Ciklotomični polinomi

Vukašin Brković

Jun 2013, Beograd

Iako možda imaju malo rogobatno ime, ovi polinomi imaju jako lepa svojstva, i predstavljaju svojevrstan spoj algebre i teorije brojeva. Osnovni cilj ovog rada je da upozna čitaoca sa nekim od tih svojstava, kao i da predstavi poznatu Žigimondijevu teoremu, ali je, takodje, predstavljena i primena ciklotomičnih polinoma u zadacima takmičarskog tipa. Svi pojmovi su uvedeni postupno, sa namerom da ova tema bude lako razumljiva i svima onima koji se sa njom prvi put sreću. Takodje, nisu zanemareni ni oni čitaoci koji imaju olimpijske aspiracije, jer, pored zadataka, u radu se mogu naći i razne teoreme i leme, sa referencama, koje imaju veliku primenu na takmičenjima.

Ovaj rad predstavlja dopunjenu verziju mog maturskog rada, pa se i ovom prilikom zahvaljujem svom mentoru, Predragu Tanoviću, koji je doprineo njegovom stvaranju.

Konačno, voleo bih da poručim svima kojima je ova tema napoznata, i zbog toga oklevaju da započnu čitanje, da ona krije mnogo više matematičke lepote, nego što možda na prvi pogled otkriva, a uporni će se, nesumnjivo, osetiti nagradjenim.

Sadržaj

1 Potrebni pojmovi

1.1 Mebijusova funkcija

Mebijusova funkcija je funkcija definisana za sve prirodne brojeve, i to na sledeći način:

$$\mu(n) = \begin{cases} 1 & \text{kada je } n = 1; \\ (-1)^k & \text{kada } n \text{ nije deljivo potpunim kvadratom, } k \text{ je broj prostih činilaca;} \\ 0 & \text{inače.} \end{cases}$$

Mebijusova funkcija je multiplikativna što znači da važi $\mu(mn) = \mu(m)\mu(n)$, za sve uzajamno proste brojeva m, n.
Ova funkcija ima nekoliko značajnih svojstava, što ćemo videti u narednim teoremama.

Teorema 1.1. *Neka je n prirodan broj. Tada važi.*

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \textit{kada je } n = 1\textit{;} \\ 0 & \textit{u suprotnom.} \end{cases}$$

Dokaz. Za $n = 1$ tvrdjenje sledi iz definicije Mebijusove funkcije. Pretpostavimo onda da važi $n \geq 2$. Neka je

$$n = \prod_{i=1}^{s} p_i^{\alpha_i}$$

kanonska faktorizacija broja n. Tada primetimo da zbog osobina Mebijusove funkcije, u traženom zbiru je $\mu(d) = 0$ za svako $d \mid n$ koje ne deli $P = \prod_{i=1}^{s} p_i$ (jer je tada d deljiv potpunim kvadratom). Takodje, lako se vidi iz multiplikativnosti Mebijusove funkcije da je $\mu(pd) = \mu(p)\mu(d) = -\mu(d)$, za svaki prost broj p, i prirodan broj d, takvih da $p \nmid d$. Ako uzmemo proizvoljan broj p td. $p \mid P$, onda iz svega navedenog važi:

$$\sum_{d|n} \mu(d) = \sum_{d|P} \mu(d) = \sum_{d|\frac{P}{p}} (\mu(d) + \mu(pd)) = \sum_{d|\frac{P}{p}} (\mu(d) - \mu(d)) = 0$$

□

Teorema 1.1 vodi ka dokazivanju mnogo bitnije teoreme, i *Mebijusove inverzne formule*:

Teorema 1.2. *Neka su $f, F : \mathbb{N} \to \mathbb{N}$ funkcije takve da važi*

$$F(n) = \sum_{d|n} f(d).$$

Tada je

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

Dokaz. Imamo da važi:

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

Poslednja suma se pregrupisanjem sabiraka može transformisati u novu, u našem dokazu, korisniju sumu. Naime, posmatrajmo proizvoljno t, koje je pod funkcijom f. Vidimo da je uz njega $\mu(d_i)$ kada god $t \mid \frac{n}{d_i}$, tj. kada $d_i \mid \frac{n}{t}$. Kako t-ovi predstavljaju skup svih delilaca brojeva koji su sami delioci broja n, to oni upravo predstavljaju skup delilaca broja n. Dakle, važi:

$$\sum_{d|n} \left(\mu(d) \sum_{t|\frac{n}{d}} f(t) \right) = \sum_{t|n} \left(f(t) \sum_{d|\frac{n}{t}} \mu(d) \right)$$

Na osnovu prethodne teoreme vidimo da je

$$\sum_{d|\frac{n}{t}} \mu(d) = \begin{cases} 1 & \text{kada je } \frac{n}{t} = 1; \\ 0 & \text{u suprotnom.} \end{cases}$$

Dakle,

$$\sum_{t|n} \left(f(t) \sum_{d|\frac{n}{t}} \mu(d) \right) = f(n)$$

što smo i hteli pokazati.

□

Napomena. *Ako je φ Ojlerova funkcija, tada važi dobro poznat identitet $n = \sum_{d|n} \varphi(d)$. Sada, na osnovu teoreme 1.2 dobijamo:*

$$\varphi(n) = \sum_{d|n} \mu(d) \frac{n}{d}$$

Ova i sledeća teorema su usko povezane, i gotovo se identično dokazuju.

Teorema 1.3. *Neka su* $f, F : \mathbb{N} \to \mathbb{N}$ *funkcije takve da važi*

$$F(n) = \prod_{d|n} f(d).$$

Tada je

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

Dokaz. Opet, kao i u prethodnom dokazu, za proizvoljno t posmatramo koje $\mu(d)$ mu je stepen, pa analognim rezonovanjem dobijamo:

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

□

1.2 Kompleksni primitivni koreni

Definicija 1. *Za dati broj* n*, definišemo* n***-ti koren jedinice****, kao kompleksan broj* θ *koji zadovoljava jednakost* $\theta^n = 1$*.*

Poznato je da su sva rešenja jednačine $x^n = 1$ brojevi oblika $\theta = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}$, za $k = 1, ..., n$, pa upravo oni predstavljaju skup n-tih korena jedinice.

Definicija 2. *Neka je* θ n*-ti koren jedinice, za proizvoljno* $n \in \mathbb{N}$*. Tada najmanji prirodan broj* k *takav da važi* $\theta^k = 1$ *nazivamo* ***poretkom*** *broja* θ *i označavamo sa* $ord(\theta)$*.*

Lema 1. *Neka je* n *prirodan broj i* θ *proizvoljni* n*-ti koren jedinice. Tada za neki ceo broj* k *važi* $\theta^k = 1$ *akko* $ord(\theta) \mid k$*. Specijalno,* $ord(\theta) \mid n$

Dokaz. Neka je $d = ord(\theta)$. Ako $d \mid k$, tada važi $\theta^k = \left(\theta^d\right)^{\frac{k}{d}} = 1$, pa je jedan smer pokazan. Neka važi $\theta^k = 1$, i neka je $k = qd + r$, gde je $0 \leq r \leq d - 1$. Kako je $1 = \theta^{qd+r} = \left(\theta^d\right)^q \theta^r = \theta^r$, sledi da je $\theta^r = 1$, ; pa pošto je $r < d = ord(\theta)$, to je $r = 0$, tj. $k = qd$, što je i trebalo pokazati. □

Posledica. *Lako se vidi i da je* $\theta^k = \theta^l$ *akko je* $k \equiv_d l$*. Specijalno, za* $1 \leq k, l \leq d$ *važi i* $k = l$*.*

Definicija 3. *Neka je* θ n*-ti koren jedinice, za neko* $n \in \mathbb{N}$*. Ukoliko važi* $ord(\theta) = n$*, onda* θ *nazivamo* ***primitivnim*** n***-tim korenom*** *jedinice.*

Lema 2. *Neka je θ primitivni n-ti koren jedinice. Tada je skup $\{\theta, \theta^2, ..., \theta^n\}$, skup svih n-tih korena jedinice*

Dokaz. Kako je $\left(\theta^k\right)^n = (\theta^n)^k = 1$, to je i θ^k $n-$ti koren jedinice. Kako su brojevi $\theta, \theta^2, ..., \theta^n$ medjusobno različiti(lako se vidi iz posledice leme 2, i definicije 3) i ima ih n, to oni predstavljaju sve n-te korene. □

Lema 3. *Neka su n, k prirodni brojevi i θ primitivni n-ti koren jedinice. Tada je i θ^k takodje primitivni n-ti koren jedinice akko je $(k, n) = 1$*

Dokaz. Neka je $d = ord(\theta^k)$. Kako je $\theta^{kd} = 1$, to iz leme 1 sledi $ord(\theta) \mid kd$, tj. $n \mid kd$. Ako je $(k, n) = 1$, onda $n \mid d$. Medjutim, zbog $ord(\theta^k) \mid n$ sledi i $d \mid n$, odakle je $d = n$, pa je, zaista, θ^k primitivni n-ti koren jedinice.
Ako je $(k, n) \neq 1$, onda zbog $1 = (\theta^n)^{\frac{k}{(n,k)}} = \left(\theta^k\right)^{\frac{n}{(n,k)}}$, sledi da $d \mid \frac{n}{(n,k)}$, odakle je $d < n$ pa zbog toga θ^k nije primitivni n-ti koren jedinice. □

Posledica. *Za dati prirodan broj n postoji $\varphi(n)$ primitivnih n-tih korena jedinice.*

Teorema 1.4. *Zbir svih primitivnih n-tih korena jedinice jednak je $\mu(n)$.*

Dokaz. Neka je

$$f(n) = \sum_{\substack{1 \leq k \leq n \\ (k,n)=1}} e^{2\pi ik/n}.$$

gde je $e^{2\pi i/n}$ primitivni n-ti koren. Pokažimo da je f multiplikativna. Za početak dokažimo da je svih $\varphi(mn)$ sabiraka iz $f(m)f(n)$ medjusobno različito. Pretpostavimo suprotno, tj da su neka dva jednaka, tj. $e^{2\pi ia/n}e^{2\pi ib/m} = e^{2\pi ic/n}e^{2\pi id/m}$. Tada je, pak $am + nb \equiv cm + dn \pmod{mn} \Leftrightarrow m(a - c) + n(b - d) \equiv 0 \pmod{mn}$, što se lako vidi da nije moguće jer je $(m, n) = 1$. Takodje, svaki od ovih sabiraka se pojavljuje i u $f(mn)$. Zaista, to je zato jer je $(am + bn, mn) = 1$ zbog $(a, n) = b, m) = 1$. Dakle, f je multiplikativna.

Pošto je očigledno $f(p) = \theta + \theta^2 + ... + \theta^{p-1} = \frac{\theta(\theta^{p-1}-1)}{\theta-1} = -1$, i sl. $f(p^k) = 0$, to iz multiplikativnosti f sledi $f(n) = \mu(n)$ za sve n. □

1.3 Neke osobine polinoma

Teorema 1.5. *Neka su f i g dva monična polinoma sa racionalnim koeficijentima. Ako su svi koeficijenti polinoma $f \cdot g$ celi brojevi, onda su to i svi koeficijenti polinoma f i g.*

Dokaz. Neka su $f(x) = x^m + a_{m-1}x^{m-1} + ... + a_0$ i $g(x) = x^n + b_{n-1}x^{n-1} + ... + b_0$ posmatrani polinomi. Neka su M i N najmanji prirodni brojevi takvi da su $Mf(x)$ i $Ng(x)$ polinomi sa celobrojnim koeficijentima (Očigledno je da takvi M i N postoje, to su najmanji zajednički sadržaoci od imenioca brojeva $a_m, a_{m-1}, ..., a_0$ tj. $b_n, b_{n-1}, ..., b_0$, u skraćenom obliku). Neka je dalje $A_i = Ma_i$, za $0 \leq i \leq m-1$, i $B_j = Mb_j$, za $0 \leq j \leq n-1$, i neka je $A_m = M$, tj. $B_n = N$. Tada je

$$MNf(x)g(x) = A_m B_n x^{m+n} + ... + A_0 B_0$$

Kako je, po pretpostavci $f(x)g(x) \in \mathbb{Z}[x]$, to su svi koeficijenti polinoma $MNf(x)g(x)$ deljivi sa MN.

Pretpostavimo da je $MN > 1$ (u suprotnom bi bilo $M = 1$, $N = 1$, čime bi tvrdjenje bilo dokazano). Neka je p prost broj takav da $p \mid MN$. Pokažimo da tada postoji $i \in 0, 1, ..., m$ takav da $p \nmid A_i$. Zaista, ako $p \nmid M$, tada je i $p \nmid A_m$. U suprotnom, ako $p \mid M$, opet ne može da važi $p \mid A_i$, za sve $i \in 0, 1, ..., m$, jer bi tada važilo da je $\left(\frac{M}{p}\right) a_i = \frac{A_i}{p} \in \mathbb{Z}$, pa bismo imali kontradikciju sa minimalnosti broja M. Analognim postupkom pokazuje se i da postoji $j \in 0, 1, ..., n$, takvo da $p \nmid B_j$. Neka su I, J najveći od svih brojeva i, j, za koje je zadovoljeno $p \nmid A_i$,$p \nmid B_j$. Tada je koeficijent uz član x^{I+J}, u polinomu $MNf(x)g(x)$, broj oblika $A_I B_J + S$, i pritom ćemo pokazati da $p \mid S$. Zaista, kako je $S = \sum_{\substack{k+l=I+J \\ k \neq I, l \neq J}} A_k B_l$, to mora za svaki sabirak u toj sumi da važi ili $k > I$, ili $l > J$, pa tada važi $p \mid A_k$, tj. $p \mid B_l$, odnosno svaki sabirak je deljiv sa p, pa $p \mid S$. Dakle, dobili smo da koeficijent uz x^{I+J} nije deljiv sa MN. Iz te kontradikcije sledi da ne može važiti $MN > 1$, iz čega sledi tvrdjenje. □

Definicija 4. *Neka je dat polinom*

$$P(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$$

sa koeficijentima iz nekog polja k.Tada je ***izvod*** *polinoma $P(x)$, novi polinom*

$$P'(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + ... + a_1$$

.

Teorema 1.6. *Neka su f, g dva polinoma iz $k[x]$. Tada važi:*
a) $(f(x) + g(x))' = f'(x) + g'(x)$
b) $(f(x) \cdot g(x))' = f(x) \cdot g'(x) + f'(x) \cdot g(x)$

Dokaz. a) Neka je $f(x) = \sum_{i=0}^{n} a_i x^i, g(x) = \sum_{i=0}^{n} b_i x^i$. Tada je

$$(f+g)' = \left(\sum_{i=0}^{n}(a_i + b_i)x^i\right)' = \sum_{i=0}^{n} i(a_i + b_i)x^{i-1} = f' + g'$$

b) Slično prvom delu

$$\begin{aligned}(f\cdot g)' &= \left(\sum_{m,n\geq 0}^{n} a_m b_n (x^m x^n)\right)' = \sum_{m,n\geq 0}^{n} a_m b_n (m+n) x^{m+n-1} \\ &= \sum_{m,n\geq 0}^{n} a_m b_n (m x^{m-1} x^n) + \sum_{m,n\geq 0}^{n} a_m b_n (x^m n x^{n-1}) = f\cdot g' + f'\cdot g\end{aligned}$$

□

Definicija 5. *Polinom je ireducibilan ako se ne može napisati kao proizvod polinoma manjih stepena, sa koeficijentima iz istog polja kao njegovi.*

Sledeća teorema važi za sva savršena polja k (videti [5]), ali ćemo se mi zadržati na poljima $\mathbb{R}, \mathbb{Q}, \mathbb{Z}, \mathbb{Z}_p$.

Teorema 1.7. *Neka je P polinom iz $k[x]$. Tada postoji nekonstantni $m(x)$ takav da važi $m(x)^2 \mid P(x)$ akko $(P(x), P'(x)) \neq 1$.*

Dakle, pokazaćemo da tvrdjenje važi za polja $\mathbb{R}, \mathbb{Q}, \mathbb{Z}, \mathbb{Z}_p$. Prvo dokažimo da sledeća lema važi:

Lema 4. *Ireducibilan nekonstantan polinom $\pi(x)$ iz opisanih polja ne može imati izvod jednak* 0.

Dokaz. Za $\mathbb{R}, \mathbb{Q}, \mathbb{Z}$ ovo se lako vidi, jer po definiciji izvoda, ako je on jednak nuli, polinom iz tih polja mora biti konstantan. Dokažimo tvrdjenje za $\mathbb{Z}_p$. Neka je $f(x) = \sum_{k\geq 0} a_k x^{pk}$ ireducibilan polinom čiji je izvod 0. Medjutim, primetimo da je $f(x) \equiv \left(\sum_{k\geq 0} a_k x^k\right)^p \pmod p$, tj. pošto radimo u $\mathbb{Z}_p$ to u poslednjem izrazu važi jednakost, što je kontradikcija sa uslovom da je f ireducibilan. Time smo dokazali tvrdjenje. □

Vratimo se sada na teoremu.

Dokaz. Ako $m(x)^2 | P(x)$, onda ako je $P(x) = m(x)^2 Q(x)$ onda je $P'(x) = 2m(x)m'(x)\cdot Q(x) + m(x)^2 \cdot Q'(x)$, tj. $m(x) | P'(x)$, pa je time prvi smer pokazan.

Za drugi smer neka je $\pi(x)$ ireducibilan činilac polinoma $(P(x), P'(x))$. Tada je $P(x) = \pi(x)\cdot Q(x)$. Pošto je: $P'(x) = \pi(x)\cdot Q'(x) + \pi'(x)\cdot Q(x)$. pa sledi da $\pi(x)$ deli $\pi'(x)\cdot Q(x)$. Kako je $\deg \pi' < \deg \pi$ a po lemi 4, $\pi'(x)$ je različit od nule, pa kako je $\pi(x)$ ireducibilan to $\pi(x)$ ne deli $\pi'(x)$, tj. $\pi(x) \mid Q(x)$. Medjutim, tada sledi $\pi(x)^2 \mid P(x)$ pa je i drugi smer pokazan. □

Posledica. *Polinom $x^n - 1$ nema dvostrukih nula, za sve prirodne brojeve n.*

Sledeća teorema glasi veoma slično prethodnoj, i na prvu loptu kontradiktorno sa njenom posledicom:

Teorema 1.8. *Neka je p prost broj. Pretpostavimo da postoji ceo broj a, i polinom $f \in \mathbb{Z}[x]$, takav da važi:*

$$x^n - 1 \equiv (x-a)^2 f(x) \pmod{p}$$

Tada $p \mid n$.

Dokaz. Primetimo da $p \nmid a$. Uvedimo smenu $y = x - a$. Tada je uslov zadatka ekvivalentan sa: $(y+a)^n \equiv y^2 f(y+a) \pmod{p}$, pa ako uporedimo koeficijente uz član y, u oba polinoma, dobijamo da je $na^{n-1} \equiv 0 \pmod{p} \Leftrightarrow p \mid n$, što se i tvrdi. □

2 Definicija i svojstva ciklotomičnih polinoma

Definicija 6. *Neka je n proizvoljan prirodan broj. Tada n-tim ciklotomičnim polinomom nazivamo moničan polinom čiji su koreni primitivni n-ti koreni jedinice (i pritom nema dvostrukih nula):*

$$\Phi_n(x) = \prod_{\substack{ord(\theta)=n \\ \theta^n=1}} (x - \theta)$$

Pošto postoji $\varphi(n)$ primitivnih n-tih korena jedinice, to je stepen polinoma $\Phi_n(X)$ upravo $\varphi(n)$.

Teorema 2.1. *Neka je n prirodan broj. Tada važi:*

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

Dokaz. Sve nule polinoma $x^n - 1$ su n-ti koreni jedinice. Neka je θ jedan od tih korena, i neka je $ord(\theta) = d$. Tada je θ primitivni d-ti koren jedinice, pa je samim tim i nula polinoma $\Phi_d(x)$, a takodje, pošto $d \mid n$, to je θ nula i polinoma sa desne strane jednakosti u našoj teoremi, pa pošto su oba polinoma u toj teoremi monična, i imaju sve jednake nule, to su i oni sami jednaki, pa je jednakost zadovoljena. Primetimo da uporedjivanjem stepena najstarijih članova dobijamo jedan od dokaza već spomenutog tvrdjenja da je $n = \sum_{d \mid n} \varphi(d)$. □

Teorema 2.2. *Neka je n prirodan broj. Tada je $\Phi_n(x) \in \mathbb{Z}[x]$*

Dokaz. Dokažimo tvrdjenje indukcijom. Za $n = 1$ je očigledno tačno jer je $\Phi_1(x) = x - 1$
Pretpostavimo da je tvrdjenje tačno za sve brojeve manje od n. Tada je

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

pa su koeficijenti polinoma $\Phi_n(x)$ racionalni brojevi, a prema teoremi 1.5 samim tim i celi. □

Teorema 2.3. *Za svaki prirodan broj n, polinom $\Phi_n(x)$ je simetričan.*

Dokaz. Tvrdjenje sledi iz činjenice da je proizvod dva simetrična polinoma takodje simetričan polinom. Dokaz može da se sprovede indukcijom po n.

Za $n = 1$ tvrdjenje je očigledno tačno. Pretpostavimo da je tačno za sve $k < n$, i dokažimo da važi i za n.

Kako je $x^n - 1 = \prod_{d|n} \Phi_d(x)$, to je, pošto su $x^n - 1$ i $\prod_{\substack{d|n \\ d \neq n}} \Phi_d(x)$ simetrični polinomi, i $\Phi_n(x)$ simetričan polinom.

□

Teorema 2.4. *Za prirodan broj n važi:*

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

Dokaz. Tvrdjenje sledi direktno iz teoreme 1.3 i teoreme 2.1. □

Ovakav zapis ciklotomicnog polinoma je dosta zgodan za njihovo izracunavanje, a može se iskoristiti i za dokaz sledeće važne teoreme:

Teorema 2.5. *Neka je p prost, a n prirodan broj. Tada važi:*

$$\Phi_{pn}(x) = \begin{cases} \Phi_n\left(x^p\right) & \textit{kada } p \mid n; \\ \frac{\Phi_n(x^p)}{\Phi_n(x)} & \textit{u suprotnom.} \end{cases}$$

Dokaz. Pretpostavimo prvo da $p \mid n$:

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

Primetimo da u poslednjoj zagradi važi $d \mid pn$, i $d \nmid n$, pa odatle odmah sledi da $p \mid d$. Medjutim pošto $p \mid n$ to važi i $p^2 \mid d$. Zaista, ako bi bilo $d = pd_0$, gde $p \nmid d_0$, tada bi iz $d \mid pn$ sledilo $d_0 \mid n$, tj. zbog $(d_0, p) = 1$ je $d_0 \mid \frac{n}{p}$, odakle sledi $d_0 p \mid n$, tj. $d \mid n$, što je nemoguće. Dakle, $p^2 \mid d$, i samim tim po definiciji Mebijusove funkcije je $\mu(d) = 0$, pa je

$$\prod_{\substack{d \mid pn \\ d \nmid n}} \left(x^{\frac{pn}{d}} - 1\right)^{\mu(d)} = 1$$

odakle je $\Phi_{pn}(x) = \Phi_n(x^p)$, što se i tvrdilo.

Drugi slučaj teoreme se može pokazati analogno prvom:

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

□

Posledica. *Neka je p prost broj, a n i k prirodni brojevi. Tada važi:*

$$\Phi_{p^k n}(x) = \begin{cases} \Phi_n\left(x^{p^k}\right) & \text{kada } p \mid n; \\ \frac{\Phi_n(x^{p^k})}{\Phi_n(x^{p^{k-1}})} & \text{kada } p \nmid n. \end{cases}$$

Dokaz. Na osnovu prethodne teoreme važi:

$$\Phi_{p^k n}(x) = \Phi_{p^{k-1}n}(x^p) = ... = \Phi_{pn}(x^{p^{k-1}}) = \begin{cases} \Phi_n\left(x^{p^k}\right) & \text{kada } p \mid n; \\ \frac{\Phi_n(x^{p^k})}{\Phi_n(x^{p^{k-1}})} & \text{kada } p \nmid n. \end{cases}$$

□

Teorema 2.6. *Ako su a, n prirodni brojevi takvi da je $(a, n) = 1$, tada važi:*

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

.

Dokaz. Dokaz ćemo sprovesti utvrdjivanjem da oba polinoma imaju jednake nule. Stepen prvog polinoma je $a\varphi(n)$, a drugog je $\sum_{d|a} \varphi(dn) = \varphi(n) \sum_{d|a} \varphi(d) = \varphi(n)a$ tj. jednakog su stepena. Dakle, pokazujemo da je svaki a-ti koren primitivnog n-tog korena jedinice takodje i koren polinoma sa desne strane.

Neka je θ primitivni n-ti koren jedinice. Tada je $\Phi_n(x^a) = \prod_{(k,n)=1}(x^a - \theta^k)$. Dakle, svaka nula ovog polinoma je oblika ω^k, gde je ω primitivni an-ti koren jedinice, i $(k, n) = 1$. Neka je tada $g = (k, a)$. Onda je ω^k primitivni $\frac{an}{g}$-ti koren jedinice. Ako je $d = \frac{a}{g}$ onda je ω^k koren polinoma $\Phi_{nd}(x)$. Odatle sledi da su im sve nule jednake, pa pošto su oba polinoma monična, dokaz je gotov. □

Teorema 2.7. *Ako je p prost broj, tada je $\Phi_p(x)$ ireducibilan.*

Proof. Da bi pokazali tvrdjenje dovoljno je pokazati da je $\Phi_p(x + 1)$ ireducibilan. Primetimo da je, na osnovu teoreme 2.5

$$\begin{aligned} \Phi_p(x+1) &= \frac{(x+1)^p - 1}{(x+1) - 1} \\ &= x^{p-1} + \binom{p}{1} x^{p-2} + ... + \binom{p}{p-1} \end{aligned}$$

Što po Ajzenštajnovom kriterijumu (vidi [6]) znači da je $\Phi_p(x+1)$ ireducibilan, pa je time dokaz gotov. □

Za kraj ovog dela, predstavljeno je prvih 10 ciklotomičnih polinoma:
$\Phi_1(x) = x - 1$
$\Phi_2(x) = x + 1$
$\Phi_3(x) = x^2 + x + 1$
$\Phi_4(x) = x^2 + 1$

$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$
$\Phi_6(x) = x^2 - x + 1$
$\Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
$\Phi_8(x) = x^4 + 1$
$\Phi_9(x) = x^6 + x^3 + 1$
$\Phi_{10}(x) = x^4 - x^3 + x^2 - x + 1$

2.1 Veza ciklotomičnih polinoma i poretka broja po prostom modulu

Lema 5. *Neka je n prirodan broj, i $d < n$ delilac broja n. Ako je x ceo broj i p prost broj takav da deli i $\Phi_n(x)$, i $\Phi_d(x)$, tada $p \mid n$.*

Dokaz. Prema teoremi 2.1 važi $x^n - 1 = \prod_{q|n} \Phi_q(x)$, pa je $x^n - 1$ deljivo sa $\Phi_n(x)\Phi_d(x)$, pa ima dvostuku nulu po modulu p, što po teoremi 1.8 znači da $p \mid n$. □

Posledica. *Neka su m, n dva prirodna broja, i p prost broj takav da $p \nmid mn$. Tada $\Phi_m(x)$ i $\Phi_n(x)$ ne mogu oba biti deljiva sa p za istu vrednost broja x.*

Dokaz. Ukoliko bi važilo $p \mid \Phi_m(x)$ i $p \mid \Phi_n(x)$, za neko x, tada bi polinom $x^{mn} - 1$ imao dvostruku po modulu p, odakle bi po teoremi 1.8 važilo da $p \mid mn$, što je nemoguće. □

Sledeća lema je usko povezana sa prethodnom.

Lema 6. *Neka su m i n prirodni brojevi, i p prost broj koji ne deli nijedan od njih. Tada u $\mathbb{Z}_p$ važi $(\Phi_n(x), \Phi_m(x)) = 1$.*

Dokaz. Pretpostavimo da je $(\Phi_n(x), \Phi_m(x)) = g(x) \neq 1$. Kako $\Phi_n(x)\Phi_m(x) \mid x^{mn} - 1$, to bi značilo da $g(x)^2 \mid x^{mn} - 1$, što je, na osnovu posledice teoreme 1.7 u $\mathbb{Z}_p$, nemoguće. □

Definicija 7. *Poredak broja a po modulu p, je najmanji broj t, takav da važi: $a^t \equiv 1 \pmod{p}$, i označava se kao $ord_p(a)$.*

Teorema 2.8. *Neka je p prost broj. Tada za sve prirodne brojeve n, i cele brojeve a, pri čemu je $(n, p) = 1$, važi ekvivalencija $p \mid \Phi_n(a) \Leftrightarrow ord_p(a) = n$.*

Dokaz. Dokaz ćemo sprovesti indukcijom. Očigledno je tvrdjenje tačno za $n = 1$, jer je $\Phi_1(x) = x - 1$. Pretpostavimo da tvrdjenje važi za svako $k < n$, i dokažimo da važi i za n.

$\Rightarrow$ Pretpostavimo da za neko a važi $p \mid \Phi_n(a)$. Tada je $a^n \equiv 1 \pmod{p}$. Pretpostavimo da je $ord_p(a) = k \neq n$. Tada iz induktivne hipoteze imamo $\Phi_k(a) \equiv 0$

(mod p). Medjutim, tada je $\Phi_n(a) \equiv \Phi_k(a) \equiv 0 \pmod{p}$, a pošto $k \mid n$, to po lemi 5 sledi da $p \mid n$. Kontradikcija.

$\Leftarrow$ Neka je $ord_p(a) = n$. Tada $0 \equiv a^n - 1 \equiv \prod_{k|n} \Phi_k(a) \pmod{p}$ pa sledi da $p \mid \Phi_k(x)$ za neko $k \mid n$. Medjutim, ne može to biti neko $k < n$, jer bi tada važilo $p \mid a^k - 1$, što je nemoguće. Dakle, $k = n$, i time je i drugi smer pokazan. □

Teorema 2.9. *Neka je n prirodan broj, i x ceo broj. Tada za svaki prost delilac p, polinoma $\Phi_n(x)$ važi ili $p \equiv 1 \pmod{n}$, ili $p \mid n$.*

Dokaz. Ako $p \mid \Phi_n(x)$, tada $p \nmid x$. Zaista, to je zbog $p \mid \Phi_n(x) \mid x^n - 1$. Neka je $k = ord_p(x)$. Pošto $p \mid x^n - 1$, to je $x^n \equiv 1 \pmod{p}$, pa $k \mid n$:

i)$k = n$.Tada pošto iz Male Fermaove teoreme važi: $x^{p-1} \equiv 1 \pmod{p}$, to $n \mid p - 1 \Leftrightarrow p \equiv 1 \pmod{n}$

ii)$k < n$ Pošto važi:

$$0 \equiv x^k - 1 = \prod_{d|k} \Phi_d(x) \pmod{p}$$

sledi da za neko $d \mid k$ važi: $p \mid \Phi_d(x)$. Medjutim, pošto $d \mid k \mid n$, to iz leme 5 sledi $p \mid n$. □

Lema 7. *Neka su a i b prirodni brojevi, i x ceo broj. Tada važi:*

$$(x^a - 1, x^b - 1) = \left|x^{(a,b)} - 1\right|$$

Neka je $T = (x^a - 1, x^b - 1)$ i $t = (a, b)$. Pošto $x^t - 1 \mid x^a - 1$, i $x^t - 1 \mid x^b - 1$ to $x^t - 1 \mid T$.

Očigledno $(x, T) = 1$. Neka je $ord_T(x) = d$. Tada $d \mid a$, i $d \mid b$, pa $d \mid t$. Sledi $T \mid x^d - 1 \mid x^t - 1$. Pošto $x^t - 1 \mid T$ i $T \mid x^t - 1$ to je $T = |x^t - 1|$.

Teorema 2.10. *Neka su a i b prirodni brojevi. Pretpostavimo da za neko x važi $(\Phi_a(x), \Phi_b(x)) > 1$. Tada je a/b stepen prostog broja.*

Dokaz. Pretpostavimo da je prost broj p deli i $\Phi_a(x)$ i $\Phi_b(x)$. Pokazaćemo da je tada a/b stepen broja p tj. ako je $a = p^\alpha A$, i $b = p^\beta B$, pokazaćemo da je $A = B$.

Kako $p \mid \Phi_a(x) \mid x^a - 1$ to je $(x, p) = 1$. Pokažimo da $p \mid \Phi_A(x)$.

Ako je $\alpha = 0$, onda smo gotovi, a u suprotnom iz posledice teoreme 2.4 važi:

$$0 \equiv \Phi_a(x) = \Phi_{p^\alpha A} = \frac{\Phi_A(x^{p^\alpha})}{\Phi_A(x^{p^{\alpha-1}})} \pmod{p},$$

pa $p \mid \Phi_A(x^{p^\alpha})$. Medjutim $x^{p^\alpha} \equiv x \cdot x^{p^\alpha - 1} \equiv x \cdot x^{p-1} \equiv x \pmod{p}$. Odatle sledi:

$$0 \equiv \Phi_A(x^{p^\alpha}) \equiv \Phi_A(x) \pmod{p}$$

Slično, $p \mid \Phi_B(x)$.

Pretpostavimo $A > B$, i neka je $t = (A, B)$, $t < A$. Pošto $p \mid \Phi_A(x) \mid x^A - 1$, i $p \mid \Phi_B(x) \mid x^B - 1$, to $p \mid (x^A - 1, x^B - 1)$, tj. iz leme 7 sledi $p \mid x^t - 1 = \prod_{d|t} \Phi_d(x)$.

Dakle, postoji delilac d broja t, takav da $p \mid \Phi_d(x)$. Medjutim $d \mid t \mid A$ i $p \mid \Phi_A(x)$, pa po lemi 5 sledi $p \mid A$. Kontradikcija. Dakle, $A = B$, i odatle sledi tvrdjenje. □

3 Žigimondijeva teorema

Ova teorema je verovatno dobro poznata takmičarima, medjutim, ona se smatra neelementarnom, i njeni dokazi su najčešće komplikovani. Ciklotomičnim polinomima, dokaz je značajno jednostavniji. Ovde će biti predstavljen specijalan slučaj teoreme koji je podesniji za ciklotomične polinome, mada ce biti govora i o generalizaciji.

Teorema 3.1 (Žigmondijeva teorema)**.** *Neka su a i n prirodni brojevi veći od 1. Tada postoji prost delilac q od $a^n - 1$ takav da q ne deli $a^j - 1$ za sve j, $0 < j < n$, sa sledećim izuzecima:*

(1) $n = 2$, $a = 2^s - 1$, gde je $s \geq 2$, i

(2) $n = 6$, $a = 2$.

Prvo preformulišimo teoremu, da bi je lakše dokazali. Tvrdjenje je ekvivalentno sa tim da za svako $a, n > 1$ možemo naći prost broj p takav da je $ord_p(a) = n$. Na osnovu tepreme 2.8, možemo zaključiti da je dobra ideja posmatrati $\Phi_n(a)$.

Lema 8. *Neka su $a, n > 1$ prirodni brojevi. Pretpostavimo da su svi prosti delioci od $\Phi_n(a)$ takodje i delioci broja n. Tada je $\Phi_n(a)$ prost broj koji deli n, ili je $n = 2$.*

Dokaz. Uzmimo proizvoljno p takvo da $p \mid \Phi_n(a)$. Jasno je da je $(p, a) = 1$ zato što je konstantan član u $\Phi_n(x)$ jedinica. Neka je $k = ord_p(a)$.

Na osnovu teoreme 2.8 imamo da važi $p \mid \Phi_k(a)$. Po teoremi 2.9 važi $n/k = p^t$ for za neki prirodan broj t (dakle, $p \mid n$). Dalje je:

$$x^n - 1 = \Phi_n(x) \cdot Q(x).$$

za neki polinom Q. Lako je videti da $(x^{n/p} - 1) \mid Q(x)$. Na osnovu LTE (videti [7]), imamo da ako je p neparan prost broj tada je $v_p(a^n - 1) = v_p(a^{n/p} - 1) + 1$ jer $p \mid a^k - 1$, a jasno je da $k \mid n/p$, pošto je $(k, p) = 1$ (zato što $p - 1 \mid k$). Dakle, $v_p(\Phi_n(a)) = 1$. Neka su p, q prosti brojevi takvi da $p, q \mid n$, tj. $n = p^{a_1} k_1 = q^{a_2} k_2$ gde je $k_1 = ord_p(a)$ i $k_2 = ord_q(a)$.

Primetimo da $\frac{n}{p^{a_1}} \mid p-1$ i $\frac{n}{q^{a_2}} \mid q-1$. Ali tada sledi da $q \mid (p-1)$ i $p \mid (q-1)$, iz čega sledi da $q \leq p-1, p \leq q-1$ što je nemoguće! Odatle sledi da n ima najviše jedan prost faktor, i ako je neparan, onda je $\Phi_n(a)$ prost.

Pretpostavimo da $2 \mid \Phi_n(a)$. Tada je očigledno da je $k=1$ pa sledi da je $n=2^t$. Ali tada se indukcijom lako pokazuje da je $\Phi_{2^t}(a) = a^{2^{t-1}} + 1 \equiv 2 \pmod 4$ kada $n \neq 2$. Dakle, kada $n \neq 2$ važi $4 \nmid \Phi_n(a)$, odakle sledi tvrdjenje. □

Lema 9. *Neka su $a, n > 1$ prirodni brojevi. Neka je $n = p^k r$ gde $p \nmid r$. Tada imamo $\Phi_n(a) > (b^{p-2}(b-1))^{\varphi(r)}$ gde je $b = a^{p^{k-1}}$.*

Dokaz. Na osnovu teoreme 2.5 imamo:

$$\Phi_n(a) = \frac{\Phi_r(b^p)}{\Phi_r(b)}$$

Lako je pokazati da je $\Phi_r(b^p) > (b^p-1)^{\varphi(r)}$ zato što je b^p za bar b^p-1 veće od bilo kog korena polinoma $\Phi_r(x)$. Slično, može se pokazati da je $\Phi_r(b) < (b+1)^{\varphi(r)}$. Odatle sledi da je:

$$\Phi_n(a) \geq \left(\frac{b^p-1}{b+1}\right)^{\varphi(r)}$$

Ako iskoristimo $b^p - 1 \geq b^{p-2}(b^2-1)$, dobijamo traženi rezultat. □

Dokaz teoreme. Lako je videti da teorema ne važi u navedenim izuzecima. Ako je $n=2$ teorema se trivijalno proverava (i utvrdjuje izuzetak), pa pretpostavimo da je $n > 2$. Ako pretpostavimo da ne postoji takav prost broj q, za koje je $ord_q(a) = n$, tada na osnovu leme 8 važi da je $\Phi_n(a) = p$ za neki prost broj p. Zaista, ne može da važi $q \mid \Phi_n(a)$, i $q \nmid n$, za neki prost broj q, jer bi to, na osnovu teoreme 2.8 značilo $ord_q(a) = n$, što je očigledno nemoguće.

Neka je $n = p^k r$. Na osnovu leme 9 imamo:

$$p > (b^{p-2}(b-1))^{\varphi(r)}$$

gde je $b = a^{p^{k-1}}$. Ako je $p \geq 5$ tada važi $b^{p-2} > p$ za sve cele brojeve b pa je potrebno proveriti $p = 3$. Ali tada je $a = 2, k = 1, r = 1$ ili $r = 2$. Odavde imamo slučajeve $n = 3$ ili $n = 6$. Slučaj $n = 3$ se lako proverava da važi, dok slučaj $a = 2, n = 6$ smo utvrdili da spada u izuzetke. Dakle, teorema važi za sve a, n pa je dokaz zavtšen. □

Posledica 3.2. *Neka su a i n prirodni brojevi veći od 1. Tada postoji prost delilac q od $a^n + 1$ takav da q ne deli $a^j + 1$ za sve j, $0 < j < n$, sa izuzetkom $n = 3$ i $a = 2$.*

Napomena. *Ova posledica se smatra drugim delom Žigimondijeve teoreme.*

Dokaz. Posmatrajmo neki prirodan broj $n > 1$. Neka je p prost broj takav da je $ord_p(a) = 2n$ (koji prema Žigimondijevoj teoremi sigurno postoji). Tada mora važiti $p \mid a^n + 1$, i takodje ne postoji $j < n$, takvo da $p \mid a^j + 1$, jer bi tada važilo i $p \mid a^{2j} - 1$, pri čemu je $2j < 2n$. Kontradikcija. Proverom za one vrednosti broja $2n$ koji su izuzeci u Žigimondijevoj teoremi, dobijamo da su $n = 3$ i $a = 2$ takodje izuzeci i u ovoj posledici. □

3.1 Primeri

Sledećih nekoliko primera je uzeto sa takmičenja širom sveta, i iako se smatraju ozbiljnim problemima, uz znanje Žigimondijeve teoreme, postaju mahom trivijalni. Za zainteresovane, izvori ovih zadataka se mogu videti u [9]. Treba napomenuti, ipak, da je pogršno nadati se da će Žigimondijeva teorema odmah rešiti problem, već je treba koristiti kao moćan alat koji može biti itekako koristan u samom rešenju. Najčešće nalazi primenu u razmatranju raznih podslučaja u okviru nekog ozbiljnog zadatka.

Primer 1. *Naći sve petorke (a, n, p, q, r) prirodnih brojeva koje zadovoljavaju jednačinu:*

$$a^n - 1 = (a^p - 1)(a^q - 1)(a^r - 1)$$

Rešenje. Ako je $a = 1$, tada sve petorke $(1, n, p, q, r)$ zadovoljavaju jednačinu.

Ako je $n > p, q, r$ $(a \neq 1)$ tada prema Žigimondijevoj teoremi $a^n - 1$ ima delilac koji ne deli nijedan od cinilaca sa desne strane naše jednačine. Zbog izuzetaka u teoremi imamo dva moguća podslučaja:

a) $n = 2$, $a = 2^s - 1 (s \geq 2)$: Tada mora biti $p = q = r = 1$. Zamenom ovih vrednosti u jednačinu dobijamo da je $a = 3$. Dakle, i petorka $(3, 2, 1, 1, 1)$ je rešenje.

b) $n = 6$, $a = 2$: Jednostavnom proverom po deliocima broja $63 (= 2^6 - 1)$ dobijamo rešenja: $(2, 6, 2, 2, 3)$, $(2, 6, 2, 3, 2)$, $(2, 6, 3, 2, 2)$.

Neka bar za jedan od p, q, r važi da je jednak n, npr. $p = n$. Tada je $(a^q - 1)(a^r - 1) = 1$, tj. $a = 2, q = 1, r = 1$. Analogno tome, dobijamo još dva rešenja, ako uzmemo da su, redom, q i r jednaki sa n. Dakle, rešenja su i petorke $(2, n, n, 1, 1)$, $(2, n, 1, n, 1)$, $(2, n, 1, 1, n)$, za proizvoljan prirodan broj n. □

Primer 2. *Naći sve trojke prirodnih brojeva (a, m, n), takvih da za njih važi:*

$$a^m + 1 \mid (a + 1)^n$$

Rešenje. Ako je $a, m > 1$, tada na osnovu posledice 3.2 postoji prost broj p, koji deli $a^m + 1$, a ne deli $a + 1$, i samim tim ni $(a + 1)^n$. Izuzeci su $m = 3$, $a = 2$, i proverom vidimo su sve trojke $(2, 3, n)$ rešenje zadatka, kada je $n \geq 2$. Ako je $a = 1$, ili $m = 1$, dobijamo nova rešenja: $(1, m, n)$, $(a, 1, n)$, gde su m, n, tj. a, n proizvoljni prirodni brojevi. □

Primer 3. *Naći sve četvorke prirodnih brojeva,*(x, r, p, n) *takvih da je* p *prost broj,* $n, r > 1$*, i važi:*

$$x^r - 1 = p^n$$

Rešenje. Očigledno je $x > 1$, pa prema Žigimondijevoj teoremi $x^r - 1$ ima delilac koji ne deli $x - 1$, pa samim tim ima sigurno bar dva prosta delioca, što je kontradikcija sa uslovom zadatka, osim za izuzetke u Žigimondijevoj teoremi. Ako je $x = 2$ i $r = 6$, tada jednačina nema rešenja, dok za $r = 2$, $x = 2^s - 1$, imamo da je $p = 2$, pa odatle važi: $(2^s - 1)^2 - 1 = 2^n$ tj. $2^{s-1} - 1 = 2^{n-s-1}$, odakle imamo $s = 2 \Leftrightarrow x = 3$, $n = 3$. Dakle, jedino rešenje je četvorka: $(x, r, p, n) = (3, 2, 2, 3)$. □

Primer 4. *Naći sve trojke prirodnih brojeva,*(x, y, p) *takvih da je* p *prost broj i važi:*

$$p^x - y^p = 1$$

Rešenje. Slično prethodnom zadatku znamo da za $y, p > 1$ broj $y^p + 1$ ima bar dva različita prosta delioca, što je moguće samo za izuzetke iz posledice 3.2, tj. $y = 2$, $p = 3$, i tada je $x = 2$. Kada je $y = 1$, tada se lako dobija $p = 2$, $x = 1$. □

Primer 5. *Neka su* a, b *prosti brojevi, takvi da je* $a > b > 2$*. Dokazati da* $2^{ab} - 1$ *ima bar tri različita prosta delioca.*

Rešenje. Očigledno je da $2^a - 1 \mid 2^{ab} - 1$ i $2^b - 1 \mid 2^{ab} - 1$. Pošto je $ab > 6$, to $2^{ab} - 1$ ima prost delilac koji ne deli ni $2^a - 1$ ni $2^b - 1$. Takodje, i $2^a - 1$ ima delilac koji ne deli $2^b - 1$, a i sam $2^b - 1$ ima bar jedan prost delilac. Time je tvrdjenje zadatka zadovoljeno. □

Primer 6. *Rešiti jednačinu* $5^x - 3^y = z^2$ *u skupu prirodnih brojeva.*

Rešenje. Razmatrajući $\pmod 3$ i $\pmod 4$, dobijamo da su x i y parni brojevi, a iz samog zadatka vidimo da je to i z. Imamo dakle da važi $3^{2y_0} = 5^{2x_0} - z^2 = (5^{x_0} - z)(5^{x_0} + z)$. Kako važi:

$$(5^{x_0} - z, 5^{x_0} + z) = (5^{x_0} - z, 2z) = (5^{x_0} - z, z) = (5^{x_0}, z) = 1$$

to je $5^{x_0} - z = 1$, i $5^{x_0} + z = 3^{2y_0}$. Sabiranjem ovih jednačina dobijamo da je $2 \cdot 5^{x_0} = 3^{2y_0} + 1$. Ako je $y_0 = 1$ tada dobijamo $x_0 = 1$, tj. $(x, y, z) = (2, 2, 4)$ je jedno rešenje zadatka. Ako je $y_0 > 1$, tada prema posledici 3.2, $3^{2y_0} + 1$ ima delilac koji ne deli $3^2 + 1 = 10$, tj. delilac različit od 2 i 5. Iz te kontradikcije sledi da nema više rešenja početne jednačine. □

Napomena. *Navešćemo sada, bez dokaza, već navedenu generalizaciju, tj. punu formu Žigimondijeve teoreme, kao i par primera koji ilustruju njenu primenu. Lako se primeti da su naredni kao i prethodni primeri svi vodjeni istom idejom, ali su stavljeni u tolikom broju da bi razvili rutinu kod čitalaca koji su vodjeni takmičarskim ambicijama.*

Teorema 3.3. *Neka su a ,b i n prirodni brojevi takvi da je $n > 1$, $a > b > 0$. Tada postoji prost delilac q od $a^n - b^n$ takav da q ne deli $a^j - b^j$ za sve j, $0 < j < n$, sa sledećim izuzecima:*

(1) $n = 2$, $a + b = 2^s$, gde je $s \geq 2$, i

(2) $n = 6$, $a = 2$, $b = 1$.

Slično, i posledica 3.2 ima svoju generalizaciju:

Teorema 3.4. *Neka su a ,b i n prirodni brojevi takvi da je $n > 1$, $a, b > 0$, i $a \neq b$. Tada postoji prost delilac q od $a^n + b^n$ takav da q ne deli $a^j + b^j$ za sve j, $0 < j < n$, sa izuzetkom $n = 3$, $a = 2$ i $b = 1$.*

Primer 7. *Dokazati da niz $a_n = 3^n - 2^n$ $(n \in \mathbb{N})$ ne sadrži tri člana koji čine geometrijsku progresiju.*

Rešenje. Pretpostavimo suprotno. Neka za neke prirodne brojeve x, y, z važi $q(3^x - 2^x) = 3^y - 2^y$, i $q^2(3^x - 2^x) = 3^z - 2^z$. Očigledno je q racionalan broj. Neka je $q = a/b$, gde je $(a, b) = 1$. Dakle, važi $a(3^x - 2^x) = b(3^y - 2^y)$, i $a^2(3^x - 2^x) = b^2(3^z - 2^z)$ $(*)$. Neka je p prost broj koji deli a_z, a ne deli a_x i a_y. Tada iz druge jednačine u $(*)$ važi $p \mid a$, ali tada da bi prva bila zadovoljena mora da $p \mid b$. Dakle, imamo kontradikciju za sve vrednosti x, y, z, jer 3 i 2 ne predstavljaju izuzetke u Žigimondijevoj teoremi. □

Primer 8. *Naći sve prirodne brojeve x, y, z koji zadovoljavaju jednačinu $x^{2013} + y^{2013} = z^{2013}$, ako je z prost broj.*

Rešenje. Vidimo da, bez izuzetaka, broj $x^{2013} + y^{2013}$ ima bar dva različita prosta delioca, jer $x + y \mid x^{2013} + y^{2013}$, pa odatle sledi da jednačina nema rešenja. Naravno, ovo je samo specijalan, i krajnje jednostavan slučaj Velike Fermaove teoreme, pa kao takav se odmah moglo zaključiti da neće imati rešenja. □

Konačno, ovu temu zatvaramo sa nekoliko zadataka koji su namenjeni za samostalan rad zainteresovanih čitalaca. Još zadataka iz ove oblasti može se naći u [2] i [10].

1. Naći sve prirodne brojeve x, y za koje važi:

$$7^x - 3 \cdot 2^y = 1$$

2. Naći sve prirodne brojeve x, y, takve da je $3^x 7^y + 1$ kvadrat neparnog broja.
3. Da li postoji prirodan broj n koji je deljiv sa tačno 2000 različitih prostih brojeva, takav da je broj $2^n + 1$ deljiv sa n.
4. Dokazati da postoji beskonačno mnogo prirodnih brojeva n, takvih da $n \mid 2^{2^n+1}+1$, a $n \nmid 2^n + 1$.

4 Primena ciklotomičnih polinoma u zadacima

Prvi zadatak je specijalan slučaj Dirihleove teoreme (videti [8]):

Zadatak 1. *Neka je n prirodan broj. Tada postoji beskonačno mnogo prostih brojeva p, takvih da je $p \equiv 1 \pmod{n}$.*

Rešenje. Za $n = 1$ je tvrdjenje trivijalno. Za $n > 1$ pretpostavimo da postoji konačno mnogo prostih brojeva koji zadovoljavaju uslove zadatka. Neka je T proizvod tih prostih brojeva, kao i prostih brojeva koji dele n. Neka je k dovoljno veliki prirodan broj takav da je $\Phi_n(T^k) > 1$ (pošto je $\Phi_n(x)$ moničan, nekonstantan polinom, takvo k postoji). Neka je tada q prost delilac broja $\Phi_n(T^k)$. Medjutim, tada $q \mid \Phi_n(T^k) \mid T^{kn} - 1$, pa $q \nmid T$, tj. zbog načina na koji je T definisan, to znači da $q \nmid n$, i $q \not\equiv 1 \pmod{n}$. Ali to je na osnovu teoreme 2.9 nemoguće. Iz ove kontradikcije sledi tvrdjenje zadatka. □

Zadatak 2. *Dokazati da nema prostih brojeva u beskonačnom nizu:*

$$10001, 100010001, 1000100010001...$$

Rešenje. Primetimo da je $10001 = 73 \cdot 137$, kao i da je drugi član deljiv sa 3, pa, dakle, nisu prosti. Takodje, vidimo da je svaki član ovog niza oblika $1+10^4+10^8+\cdots+10^{4n}$, pa treba pokazati da je taj broj složen, za svaki prirodan broj n.

Ako je $n+1$ složen broj, tada ako $m+1 \mid n+1$ onda $10^{4(m+1)} - 1 \mid 10^{4(n+1)} - 1$, tj. $1 + 10^4 + 10^8 + \cdots + 10^{4m} \mid 1 + 10^4 + 10^8 + \cdots + 10^{4n}$, pa je u tom slučaju n-ti član niza složen.

Ako je $n+1$ prost broj, tada je $1+10^4+10^8+\cdots+10^{4n} = \frac{10^{4(n+1)}-1}{10^4-1} = \frac{\Phi_{n+1}(10^4)}{\Phi_1(10^4)} = \Phi_{n+1}(10^4)$, što je, po teoremi 2.6, dalje jednako $\Phi_{n+1}(10) \cdot \Phi_{4(n+1)}(10)$, odakle sledi tvrdjenje zadatka. □

Zadatak 3. *Neka su $p_1, p_2, ..., p_n$ različiti prosti brojevi veći od 3. Dokazati da tada broj $2^{p_1 p_2 \cdots, p_n} + 1$ ima bar $2^{2^{n-1}}$ delilaca*

Rešenje. Ovaj zadatak daje mnogo jaču ocenu nego zadatak predložen za medjunarodnu olimpijadu 2002. Tada je trebalo pokazati da broj iz zadatka ima bar 4^n delilaca, i dokaz se služio matematičkom indukcijom.

Dovoljno je pokazati da broj $2^{p_1 p_2 \cdots p_n} + 1$ ima bar 2^{n-1} različitih uzajamno prostih

delilaca. Vidimo da važi:

$$\begin{aligned}(2^{p_1p_2\dots p_n}-1)(2^{p_1p_2\dots p_n}+1) &= 2^{2p_1p_2\dots p_n}-1=\prod_{d|2p_1p_2\dots p_n}\Phi_d(2)\\ &= \left(\prod_{d|p_1p_2\dots p_n}\Phi_d(2)\right)\left(\prod_{d|p_1p_2\dots p_n}\Phi_{2d}(2)\right)\\ &= (2^{p_1p_2\dots p_n}-1)\left(\prod_{d|p_1p_2\dots p_n}\Phi_{2d}(2)\right)\end{aligned}$$

pa sledi da je

$$2^{p_1p_2\dots p_n}+1=\left(\prod_{d|p_1p_2\dots p_n}\Phi_{2d}(2)\right)$$

Iz teoreme 2.10 znamo da ako $\Phi_a(x)$, i $\Phi_b(x)$ nisu uzajamno prosti, tada je a/b stepen prostog broja. Odatle sledi da je dovoljno da pokažemo da je moguće uzeti 2^{n-1} različitih delilaca broja $p_1p_2\cdots p_n$, takvih da količnik nikoja dva nije prost broj. Izbor delilaca broja $p_1p_2\cdots p_n$, koji sami imaju paran broj delilaca očigledno zadovoljava te uslove, i time je dokaz završen. □

Zadatak 4. *Naći sva celobrojna rešenja jednačine*

$$\frac{x^7-1}{x-1}=y^5-1$$

Rešenje. Jednačina je ekvivalentna sa

$$1+x+...+x^6=(y-1)(1+y+y^2+y^3+y^4)$$

Lema 10. *Neka je p prost broj i x ceo broj. Tada svaki prost delilac q polinoma $1+x+...+x^{p-1}$ zadovoljava ili $q\equiv 1 \pmod p$ ili $q=p$.*

Dokaz. Primetimo da je $1+x+...+x^{p-1}=\frac{x^p-1}{x-1}=\Phi_p(x)$. Tvrdjenje dalje sledi iz teoreme 2.9. □

Na osnovu ove leme znamo da svaki prost broj p, koji deli $y-1$ zadovoljava ili $p=7$, ili $p\equiv 1 \pmod 7$, pa zato je i $y-1\equiv 0 \pmod 7$, ili $y-1\equiv 1 \pmod 7$, tj. $y\equiv 1 \pmod 7$ ili $y\equiv 2 \pmod 7$.

Ako je $y\equiv 1 \pmod 7$, tada $1+y+y^2+y^3+y^4\equiv 5\not\equiv 0,1 \pmod 7$.

Ako je $y\equiv 1 \pmod 7$, tada $1+y+y^2+y^3+y^4\equiv 31\equiv 3\not\equiv 0,1 \pmod 7$.

Dakle, jednačina nema celobrojnih rešenja.

□

Zadatak 5. *Neka je p prost broj. Dokazati da postoji prost broj q takav da $q \nmid n^p - p$ za svaki prirodan broj n.*

Rešenje. Primetimo da ako $q \mid n^p - p$, tada $1 \equiv n^{q-1} \equiv p^{\frac{q-1}{p}} \pmod{q}$, pa je dovoljno da pokažemo da postoji prost broj q takav da je poredak broja p po modulu q jednak p, i da $p^2 \nmid q - 1$.

Neka je q prost delilac broja $1 + p + \cdots + p^{p-2} + p^{p-1}$. Tada, kao i u prethodnom zadatku zaključujemo da je $q \equiv 1 \pmod{p}$. Kako $q \nmid p - 1$, to je $ord_q(p) = p$. Pretpostavimo da za svaki ovakav broj q važi $p^2 \mid q - 1$. To, medjutim, povlači da je $1 + p + \cdots + p^{p-2} + p^{p-1} \equiv 1 \pmod{p^2}$, što je nemoguće. Iz ove kontradikcije sledi tvrdjenje zadatka. □

Zadatak 6. *Dokazati da postoji beskonačno mnogo prirodnih brojeva n takvih da nijedan od prostih delilaca broja $n^2 + n + 1$ nije veći od $\sqrt{n}$.*

Rešenje. Pošto samo treba da postoji beskonačno mnogo brojeva n koji zadovoljavaju tvrdjenje, možemo sami da konstruišemo niz takvih brojeva. Gledaćemo brojeve oblika $n = k^m$, gde je $(m, 3) = 1$. Iz teoreme 2.6 imamo da je $\Phi_a(x^n) = \prod_{d \mid n} \Phi_{ad}(x)$ kada je $(a, n) = 1$.

Primetimo da je $n^2 + n + 1 = \Phi_3(k^m)$, pa važi:

$$n^2 + n + 1 = \prod_{d \mid m} \Phi_{3d}(k)$$

Očigledno je da je $(k+1)^{\varphi(3n)} > \Phi_{3n}(k)$, za svako n pošto je $k + 1 > k - \theta$, gde je θ proizvoljni $3n$-ti koren jedinice. Zato želimo da pokažemo da za neko k postoji broj m, takav da je $(k+1)^{\varphi(3m)} < k^{m/2}$, jer bi tada tvrdjenje bilo zadovoljeno, zato što je svaki činilac u proizvodu ne veći od $\sqrt{n}$, što bi značilo da ne postoji prost delilac veći od $\sqrt{n}$.

Kako $\dfrac{\varphi(x)}{x}$ može biti proizvoljno blizu 0, možemo izabrati neko x takvo da je $\dfrac{\varphi(x)}{x} < 0.01$. Ako uzmemo $m = x$ imaćemo $(k+1)^{\varphi(3m)} < (k+1)^{3 \cdot 0.01 \cdot m}$. Tada očigledno imamo da važi $(k+1)^{3 \cdot 0.01 \cdot m} < k^{m/2}$ za dovoljno veliko k, pa smo time završili dokaz. □

Još zadataka iz ove oblasti može se naći u [2].

5 Literatura

[1] Elementary Properties of Cyclotomic Polynomials, *Yimin Ge*
[2] Cyclotomic Polynomials in Olympiad Number Theory,*Lawrence Sun*
[3] On Zsigimondy primes,*Moshe Ritman*,AMERICAN MATHEMATICAL SOCIETY Volume 125, Number 7, July 1997, Pages 19131919
[4] Several proofs of the irreducibility of the cyclotomic polynomials,*Steven H. Weintraub*
[5] http://planetmath.org/perfectfield
[6] http://en.wikipedia.org/wiki/Eisenstein's criterion
[7] Lifting The Exponent Lemma (LTE),*Amir Hossein Parvardi*
[8] Dirichlet's theorem on primes in arithmetic progressions,*Pete L. Clark*
[9] Zsigmondys Theorem, *Andy Loo*, Mathematical excalibur, Volume 16, Number 4, February 2012
[10] The Zsigmondy Theorem, *PISOLVE*