p(a) = m$, wbrew temu, że $n < m$. ⊠

★ A. S. Bang, *Taltheoretiske Undersøgelser*, Tidsskrift for Math. 5(1886) 70-80, 130-137.

oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

12.16 Liczby pierwsze w postępach arytmetycznych

oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

Za pomocą wielomianów cyklotomicznych można udowodnić następujący szczególny przypadek twierdzenia Dirichleta o liczbach pierwszych w postępie arytmetycznym. Wspominaliśmy o tym w [N-4].

12.16.1. *Niech $m \in \mathbb{N}$. Liczb pierwszych postaci $mk+1$ jest nieskończenie wiele.*

D. ([Mot1], [Mot5], [N-4]). Ponieważ wiemy, że wszystkich liczb pierwszych jest nieskończenie wiele, więc możemy założyć, że $m \geqslant 3$. Z twierdzenia Banga 12.15.7 wiemy, że istnieje liczba pierwsza p taka, że

$$\delta_p(4) = m.$$

Wtedy $m \leqslant p-1$, więc $p \geqslant 5$. Liczba m jest więc najmniejszą liczbą naturalną taką, że

$$4^m \equiv 1 \pmod{p}.$$

Ponieważ $4^{p-1} \equiv 1 \pmod{p}$ (małe twierdzenie Fermata), więc $m \mid p-1$. Zatem $p-1 = km$ dla pewnego naturalnego k i stąd $p = mk+1$. Istnieje więc co najmniej jedna liczba pierwsza postaci $mk+1$.

Przypuśćmy, że liczb pierwszych postaci $mk+1$ jest tylko skończenie wiele. Niech p będzie największą z nich. Z twierdzenia Banga wynika, że istnieje liczba pierwsza q taka, że

$$\delta_q(4) = pm.$$

Wtedy $pm \mid q-1$, czyli $q = pmt+1$, gdzie $t \in \mathbb{N}$. Liczba pierwsza q jest więc postaci $pm+1$ i $q > p$, gdyż $q = pmt+1$. Otrzymaliśmy sprzeczność z minimalnością liczby pierwszej p. ⊠

Za pomocą wielomianów cyklotomicznych udowodniono:

12.16.2. *Niech $m \geqslant 2$. Najmniejsza liczba pierwsza postaci $mk+1$ jest mniejsza od*

$$\frac{1}{2}(3^m - 1).$$

(J. Sabia, S. Tesauri, 2009).

12.16.3. *Niech $m \geqslant 2$. Najmniejsza liczba pierwsza postaci $mk+1$ jest mniejsza od*

$$2^{\varphi(m)+1}.$$

(R.Thangadurai, A.Vatwani, [Mon] 118(8)(2011) 737-742).

★ R. Thangadurai, A. Vatwani, *The least prime congruent to one modulo n*, [Mon] 118(8)(2011) 737-742.

oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

12.17 Wielomiany podzielne przez $x^2 + x + 1$

oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

W popularnonaukowej literaturze matematycznej często pojawiają się zagadnienia lub zadania dotyczące podzielności wielomianów o współczynnikach całkowitych przez wielomian x^2+x+1. Ten wielomian x^2+x+1 niczym specjalnym się nie wyróżnia. Jest to jednak wielomian cyklotomiczny;

$$x^2 + x + 1 = \Phi_3(x).$$

Sprawdzanie czy dany wielomian $f(x)$, o współczynnikach całkowitych, jest podzielny przez jakiś wielomian cyklotomiczny $\Phi_n(x)$ sprowadza się do zbadania wartości $f(\varepsilon)$, gdzie ε jest pierwiastkiem pierwotnym n-tego stopnia z jedynki. Wyjaśnijmy to dokładniej.

12.17.1. *Niech $n \in \mathbb{N}$ i niech $f(x) \in \mathbb{Z}[x]$. Następujące warunki są równoważne.*

(1) *Wielomian $f(x)$ jest podzielny w $\mathbb{Z}[x]$ przez $\Phi_n(x)$.*

(2) *$f(\varepsilon) = 0$ dla pewnego pierwiastka pierwotnego n-tego stopnia z jedynki.*

(2) *$f(\varepsilon) = 0$ dla każdego pierwiastka pierwotnego n-tego stopnia z jedynki.*

D. Przypomnijmy, że przez U_n oznaczamy zbiór wszystkich pierwiastków pierwotnych n-tego stopnia z jedynki.

(1) $\Rightarrow$ (3). Załóżmy, że wielomian $f(x)$ jest podzielny w $\mathbb{Z}[x]$ przez $\Phi_n(x)$. Istnieje wtedy taki wielomian o współczynnikach całkowitych $g(x)$, że

$$f(x) = g(x)\Phi_n(x).$$

Niech ε będzie dowolnym pierwiastkiem pierwotnym n-tego stopnia z jedynki. Wtedy $\Phi_n(\varepsilon) = 0$ i stąd $f(\varepsilon) = g(\varepsilon)\Phi_n(\varepsilon) = g(\varepsilon) \cdot 0 = 0$.

(3) $\Rightarrow$ (2). Ta implikacja jest oczywista.

(2) $\Rightarrow$ (1). Załóżmy, że $f(\varepsilon) = 0$ dla pewnego $\varepsilon \in U_n$. Ponieważ $\varepsilon^n = 1$, więc ε jest elementem algebraicznym nad ciałem $\mathbb{Q}$ i (jak wiemy) jego wielomianem minimalnym nad $\mathbb{Q}$ jest wielomian cyklotomiczny $\Phi_n(x)$. Zatem

$$f(x) = g(x)\Phi_n(x)$$

dla pewnego wielomianu $g(x)$, należącego do pierścienia $\mathbb{Q}[x]$. Wszystkie współczynniki wielomianów $f(x)$ i $\Phi_n(x)$ są liczbami całkowitymi oraz $\Phi_n(x)$ jest wielomianem monicznym (tzn. jego wsółczynnik wiodący jest równy 1). Stąd wynika, że wszystkie współczynniki wielomian $g(x)$ są również liczbami całkowitymi. Zatem $f(x) = g(x)\Phi_n(x)$, gdzie $g(x) \in \mathbb{Z}[x]$. Wielomian $f(x)$ jest więc podzielny w $\mathbb{Z}[x]$ przez $\Phi_n(x)$. $\boxtimes$

Następne stwierdzenie opisuje wielomiany podzielne przez kwadrat wielomianu cyklotomicznego.

12.17.2. *Niech $n \in \mathbb{N}$ i niech ε będzie pierwiastkiem pierwotnym n-tego stopnia z jedynki. Niech $f(x) \in \mathbb{Z}[x]$ i niech $f'(x)$ oznacza pochodną wielomianu $f(x)$. Następujące warunki są równoważne.*

(1) *Wielomian $f(x)$ jest podzielny w $\mathbb{Z}[x]$ przez $\Phi_n(x)^2$.*

(2) *$f(\varepsilon) = f'(\varepsilon) = 0$.*

D. (1) $\Rightarrow$ (2). Załóżmy, że wielomian $f(x)$ jest podzielny w $\mathbb{Z}[x]$ przez $\Phi_n(x)^2$. Istnieje wtedy taki wielomian o współczynnikach całkowitych $g(x)$, że $f(x) = g(x)\Phi_n(x)^2$. Mamy wtedy:

$$f'(x) = g'(x)\Phi_n(x)^2 + 2g(x)\Phi_n(x)\Phi'_n(x).$$

Ale $\Phi_n(\varepsilon) = 0$, więc $f(\varepsilon) = g(\varepsilon)\Phi_n(\varepsilon)^2 = g(\varepsilon) \cdot 0^2 = 0$ oraz $f'(\varepsilon) = g'(\varepsilon)\Phi_n(\varepsilon)^2 + 2g(\varepsilon)\Phi_n(\varepsilon)\Phi'_n(\varepsilon) = g'(\varepsilon) \cdot 0^2 + 2g(\varepsilon) \cdot 0 \cdot \Phi'_n(\varepsilon) = 0$. Zatem $f(\varepsilon) = f'(\varepsilon) = 0$.

(2) $\Rightarrow$ (1) Załóżmy, że $f(\varepsilon) = f'(\varepsilon) = 0$. Z tego założenia wynika (na mocy stwierdzenia 12.17.1), że wielomiany $f(x)$ i $f'(x)$ są podzielne w $\mathbb{Z}[x]$ przez $\Phi_n(x)$. Niech

$$f(x) = g(x)\Phi_n(x),$$

gdzie $g(x) \in \mathbb{Z}[x]$. Ponieważ

$$f'(x) = g'(x)\Phi_n(x) + g(x)\Phi'_n(x)$$

oraz $\Phi_n(x)$ dzieli $f'(x)$, więc $\Phi_n(x)$ dzieli $g(x)\Phi'_n(x)$. Ale $\Phi_n(x) \nmid \Phi'_n(x)$ (gdyż $\deg \Phi'_n(x) < \deg \Phi_n(x)$) oraz $\Phi_n(x)$ jest wielomianem nierozkładalnym nad $\mathbb{Q}$, więc wielomian $g(x)$ jest podzielny (nad $\mathbb{Q}$) przez $\Phi_n(x)$. Istnieje więc taki wielomian $h(x) \in \mathbb{Q}[x]$, że

$$g(x) = h(x)\Phi_n(x).$$

Wszystkie współczynniki wielomianów $g(x)$ i $\Phi_n(x)$ są liczbami całkowitymi oraz $\Phi_n(x)$ jest wielomianem monicznym (tzn. jego wsółczynnik wiodący jest równy 1). Wszystkie więc współczynniki wielomian $h(x)$ są również liczbami całkowitymi. Zatem $g(x) = h(x)\Phi_n(x)$, gdzie $h(x) \in \mathbb{Z}[x]$ i stąd mamy równość $f(x) = h(x) \cdot \Phi_n(x)^2$, w której $h(x)$ jest wielomianem o współczynnikach całkowitych. Wielomian $f(x)$ jest więc podzielny w $\mathbb{Z}[x]$ przez $\Phi_n(x)^2$. ⊠

W podobny sposób można udowodnić ogólniejsze stwierdzenie.

12.17.3. *Niech n oraz $s \geqslant 2$ będą liczbami naturalnymi i niech ε będzie pierwiastkiem pierwotnym n-tego stopnia z jedynki. Niech $f(x)$ będzie wielomianem o współczynnikach całkowitych. Następujące warunki są równoważne.*

(1) *Wielomian $f(x)$ jest podzielny w $\mathbb{Z}[x]$ przez $\Phi_n(x)^s$.*

(2) *$f(\varepsilon) = f^{(1)}(\varepsilon) = \cdots = f^{(s-1)}(\varepsilon) = 0$, gdzie $f^{(j)}(x)$, dla $j = 1, \ldots, s-1$, oznacza j-tą pochodną wielomianu $f(x)$.*

Teraz zajmiemy się zapowiedzianą podzielnością przez wielomian cyklotomiczny

$$\Phi_3(x) = x^2 + x + 1.$$

Z wielomianem tym spotkaliśmy się już wcześniej, patrz na przykład: 1.4.1, 3.1.2, 3.1.3, 3.4.2, 3.11.3, 3.11.6, 3.11.7, 4.1.7.

W dowodach następnych stwierdzeń przez ε oznaczamy pierwiastek pierwotny trzeciego stopnia z jedynki. W tym przypadku mamy:

$$\varepsilon^3 = 1, \quad \varepsilon^2 + \varepsilon + 1 = 0, \quad \overline{\varepsilon} = \varepsilon^2, \quad \overline{\varepsilon^2} = \varepsilon.$$

12.17.4. *Wielomian $x^{2n} + x^n + 1$ dzieli się przez wielomian $x^2 + x + 1$ wtedy i tylko wtedy, gdy $3 \nmid n$.* ([BoW] 11 s.47, [Szn] 7.39).

D. Oznaczmy $f_n(x) = x^{2n} + x^n + 1$. Zauważmy, że:

$$\begin{aligned}
f_{3k}(\varepsilon) &= \left(\varepsilon^3\right)^{2k} + \left(\varepsilon^3\right)^k + 1 = 1^{2k} + 1^k + 1 = 3 \neq 0,\\
f_{3k+1}(\varepsilon) &= \left(\varepsilon^3\right)^{2k}\varepsilon^2 + \left(\varepsilon^3\right)^k\varepsilon^1 + 1 = 1^{2k}\varepsilon^2 + 1^k\varepsilon + 1 = \varepsilon^2 + \varepsilon + 1 = 0,\\
f_{3k+2}(\varepsilon) &= \left(\varepsilon^3\right)^{2k}\varepsilon^4 + \left(\varepsilon^3\right)^k\varepsilon^2 + 1 = 1^{2k}\varepsilon + 1^k\varepsilon^2 + 1 = \varepsilon^2 + \varepsilon + 1 = 0.
\end{aligned}$$

Teza wynika zatem ze stwierdzenia 12.17.1. ⊠

12.17.5. *Dla dowolnej liczby naturalnej n, wielomian*

$$x^{n+2} + (x+1)^{2n+1}$$

jest rozkładalny w $\mathbb{Z}[x]$. Ma on czynnik $x^2 + x + 1$. ([Str72]).

D. (**Sposób I**). Zauważmy najpierw, że

$$(x+1)^{2n} = \big((x+1)^2\big)^n = \big(x+(x^2+x+1)\big)^n = x^n + (x^2+x+1)q(x),$$

gdzie $q(x)$ jest wielomianem zmiennej x o współczynnikach w $\mathbb{Z}$. Wobec tego

$$\begin{aligned} x^{n+2} + (x+1)^{2n+1} &= x^2x^n + (x+1)(x+1)^{2n} = x^2x^n + (x+1)\big(x^n + (x^2+x+1)q(x)\big) \\ &= (x^2+x+1)\,(x^n + (x+1)q(x))\,. \end{aligned}$$

Zatem rozważany wielomian jest podzielny przez x^2+x+1.

(**Sposób II**). Niech $f(x) = x^{n+2} + (x+1)^{2n+1}$. Mamy wtedy:

$$\begin{aligned} f(\varepsilon) &= \varepsilon^{n+2} + (\varepsilon+1)^{2n+1} \\ &= \varepsilon^{n+2} + (-\varepsilon^2)^{2n+1} \\ &= \varepsilon^{n+2} - (\varepsilon^4)^n\varepsilon^2 \\ &= \varepsilon^{n+2} - (\varepsilon^1)^n\varepsilon^2 \\ &= \varepsilon^{n+2} - \varepsilon^{n+2} = 0 \end{aligned}$$

i teza wynika z 12.17.1. ⊠

12.17.6. *Wielomian* $(x+1)^n - x^n - 1$ *dzieli się przez wielomian* x^2+x+1 *wtedy i tylko wtedy, gdy* $n = 6k \pm 1$. ([BoW] 12 s.47, [Szn] 7.39).

D. Oznaczmy: $f_n(x) = (x+1)^n - x^n - 1$. Mamy wtedy:

$$\begin{aligned} f_{6k}(\varepsilon) &= (\varepsilon+1)^{6k} - \varepsilon^{6k} - 1 = (-\varepsilon^2)^{6k} - \varepsilon^{6k} - 1 = (\varepsilon^3)^{4k} - (\varepsilon^3)^{2k} - 1 = 1^{4k} - 1^{2k} - 1 = -1 \neq 0, \\ f_{6k+1}(\varepsilon) &= (\varepsilon+1)^{6k+1} - \varepsilon^{6k+1} - 1 = (-\varepsilon^2)^{6k+1} - \varepsilon^{6k+1} - 1 = -\big(\varepsilon^2+\varepsilon+1\big) = 0, \\ f_{6k+2}(\varepsilon) &= (\varepsilon+1)^{6k+2} - \varepsilon^{6k+2} - 1 = (-\varepsilon^2)^{6k+2} - \varepsilon^{6k+2} - 1 = \varepsilon^4 - \varepsilon^2 - 1 = \varepsilon - \varepsilon^2 - 1 = 2\varepsilon \neq 0, \\ f_{6k+3}(\varepsilon) &= (\varepsilon+1)^{6k+3} - \varepsilon^{6k+3} - 1 = (-\varepsilon^2)^{6k+3} - \varepsilon^{6k+3} - 1 = -1 - 1 - 1 = -3 \neq 0, \\ f_{6k+4}(\varepsilon) &= (\varepsilon+1)^{6k+4} - \varepsilon^{6k+4} - 1 = (-\varepsilon^2)^{6k+4} - \varepsilon^{6k+4} - 1 = \varepsilon^8 - \varepsilon^4 - 1 = \varepsilon^2 - \varepsilon - 1 = 2\varepsilon^2 \neq 0, \\ f_{6k+5}(\varepsilon) &= (\varepsilon+1)^{6k+5} - \varepsilon^{6k+5} - 1 = (-\varepsilon^2)^{6k+5} - \varepsilon^{6k+5} - 1 = -\varepsilon - \varepsilon^2 - 1 = 0. \end{aligned}$$

Wykazaliśmy, że $f_n(\varepsilon) = 0 \iff n = 6k \pm 1$. Teza wynika zatem ze stwierdzenia 12.17.1. ⊠

12.17.7. *Wielomian*

$$(x+1)^n - x^n - 1$$

dzieli się przez wielomian $(x^2+x+1)^2$ *wtedy i tylko wtedy, gdy* $n = 6k+1$.

D. Oznaczmy przez $f(x)$ wielomian $(x+1)^n - x^n - 1$ i przez $f'(x)$ jego pochodną, tzn.

$$f'(x) = n(x+1)^{n-1} - nx^{n-1}.$$

Załóżmy, że $n = 6k+1$. Z poprzedniego stwierdzenia wiemy, że wtedy $f(\varepsilon) = 0$. Ponadto,

$$f'(\varepsilon) = n\,(\varepsilon+1)^{6k} - n\varepsilon^{6k} = n\,\big(=\varepsilon^2\big)^{6k} - n\varepsilon^{6k} = n - n = 0.$$

Ze stwierdzenia 12.17.2 wynika zatem, że wielomian $f(x)$ jest podzielny w $\mathbb{Z}[x]$ przez $(x^2+x+1)^2$.

Załóżmy teraz, że wielomian $f(x)$ jest podzielny przez $(x^2+x+1)^2$. Wtedy wielomian ten jest podzielny przez x^2+x+1, a więc, na mocy 12.17.6, liczba n jest postaci $6k \pm 1$. Łatwo sprawdzić, że jeśli $n = 6k-1$, to $f'(\varepsilon) \neq 0$ i wtedy (patrz stwierdzenie 12.17.2) $f(x)$ nie jest podzielne przez $(x^2+x+1)^2$. Zatem, $n = 6k+1$. ⊠

Wielomian $(x+1)^n - x^n - 1$ jest oczywiśście podzielny przez x. Można udowodnić:

12.17.8. *Dla $n \geqslant 2$ rozpatrzmy wielomian*

$$f_n(x) = \frac{(x+1)^n - x^n - 1}{x}.$$

(1) *Jeśli $\alpha \in \mathbb{C}$ jest pierwiastkiem wielomianu $f_n(x)$, to $1/\alpha$ również jest pierwiastkiem tego wielomianu.*

(2) *Jeśli $p \geqslant 3$ jest liczbą pierwszą, to wielomian f_{2p} jest nierozkładalny.* ([Fila] s.35).

Nie znamy odpowiedzi na anstępujące pytanie.

12.17.9. *Czy dla każdej liczby parzystej n powyższy wielomian $f_n(x)$ jest nierozkładalny nad $\mathbb{Q}$?.* ([Fila] s.35).

12.17.10. *Wielomian $(x+1)^n + x^n + 1$ dzieli się przez wielomian $x^2 + x + 1$ wtedy i tylko wtedy, gdy $n = 6k \pm 2$.* ([BoW] 12 s.47, [Szn] 7.39).

Dowodzimy to dokładnie tak samo jak stwierdzenie 12.17.6. Drobne zmiany w dowodzie stwierdzenia 12.17.7 pozwalają natomiast udowodnić:

12.17.11. *Wielomian $(x+1)^n + x^n + 1$ dzieli się przez wielomian $(x^2 + x + 1)^2$ wtedy i tylko wtedy, gdy $n = 6k + 4$.*

12.18 Inne zastosowania wielomianów cyklotomicznych

Przy pomocy wielomianów cyklotomicznych łatwo dowodzi się następujące znane fakty.

12.18.1. *Niech G będzie skończoną grupą abelową. Istnie wtedy rozszerzenie Galois ciała liczb wymiernych, którego grupą Galois jest G.* ([Mot1]).

12.18.2 (Wedderburn)**.** *Każde (skośne) ciało skończone jest przemienne.* ([Mot4]).

12.18.3. *Każda skończona podgrupa multyplikatywnej grupy ciała jest cykliczna.* ([Mot5]).

12.18.4. *Niech L będzie podciałem ciała liczb zespolonych i niech G będzie grupą wszystkich jego elementów skończonego rzędu. Wtedy G jest skończoną grupą cykliczną.* ([Mot7]).

12.18.5. *Niech k będzie skończonym ciałem. Dla każdej liczby naturalnej n istnieje nierozkładalny wielomian stopnia n należący do $k[x]$.* ([Mot5]).

★ J. B. Dence, *Primitive roots the cyclotomic way*, preprint.

D. C. van Leijenhorst, *A simple proof of Wedderburn's theorem*, preprint.

K. Motose, *Let's use cyclotomic polynomials in your lecture for your students*, 2003.

B. Tuckerman, *Factorization of $x^{2n} + x^n + 1$ using cyclotomic polynomials*, [MM] 42(1)(1969) 41-42.

Literatura

[Apl] T. M. Apostol, *Resultants of cyclotomic polynomials*, Proceedings of the American Mathematical Society, 24(3)(1970), 457-462.

[ArB] J.M. Arnaudiès, J. Bertin, *Groupes, Algèbres et Géométrie* (Tome 1) Ellipses.

[Bams] Bulletin of the American Mathematical Society, (Bull. Amer. Math. Soc.), czasopismo matematyczne.

[Bang] A. S. Bang, *Om Ligningen* $\phi_n(x) = 0$, Nyt Tidsskrift for Mathematik 6(1895) 6-12.

[BirV] G. Birkhoff, H.S. Vandiver, *On the integral divisors of* $a^n - b^n$, Annals of Math. 2(5)(1904), 173-180.

[Bloo] D. M. Bloom, *On the coefficients of the cyclotomic polynomials*, The American Mathematical Monthly, 75(1968), 372-377.

[BoC] P. Borwein, K-K. S. Choi, *On cyclotomic polynomials with* ± 1 *coefficients*, preprint.

[BoW] W. G. Bołtiański, I. J. Wilenkij, *Symetria w Algebrze* (po rosyjsku), Nauka, Moskwa, 1967.

[Br68] J. Browkin, *Wybrane Zagadnienia Algebry*, PWN, Warszawa, 1968.

[Br77] J. Browkin, *Teoria Ciał*, PWN, Warszawa, 1977.

[Drn] G. Dresden, *Resultants of cyclotomic polynomials*, Rocky Mountain Journal of Mathematics, 42(5)(2012), 1-9.

[Fil] M. Filaseta, *Coverings of the integers associated with an irreducibility theorem of A. Schinzel*, Number Theory for the Millennium, II Urbana, IL, 2000, 1-24, A.K. Peters Natick, MA, 2002.

[Fila] M. Filaseta, *The Theory of Irreducible Polynomials*, Preprint, 2000. `http://www.math.sc.edu/~filaseta`.

[Golo] S. W. Golomb, *Cyclotomic polynomials and factorization theorems*, The American Mathematical Monthly, 85(9)(1978), 734-737.

[Isaa] I. M. Isaacs, *Algebra*, A Graduate Course, Brooks/Cole Publishing Company, Pacific Grove, California, 1994.

[Kw] Kwant, popularne czasopismo rosyjskie.

[La84] S. Lang, *Algebra*, Second Edition, Addison–Wesley Publ. Comp. 1984.

[MG] The Mathematical Gazette, angielskie popularne czasopismo matematyczne.

[MM] Mathematics Magazine, popularne czasopismo matematyczne.

[Mon] The American Mathematical Monthly, Mathematical Association of America.

[Mot1] K. Motose, *On values of cyclotomic polynomials*, Math. J. Okayama Univ. 35(1993) 35-40.

[Mot2] K. Motose, *On values of cyclotomic polynomials II*, Math. J. Okayama Univ. 37(1995) 27-36.

[Mot3] K. Motose, *On values of cyclotomic polynomials III*, Math. J. Okayama Univ. 38(1996) 115-122.

[Mot4] K. Motose, *On values of cyclotomic polynomials IV*, Bull. Fac. Sci. Tech. Hirosaki Univ. 1(1998) 1-7.

[Mot5] K. Motose, *On values of cyclotomic polynomials V*, Math. J. Okayama Univ. 45(2003) 29-36.

[Mot7] K. Motose, *On values of cyclotomic polynomials VII*, Bull. Fac. Sci. Tech. Hirosaki Univ. 7(2004) 1-8.

[N-4] A. Nowicki, *Liczby Pierwsze*, Podróże po Imperium Liczb, cz.4, Wydawnictwo OWSIiZ, Toruń, Olsztyn. Wydanie pierwsze 2009; Wydanie drugie 2012.

[N-5] A. Nowicki, *Funkcje Arytmetyczne*, Podróże po Imperium Liczb, cz.5, Wydawnictwo OWSIiZ, Toruń, Olsztyn. Wydanie pierwsze 2009; Wydanie drugie 2012.

[N-6] A. Nowicki, *Podzielność w Zbiorze Liczb Całkowitych*, Podróże po Imperium Liczb, cz.6, Wydawnictwo OWSIiZ, Toruń, Olsztyn. Wydanie pierwsze 2009; Wydanie drugie 2012.

[N-8] A. Nowicki, *Liczby Mersenne'a, Fermata i Inne Liczby*, Podróże po Imperium Liczb, cz.8, Wydawnictwo OWSIiZ, Toruń, Olsztyn. Wydanie pierwsze 2010; Wydanie drugie 2012.

[Nagl] T. Nagell, *Introduction to Number Theory*, Chelsea Publishing Company, New York, 1964.

[Nar03] W. Narkiewicz, *Teoria Liczb*, PWN, Wydanie trzecie, Warszawa, 2003.

[Pjap] Proceedings of the Japan Academy, Ser. A, Mathematical Sciences.

[Pmgr] Praca magisterska, Uniwersytet Mikołaja Kopernika w Toruniu, Wydział Matematyki i Informatyki.

[Ri01] P. Ribenboim, *Wielkie Twierdzenie Fermata dla Laików*, WNT, Warszawa, 2001.

[Rtk] A. Rotkiewicz, *Elementarny dowód istnienia dzielnika pierwszego pierwotnego liczby* $a^n - b^n$, Prace Matematyczne, 4(1960), 21-28.

[Str72] S. Straszewicz, *Zadania z Olimpiad Matematycznych*, tom IV, 16-20, 64/65 - 68/69, PZWS, Warszawa, 1972.

[Szn] L. B. Szneperman, *Zbiór Zadań z Algebry i Teorii Liczb* (po rosyjsku), Minsk, 1982.

[Zeit] D. Zeitlin, *On coefficints identities for cyclotomic polynomials* $F_{pq}(x)$, The American Mathematical Monthly, 75(9)(1968), 976-980.