UNIVERZITET U NOVOM SADU
PRIRODNO-MATEMATIČKI FAKULTET
DEPARTMAN ZA
MATEMATIKU I INFORMATIKU

Jovana Tomik Ognjenović

Ciklotomični polinomi

-master rad-

Mentor dr Petar Marković

Novi Sad, 2020.

Sadržaj

Glava 1

Uvod

Ciklotomični polinomi predstavljaju poseban spoj algebre i teorije brojeva. Ovi polinomi imaju lepe osobine, a sa nekima od njih ćemo se upoznati kroz ovaj rad. Da bismo došli do definicije i osobina ciklotomičnih polinoma, potrebno je da se podsetimo pojmova kao što su Mebijusova funkcija, zatim nekih osobina ove funkcije, pojma primitivnog korena, kao i nekih osnovnih osobina polinoma. Svi pojmovi biće uvedeni postupno i osobine će biti dokazane radi lakšeg razumevanja teme. Svi ovi pojmovi će nam koristiti u dokazivanju osobina ciklotomičnih polinoma i njihove nesvodljivosti. U daljem tekstu biće reči i o vezi ciklotomičnih polinoma i poretka broja po prostom modulu, kao i o primeni ciklotomičnih polinoma u dokazivanju poznatih teorema, kao što su Vederburnova i Žigmondijeva teorema.

Glava 2

Osobine polinoma i Mebijusova funkcija

2.0.1 Mebijusova funkcija

Definicija 2.1. Mebijusova funkcija je funkcija definisana za sve prirodne brojeve na sledeći način:

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

Za ovu funkciju važi, ako su m i n uzajamno prosti brojevi, onda je $\mu(mn) = \mu(m)\mu(n)$. Ovu osobinu zvaćemo up-multiplikativnost Mebijusove funkcije i pokazaćemo je. Neka su $\mu(m)$ i $\mu(n)$ definisane na sledeći način:

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

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

Tada je

$$\mu(m)\mu(n) = \begin{cases} 1, & \text{kada su i } m = 1 \text{ i } n = 1; \\ (-1)^{k+l}, & \text{kada ni } m \text{ ni } n \text{ nisu deljivi potpunim} \\ & \text{kvadratom, tj. } mn \text{ nije deljiv potpunim} \\ & \text{kvadratom, jer je NZD}(m,n)=1; \\ 0, & \text{inače.} \end{cases}$$

što je baš $\mu(mn)$.

Primer 2.1. Izračunati vrednosti Mebijusove funkcije za prirodne brojeve 1036, 1001 i 22.

$\mu(1036) = \mu(2^2 \cdot 7 \cdot 37)$ Kako je 1036 deljivo potpunim kvadratom (kvadratom broja 2), onda je $\mu(1036) = 0$

$\mu(1001) = \mu(7 \cdot 11 \cdot 13) = \mu(7)\mu(11)\mu(13) = (-1)^1 \cdot (-1)^1 \cdot (-1)^1 = (-1)^3 = -1$

$\mu(22) = \mu(2 \cdot 11) = \mu(2)\mu(11) = (-1)^2 = 1$

Teorema 2.1. *Za svaki prirodan broj $n > 1$ važi da je*

$$\sum_{d|n} \mu(d) = 0$$

gde je $\mu(n)$ Mebijusova funkcija.

Dokaz. Neka je broj n faktorisan tako da je $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_s^{\alpha_s}$ gde su p_i prosti brojevi, a $\alpha_i > 0$ prirodni brojevi. U zbiru $\sum_{d|n} \mu(d)$ nenula vrednosti imaju oni sabirci $\mu(d)$, gde je d delilac broja n koji je oblika $d = p_1^{\beta_1} p_2^{\beta_2} ... p_s^{\beta_s}$ gde je $0 \leq \beta_i \leq 1$, jer ako je neko $\beta_j \geq 2$ onda je d deljivo potpunim kvadratom, pa je $\mu(d) = 0$. Iz up-multiplikativnosti Mebijusove funkcije μ znamo da je $\mu(d) = \mu(p_1^{\beta_1} p_2^{\beta_2} ... p_s^{\beta_s}) = \mu(p_1^{\beta_1})\mu(p_2^{\beta_2}) ... \mu(p_s^{\beta_s})$ i $\mu(1) = 1$ i $\mu(p_i) = (-1)^1 = -1$. Takođe znamo da je

$$\sum_{d|n} \mu(d) = \sum_{0 \leq \beta_i \leq 1} \mu(p_1^{\beta_1})\mu(p_2^{\beta_2}) ... \mu(p_s^{\beta_s}) =$$
$$(\mu(1) + \mu(p_1))(\mu(1) + \mu(p_2)) ... (\mu(1) + \mu(p_s)) = 0 \cdot 0 ... 0 = 0$$

jer znamo da je $\mu(p_i^{\beta_i}) = \mu(p_i)^{\beta_i}$, za proste brojeve p_i i $0 \leq \beta_i \leq 1$. □

Sada ćemo dokazati teoremu poznatu kao Mebijusova formula inverije.

Teorema 2.2. *Neka su funkcije f i F definisane na skupu prirodnih brojeva i neka je*

$$F(n) = \sum_{d|n} f(d) \text{ za svako } n \in N.$$

Tada je

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

Dokaz. Izračunaćemo sumu $\sum_{d|n} \mu(d) \cdot F\left(\frac{n}{d}\right)$ uzimajući u obzir ono što smo malopre dokazali, da je $\sum_{d|n} \mu(d) = 0$ kada je $n > 1$.
Neka je $n = d_1 \cdot d_2$ gde je $d_2 = \frac{n}{d_1}$ za svaki delilac d_1 broja n. Tada će tražena suma biti jednaka $\sum_{d|n} \mu(d) \cdot F\left(\frac{n}{d}\right) = \sum_{n=d_1 \cdot d_2} \mu(d_1) \cdot F(d_2)$. Iz definicije funkcije F znamo da je to dalje jednako

$$\sum_{n=d_1 \cdot d_2} \mu(d_1) \cdot F(d_2) = \sum_{n=d_1 \cdot d_2} \mu(d_1) \cdot \left(\sum_{d_3|d_2} f(d_3) \right) = \sum_{\substack{n=d_1 \cdot d_2 \\ d_3|d_2}} \mu(d_1) \cdot f(d_3).$$

Pregrupisavanjem sabiraka u zbiru imamo sledeću jednakost

$$\sum_{\substack{n=d_1 \cdot d_2 \\ d_3|d_2}} \mu(d_1) \cdot f(d_3) = \sum_{d_3|n} f(d_3) \cdot \left(\sum_{d_1|\frac{n}{d_3}} \mu(d_1) \right).$$

Prema teoremi 2.1 , $\sum_{d_1|\frac{n}{d_3}} \mu(d_1) = 0$ za sve $\frac{n}{d_3} > 1$, a jednaka jedinici kada je $\frac{n}{d_3} = 1$, tj. kada je $n = d_3$. Na osnovu ovoga nam u konačnoj sumi ostaje samo sabirak kada je $n = d_3$, tj. $\sum_{n|n} f(n) \cdot \sum_{d_1|1} \mu(d_1)$, što je $f(n)$. Time je dokaz završen. □

U slučaju kada je $f(n)$ Ojlerova funkcija $\varphi(n)$, na osnovu ove teoreme, dobijamo da je

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

jer je $n = \sum_{d|n} \varphi(d)$.

U sledećem primeru ćemo izračunati vrednosti Ojlerove funkcije φ koristeći formulu

$$\varphi(n) = n\left(1 - \tfrac{1}{p_1}\right)\left(1 - \tfrac{1}{p_2}\right)...\left(1 - \tfrac{1}{p_k}\right),$$

za $n = p_1^{\alpha_1}...p_k^{\alpha_k}$.

Primer 2.2. Izračunati vrednosti Ojlerove funkcije za brojeve 57 i 342.

$\varphi(57) = \varphi(3 \cdot 19) = 57 \cdot (1 - \frac{1}{3})(1 - \frac{1}{19}) = 3 \cdot (1 - \frac{1}{3}) \cdot 19 \cdot (1 - \frac{1}{19}) = 2 \cdot 18 = 36$

$\varphi(342) = \varphi(2 \cdot 3^2 \cdot 19) = 342 \cdot (1 - \frac{1}{2})(1 - \frac{1}{3})(1 - \frac{1}{19}) = 2 \cdot (1 - \frac{1}{2}) \cdot 9 \cdot (1 - \frac{1}{3}) \cdot 19 \cdot (1 - \frac{1}{19}) = 1 \cdot 6 \cdot 18 = 108.$

Teorema 2.3. *Neka su funkcije f i F definisane na skupu prirodnih brojeva i neka je funkcija $F(n)$ takva da važi jednakost*

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

Tada je

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

Dokaz. Definisaćemo dve pomoćne funkcije $g(n) = \ln f(n)$ i $G(n) = \ln F(n)$ za svako n. Tada će

$$G(n) = \ln F(n) = \ln\left(\prod_{d|n} f(d)\right) = \sum_{d|n} \ln f(d) = \sum_{d|n} g(d) \text{ za svako } n.$$

Prema teoremi 2.2 važi da je $g(n) = \sum_{d|n} \mu(d) G\left(\frac{n}{d}\right)$. Dalje je

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

Dakle, $g(n)=\ln\prod_{d|n}F\left(\frac{n}{d}\right)^{\mu(d)}$ tj. $\ln f(n)=\ln\prod_{d|n}F\left(\frac{n}{d}\right)^{\mu(d)}$, odnosno

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

2.0.2 Kompleksni primitivni koreni

U ovom odeljku ćemo definisati pojam n-tog korena i primitivnog n-tog korena jedinice, a potom videti koliko takvih korena postoji i koliki je zbir svih primitivnih n-tih korena jedinice.

Definicija 2.2. Neka je n prirodan broj. Kompleksni broj ε nazivamo n-tim korenom jedinice ako zadovoljava jednakost

$$\varepsilon^n=1.$$

Primer 2.3. Pokazati da su rešenja jednačine $x^n-1=0$

$$x_k=\cos\tfrac{2k\pi}{n}+i\cdot\sin\tfrac{2k\pi}{n}\ ,\ k=0,1,...,n-1.$$

Rešenja jednačine x_k računamo primenom Moavrove formule

$$x_k^n=(\cos\tfrac{2k\pi}{n}+i\cdot\sin\tfrac{2k\pi}{n})^n=\cos\tfrac{n\cdot 2k\pi}{n}+i\cdot\sin\tfrac{n\cdot 2k\pi}{n}=\cos 2k\pi+i\cdot\sin 2k\pi=\cos 2k\pi=1$$

što znači da x_k jesu nule datog polinoma, a da su to i jedine nule garantuje nam Osnovna teorema algebre koja kaže da polinom sa kompleksnim koeficijentima n-tog stepena ima tačno n nula, računajući i njihovu višestrukost.

Primer 2.4. Još jedan zanimljiv primer je način geometrijske interpretacije skupa nula polinoma x^n-1.
Pokazali smo da su sve nule ovakvog polinoma oblika $x_k=\cos\frac{2k\pi}{n}+i\cdot\sin\frac{2k\pi}{n}$, $k=0,1,...,n-1$. Kako je moduo svake nule polinoma

$$\sqrt{(\cos\frac{2k\pi}{n})^2+(\sin\frac{2k\pi}{n})^2}=1,$$

znamo da se sve nule nalaze na jediničnoj kružnici. Znamo i to da je rastojanje između susednih nula konstantno, odnosno da važi

$$|x_k - x_{k-1}| = |\cos\tfrac{2k\pi}{n} + i\cdot\sin\tfrac{2k\pi}{n} - \cos\tfrac{2(k-1)\pi}{n} - i\cdot\sin\tfrac{2(k-1)\pi}{n}| =$$
$$|(\cos\tfrac{2k\pi}{n} - \cos\tfrac{2(k-1)\pi}{n}) + i\cdot(\sin\tfrac{2k\pi}{n} - \sin\tfrac{2(k-1)\pi}{n})| =$$
$$\sqrt{(\cos\tfrac{2k\pi}{n} - \cos\tfrac{2(k-1)\pi}{n})^2 + (\sin\tfrac{2k\pi}{n} - \sin\tfrac{2(k-1)\pi}{n})^2} =$$
$$\sqrt{(-2\sin\tfrac{\pi}{n}\sin\tfrac{(2k-1)\pi}{n})^2 + (2\sin\tfrac{\pi}{n}\cos\tfrac{(2k-1)\pi}{n})^2} =$$
$$\sqrt{(2\sin\tfrac{\pi}{n})^2((\sin\tfrac{(2k-1)\pi}{n})^2 + (\cos\tfrac{(2k-1)\pi}{n})^2)} = \sqrt{(2\sin\tfrac{\pi}{n})^2} = 2\sin\tfrac{\pi}{n}.$$

Kako je jedna nula sigurno $x_0 = 1$ i kako znamo rastojanje između susednih nula, lako ih ucrtavano na jediničnoj kružnici.

Definicija 2.3. Neka je ε n-ti koren jedinice, za proizvoljan prirodan broj n. Tada najmanji prirodan broj k za koji važi da je $\varepsilon^k = 1$ nazivamo redom broja ε i označavamo ga sa $ord(\varepsilon)$.

Sledeća lema pokazuje nam vezu između reda broja ε i broja n.

Lema 2.4. *Neka je n prirodan broj i ε proizvoljan n-ti koren jedinice. Tada za neki ceo broj k važi $\varepsilon^k = 1$ ako i samo ako $ord(\varepsilon)$ deli k. Specijalno, $ord(\varepsilon)$ deli n.*

Dokaz. Neka je $d = ord(\varepsilon)$.
($\Rightarrow$) Neka je sada $\varepsilon^k = 1$ i neka je $k = qd + c$, gde je $0 \leq c \leq d-1$. Kako je $1 = \varepsilon^k = \varepsilon^{qd+c} = (\varepsilon^d)^q\varepsilon^c = \varepsilon^c$, zaključujemo da je $\varepsilon^c = 1$, pa kako je $c < d$, a d je najmanji prirodan broj za koji važi da je $\varepsilon^d = 1$, dobijamo da je $c = 0$, tj. $k = qd$. Dakle, $ord(\varepsilon)$ deli k.
($\Leftarrow$) Ako $d|k$, onda važi da je $\varepsilon^k = (\varepsilon^d)^{\frac{k}{d}} = 1^{\frac{k}{d}} = 1$, čime je dokaz završen. □

Posledica 2.5. *Neka je n prirodan broj, ε proizvoljan n-ti koren iz jedinice, k neki ceo broj za koji važi da je $\varepsilon^k = 1$ i $d = ord(\varepsilon)$. Tada je $\varepsilon^k = \varepsilon^l$ ako i samo ako je $k \equiv_d l$. Specijalno, za $1 \leq k, l \leq d$ važi da je $k = l$.*

Sada ćemo definisati primitivni n-ti koren jedinice, pošto nam on treba za definiciju ciklotomičnih polinoma.

Definicija 2.4. Neka je n prirodan broj i ε n-ti koren iz jedinice. Ako je $ord(\varepsilon) = n$, onda ε nazivano primitivnim n-tim korenom jedinice.

Definicija 2.5. Neka je a ceo broj i n prirodan broj, pri čemu su a i n uzajamno prosti brojevi. Najmanji prirodan broj t za koji važi da je $a^t \equiv 1$ $(mod\ n)$ naziva se red ostatka a po modulu n i obeležavamo ga sa $o_n(a)$.

Definicija 2.6. Ceo broj θ je primitivni koren po modulu n ako je red ostatka broja θ po modulu n jednak $\varphi(n)$, tj. $o_n(\theta) = \varphi(n)$.

Primer 2.5. Odrediti primitivne korene po modulu 23 i 8.

Za prost broj 23 imamo 22 uzajamno prosta broja sa 23, koja nisu veća od 23. Kako je $22 = 2 \cdot 11$, treba da odredimo elemente reda 2 i 11 u grupi 1,2,...,22. Kako za prvi element mora važiti

$$x^2 \equiv 1 \ (mod\ 23) \text{ i nije } x \equiv 1 \ (mod\ 23)$$

što zbog $x^2 - 1 = (x-1)(x+1)$ daje $x + 1 \equiv 0 \ (mod\ 23)$. Dakle, to je broj 22. Sledeći broj mora imati red 11, tj.

$$x^{11} \equiv 1 \ (mod\ 23).$$

Proverom dobijamo da su rešenja 1,2,3,4,6,8,9,12,13 i 16. Izbacujemo 1 jer je reda 1, a preostale vrednosti množimo sa prvim elementom, tj. 22, i dobijamo sledeće primitivne korene 7,10,11,14,15,17,19,20,21.

Za složen broj 8 imamo 4 uzajamno prosta broja sa njim, a to su 1,3,5 i 7. Kako je $8 = 2^4$ tražimo elemente reda 2. Kako mora $x^2 \equiv 1 \ (mod\ 8)$ i nije $x \equiv 1 \ (mod\ 8)$ imamo da

$$3^2 \equiv 1 \ (mod\ 8)$$

$$5^2 \equiv 1 \ (mod\ 8)$$

$$7^2 \equiv 1 \ (mod\ 8)$$

sledi da 3, 5 i 7 nisu primitivni koreni po modulu 8, jer je $\varphi(8) = 4$, a $2 < 4$. Dakle, broj 8 nema primitivne korene.

Primitivni koren po modulu n postoji samo za određene brojeve n, što je određeno sledećom teoremom. Teoremu dajemo bez dokaza.

Teorema 2.6. *Primitivni koren po modulu n postoji ako i samo ako je* $n = 2$, $n = 4$, $n = p^k$ *ili* $n = 2p^k$, *gde je p neparan prost broj, a k bilo koji prirodan broj.*

Lema 2.7. *Neka je* ε *primitivni n-ti koren jedinice. Tada je skup* $\varepsilon, \varepsilon^2, ..., \varepsilon^n$, *skup svih n-tih korena iz jedinice.*

Dokaz. Kako je ε primitivni n-ti koren jedinice, znamo da važi $\varepsilon^n = 1$. Dalje, kako je $(\varepsilon^k)^n = (\varepsilon^n)^k = 1^k = 1$, onda je i ε^k n-ti koren jedinice. Pošto su svi $\varepsilon, \varepsilon^2, ..., \varepsilon^n$ međusobno različiti brojevi, što se može zaključiti iz posledice 2.5 i definicije primitivnog n-tog korena, i ima ih n, oni su i svi n-ti koreni. □

Dobra osobina primitivnih n-tih korena jedinice jeste što ih možemo generisati ako znamo kako izgleda jedan od njih. U načinu na koji se generišu će nam pomoći sledeća lema.

Lema 2.8. *Neka su n i k prirodni brojevi i ε primitivni n-ti koren jedinice. Tada je ε^k takođe primitivni n-ti koren jedinice ako i samo ako su n i k uzajamno prosti prirodni brojevi.*

Dokaz. ($\Rightarrow$) Neka je ε^k primitivni koren i neka je $1 < k < n$. Pretpostavimo da k i n nisu uzajamno prosti, tj. neka je $(k, n) = d$, gde je $d > 1$. Kako je $d > 1$, postoje brojevi k_1 i n_1 takvi da je $k = dk_1$ i $n = dn_1$ i $(k_1, n_1) = 1$. Tada imamo da je

$$(\varepsilon^k)^{n_1} = \varepsilon^{dk_1 n_1} = \varepsilon^{nk_1} = (\varepsilon^n)^{k_1} = 1^{k_1} = 1$$

i $n_1 = \frac{n}{d} < n$, pa je ε^k najviše reda n_1 i $n_1 < n$, pa ε^k nije primitivni koren. Primenom kontrapozicije dobijamo da važi smer ($\Rightarrow$).
($\Leftarrow$) Neka su k i n uzajamno prosti prirodni brojevi, tj. neka je $(k, n) = 1$. Tada je $(\varepsilon^k)^a = 1$ ako i samo ako n deli ka, jer je ε reda n. Kako su k i n uzajamno prosti brojevi mora $n \mid a$, pa je $a = 0$ ili $a \geq n$. Ovo znači da je red elementa ε^k jednak n, pa je ε^k primitivni koren. □

Posledica 2.9. *Za dati prirodan broj n postoji $\varphi(n)$ primitivnih n-tih korena jedinice.*

Teorema 2.10. *Zbir svih primitivnih n-tih korena jedinice jednak je $\mu(n)$.*

Dokaz. Neka je

$$f(n) = \sum_{\substack{1 \leq k \leq n \\ (n,k)=1}} e^{\frac{2ki\pi}{n}}$$

gde je $e^{\frac{2i\pi}{n}}$ primitivni n-ti koren. Pokažimo da je f up-multiplikativna funkcija. Za početak pokažimo da je svih $\varphi(mn)$ sabiraka iz $f(m)f(n)$ međusobno

različito.
Pretpostavimo suprotno, tj. da su neka dva jednaka, tj.

$$e^{\frac{2ia\pi}{n}} e^{\frac{2ib\pi}{m}} = e^{\frac{2ic\pi}{n}} e^{\frac{2id\pi}{m}}.$$

Sređivanjem ove jednakosti dobijamo

$$e^{\frac{(am+bn)2i\pi}{mn}} = e^{\frac{(cm+dn)2i\pi}{mn}},$$

tj. $am + bn \equiv cm + dn$ po modulu mn. Dalje je $am + bn - cm - dn \equiv 0$ po modulu mn, tj. $m(a-c) + n(b-d) \equiv 0$ po modulu mn. Iz ovoga dalje sledi da n deli $a-c$, a m deli $b-d$, pošto je $(m,n) = 1$, što je nemoguće, jer a i c, odnosno b i d biramo različite po modulima, redom, m i n i koji su sa njima uzajamno prosti. Takođe se svaki od ovih sabiraka pojavljuje i u $f(mn)$. To je zato što su $am+bn$ i mn uzajamno prosti zbog $(a,n) = (b,m) = (m,n) = 1$. Dakle, f je up-multiplikativna.
Obeležimo sa ε n-ti primitivni koren iz jedinice. Pošto je

$$f(p) = \varepsilon + \varepsilon^2 + ... + \varepsilon^{p-1} = \frac{\varepsilon(\varepsilon^{p-1} - 1)}{\varepsilon - 1} = \frac{\varepsilon^p - \varepsilon}{\varepsilon - 1} = \frac{1 - \varepsilon}{\varepsilon - 1} = \frac{-1(\varepsilon - 1)}{\varepsilon - 1} = -1$$

i slično je $f(p^k) = 0$ za $k > 1$, to iz multiplikativnosti f sledi $f(n) = \mu(n)$ za sve n. □

2.0.3 Osobine polinoma

U ovom odeljku ćemo se podsetiti nekih osobina polinoma, izvoda polinoma, nesvodljivosti polinoma, kao i nula polinoma.

Definicija 2.7. Polinom $p(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0$ je monički ako mu je vodeći koeficijent $a_n = 1$.

Definicija 2.8. Neka je polinom $p(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0$ polinom sa koeficijentima iz nekog polja K. Tada je izvod polinoma $p(x)$ novi polinom

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

Teorema 2.11. *Neka su p i q dva polinoma iz $K[x]$. Tada važi*
1) $(p(x) + q(x))' = p'(x) + q'(x)$
2) $(p(x)q(x))' = p(x)q'(x) + p'(x)q(x)$.

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

1)

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

2)

$$(p(x) \cdot q(x))' = \left(\sum_{m,n \geq 0} a_m b_n x^{m+n} \right)' = \sum_{m,n \geq 0} a_m b_n (m+n) x^{m+n-1} =$$

$$\sum_{m,n \geq 0} a_m b_n (m x^{m-1} x^n) + \sum_{m,n \geq 0} a_m b_n (x^m n x^{n-1}) = \sum_{m \geq 0} m a_m x^{m-1} \left(\sum_{n \geq 0} b_n x^n \right)' +$$

$$\sum_{n \geq 0} n b_n x^{n-1} \left(\sum_{m \geq 0} a_m x^m \right)' = p(x) \cdot q'(x) + p'(x) \cdot q(x).$$

□

Primer 2.6. Dati su polinomi $p(x) = x^4 + 5x^3 + 3x^2 - 19x - 30$ i $q(x) = x^4 + 4x^3 + 4x^2 - 1$ iz $Q[x]$. Odrediti izvode zbira i proizvoda ova dva polinoma.

Sabiranjem data dva polinoma dobićemo novi polinom iz istog polja, a onda ćemo po definiciji za izvod polinoma naći izvod.

$$(p(x) + q(x))' = (x^4 + 5x^3 + 3x^2 - 19x - 30 + x^4 + 4x^3 + 4x^2 - 1)' =$$
$$(2x^4 + 9x^3 + 7x^2 - 19x - 31)' = 2 \cdot 4x^3 + 9 \cdot 3x^2 + 7 \cdot 2x - 19 = 8x^3 + 27x^2 + 14x - 19.$$

Za traženje proizvoda ova dva polinoma koristićemo teoremu 2.11 iako se može prvo naći proizvod dva polinoma, pa po definiciji uraditi izvod novodobijenog polinoma. $(p(x) \cdot q(x))' = (x^4 + 5x^3 + 3x^2 - 19x - 30)' \cdot (x^4 + 4x^3 + 4x^2 - 1) + (x^4 + 5x^3 + 3x^2 - 19x - 30) \cdot (x^4 + 4x^3 + 4x^2 - 1)' = 4x^7 + 16x^6 + 16x^5 - 4x^3 + 15x^6 + 60x^5 + 60x^4 - 15x^2 + 6x^5 + 24x^4 + 24x^3 + 6x - 19x^4 - 76x^3 - 76x^2 + 19 + 4x^7 + 12x^6 + 8x^5 - x^4 + 20x^6 + 60x^5 + 40x^4 - 5x^3 + 12x^5 + 36x^4 + 24x^3 - 3x^2 - 76x^4 - 228x^3 - 152x^2 + 19x - 120x^3 - 360x^2 - 240x + 30 = 5x^7 + 63x^6 + 162x^5 + 64x^4 - 385x^3 - 606x^2 - 215x + 49.$

Pošto ćemo se kasnije baviti nesvodljivošću ciklotomičnih polinoma, onda ćemo u ovom delu definisati nesvodljivost ili ireducibilnost polinoma, kao i neke osobine takvih polinoma.

Definicija 2.9. Polinom $p(x)$ sa koeficijentima u prstenu R je nesvodljiv nad R ako iz $p(x) = q(x)r(x)$ sledi da je bar jedan od polinoma $q(x)$ i $r(x)$ invertibilan nad istim prstenom.

Primer 2.7. Ispitati da li je polinom $p(x) = x^4 + 4x^3 + 4x^2 + 1$ svodljiv u $Z[x]$.

Vidimo da su delioci slobodnog člana polinoma ± 1, a vodeći koeficijent 1 jedina moguća celobrojna rešenja su 1 i -1. Bezuovim stavom proverićemo da li je neki od ovih brojeva nula traženog polinoma. Kako je

$$p(1) = 1 + 4 + 4 + 1 = 10,\ p(-1) = 1 - 4 + 4 + 1 = 2,$$

onda ovo nisu nule polinoma, pa nemamo faktora stepena 1, a ni stepena 3 pri rastavljanju u $Z[x]$. Sada ćemo ovaj polinom pokušati da rastavimo na dva polinoma stepena 2, tj.

$$x^4 + 4x^3 + 4x^2 + 1 = (x^2 + ax + b)(x^2 + cx + d)$$

gde koeficijenti a, b, c i d moraju biti iz skupa celih brojeva. Množenjem ovih polinoma i izjednačavanjem koeficijenata ćemo proveriti da li ovakvi polinomi postoje.

$$x^4 + 4x^3 + 4x^2 + 1 = x^4 + (a + c)x^3 + (b + d + ac)x^2 + (ad + bc)x + bd$$

odnosno izjednačavanjem koeficijenata dobijamo sistem jednačina:

$$\begin{gathered} a + c = 4 \\ b + d + ac = 4 \\ ad + bc = 0 \\ bd = 1. \end{gathered}$$

Iz poslednje jednakosti imamo $b = d = \pm 1$. Ako je $b = d = 1$, onda iz prve i treće jednakosti dobijamo da je $4 = a + c = 0$ što je nemoguće, pa u ovom slučaju nemamo rešenje. Ako je $b = d = -1$, onda treća jednačina postaje $-a - c = 0 \Leftrightarrow a + c = 0$, pa iz ove i prve jednačine ponovo dobijamo kontradikciju da je $4 = a + c = 0$ iz čega zaključujemo da se traženi polinom ne može rastaviti u $Z[x]$, odnosno on je nesvodljiv nad poljem $Z[x]$.

Posledica 2.12. *Ako je R polje, onda su svi nenula polinomi stepena 0 invertibilni, pa nesvodljivost nad poljem znači da se polinom ne može napisati kao proizvod dva polinoma manjeg stepena nad tim poljem.*

Primer 2.8. Ispitati svodljivost polinoma $p(x) = x^2 - 2$ nad Z i R.

Nule ovog polinoma dobijamo iz jednakosti $x^2 - 2 = 0$, odnosno $x^2 = 2$. Ova jednakost nema rešenje u skupu Z, pa je ovaj polinom nesvodljiv nad Z. U skupu R postoje rešenja jednačine, to su $\pm\sqrt{2}$. Dakle, polinom $p(x)$ je svodljiv nad R i $p(x) = (x - \sqrt{2})(x + \sqrt{2})$.

Teorema 2.13 (Gausova lema)**.** *Neka je R domen jednoznačne faktorizacije, F količničko polje domena R, a $p(x)$ polinom sa koeficijentima u R. Ako je $p(x)$ nesvodljiv nad R i stepena većeg od 0, onda je nesvodljiv i nad F. Ako je $p(x)$ nesvodljiv nad F i NZD svih njegovih koeficijenata, izračunat u R je jednak 1, onda je $p(x)$ nesvodljiv i nad R.*

Ajzenštajnov kriterijum je najpoznatiji kriterijum za proveravanje nesvodljivosti polinoma, pa ćemo ga definisati i dati primer njegove primene.

Teorema 2.14. *Neka je dat polinom $q(x) \in Z[x]$, tako da je*

$$q(x) = c_n x^n + c_{n-1} x^{n-1} + ... + c_1 x + c_0$$

i neka je p prost broj koji ne deli c_n, deli sve c_i, $i = 0, 1, ..., n-1$ i p^2 ne deli c_0. Tada je polinom $q(x)$ nesvodljiv na $Q[x]$.

Primer 2.9. Dokazati da je polinom $x^7 + 24x - 48$ nesvodljiv na $Z[x]$.

Za polinom $x^7 + 24x - 48$ postoji broj p, $p = 3$ koje deli 24 i -48, a ne deli 1 i $3^2 = 9$ ne deli -48, pa na osnovu Ajzenštajnovog kriterijuma je ovaj polinom nesvodljiv na $Z[x]$.

Sledeća teorema važi za sva savršena polja K. Pre nego što budemo dokazali teoremu, definisaćemo savršeno polje, a zatim lemu koja će nam pomoći u dokazu teoreme.

Definicija 2.10. Polje K je savršeno ako i samo ako je svaki nesvodljiv polinom $p(x) \in K[x]$ separabilan.

Definicija 2.11. Nesvodljiv polinom $p(x)$ nad poljem K je separabilan nad tim poljem ako i samo ako ima samo jednostruke nule (u nekom svom polju razlaganja).

Lema 2.15. *Nesvodljiv nekonstantan polinom $q(x)$ nad poljem R, Q ili Z_p, kao ni nad prstenom Z, ne može imati izvod jednak 0.*

Dokaz. Za polja R i Q, kao i prsten Z, iz definicije izvoda polinoma, ako znamo da je izvod jednak nuli onda on mora biti konstantan, jer je karakteristika 0. Pokazaćemo da tvrđenje važi za polje Z_p.

Tvrdimo da je nesvodljiv polinom $f(x)$ čiji je izvod jednak 0 oblika $f(x) = \sum_{k\geq 0} c_k x^{pk}$. Ako je polinom $f(x) = a_n x^n + ... + a_1 x + a_0$, njegov izvod je $f'(x) = na_n x^{n-1} + ... + a_1$. Kako je taj izvod jednak 0, zaključujemo da je $ia_i = 0$ za svako i, što dalje znači da je $a_i = 0$ ili $p|i$. Time je ovo tvrđenje dokazano. Dalje, fiksiramo koeficijente polinoma $f(x)$, dakle

$$f(x) = a_0 + a_p x^p + a_{2p} x^{2p} + \cdots + a_{mp} x^{mp}.$$

Neka je $a_{pi} \neq 0$, tada je $a_{pi}^{p-1} = 1$ u Z_p, dok je $a_{pi}^p = a_{pi}$ u Z_p. Neka je $q(x) = \sum_{i=0}^{m} a_{pi} x^i$. Tada je $(q(x))^p = \sum_{i=0}^{m} a_{pi}^p x^{pi}$, jer ostali koeficijenti postaju 0 po modulu p. Da vidimo zašto to važi: kako je p prost broj, u sumi

$$\left(\sum_{i=0}^{m} a_{pi} x^i\right)^p = \sum_{t_0+t_1+...+t_m=p} \frac{p!}{t_0!t_1!...t_m!} a_0^{t_0} (a_p x)^{t_1} ... (a_{pm} x^m)^{t_m}$$

broj $\frac{p!}{t_0!...t_m!}$ nije deljiv sa p jedino ako je neki od brojeva $t_0, ..., t_m$ baš jednak p, a ostali t_i moraju biti jednaki 0. Dakle,

$$\left(\sum_{i=0}^{m} a_{pi} x^i\right)^p \equiv (a_{pm} x)^p + ... + (a_p x)^p + (a_0)^p \pmod{p}.$$

Dalje je $(a_{ip})^p = a_{ip}$, pa sledi da je

$$(q(x))^p = \sum_{i=0}^{m} a_{ip} x^{ip} = \sum_{i=0}^{n} a_i x^i = f(x),$$

jer $n = mp$ i jer su ostali $a_i = 0$ kada p ne deli i. Iz ovoga sledi da $f(x)$ nije nesvodljiv. Time je naše tvrđenje dokazano. □

Teorema 2.16. *Neka je polinom $p(x)$ sa koeficijentima iz polja K. Tada postoji nekonstantni polinom $a(x)$ takav da važi $a(x)^2$ deli $p(x)$ ako i samo ako polinomi $p(x)$ i $p'(x)$ nisu uzajamno prosti.*

Dokaz. ($\Rightarrow$) Ako $a(x)^2 | p(x)$, onda je $p(x) = a(x)^2 q(x)$, za neki polinom $q(x) \in K[x]$. Dalje je izvod polinoma $p(x)$ jednak

$$p'(x) = 2a(x)a'(x)q(x) + a(x)^2 q'(x)$$

odakle vidimo da $a(x)|p'(x)$.

($\Leftarrow$) Neka najmanji zajednički delilac polinoma $p(x)$ i $p'(x)$ ima stepen veći od nule. Onda postoji nesvodljivi polinom $b(x)$ koji deli najmanji zajednički delilac polinoma $p(x)$ i $p'(x)$. Tada je $p(x) = b(x) \cdot q(x)$. Po definiciji izvoda polinoma je $p'(x) = b(x)q'(x) + b'(x)q(x)$, iz čega zaključujemo da $b(x)$ mora da deli $b'(x)q(x)$. Kako je stepen polinoma $b'(x)$ manji od stepena polinoma $b(x)$ i po prethodnoj lemi $b'(x)$ je različit od 0, a znamo i da je $b(x)$ nesvodljiv, onda $b(x)$ ne može da deli $b'(x)$ već mora da deli $q(x)$. Međutim, kako je $p(x) = b(x) \cdot q(x)$ i $b(x) \mid q(x)$ sledi da $b(x)^2$ deli $p(x)$. Time je dokaz završen. □

Posledica 2.17. *Neka je n prirodan broj. Tada polinom $x^n - 1$ nema dvostrukih nula u C.*

Teorema 2.18. *Neka je p prost broj. Ako postoji kompleksan broj a i polinom $g(x) \in Z[x]$ tako da važi*

$$x^n - 1 \equiv (x - a)^2 g(x) \ (mod\ p)$$

onda p deli n.

Glava 3

Definicija i osobine ciklotomičnih polinoma

Definicija 3.1. Neka je n proizvoljan prirodan broj. Tada je n-ti ciklotomični polinom monički polinom čiji su koreni svi primitivni n-ti koreni jedinice, a nema dvostrukih nula

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

Stepen polinoma $\Phi_n(x)$ je $\varphi(n)$, pošto postoji $\varphi(n)$ primitivnih n-tih korena jedinice.

Ako je $n > 2$, onda ± 1 nisu primitivni koreni jedinice stepena n. U ovom slučaju primitivni koreni su konjugovano kompleksni brojevi.
Za $n = 1$, $\Phi_1(x) = x - 1$. Za $n = 2$ imamo $x^2 - 1 = (x - 1)(x + 1)$ što znači da je $\Phi_2(x) = x + 1$. Za $n = 3$, $x^3 - 1 = (x - 1)(x^2 + x + 1)$, pa je $\Phi_3(x) = x^2+x+1$. Za $n = 4$, $x^4-1 = (x^2-1)(x^2+1) = (x-1)(x+1)(x^2+1)$, pa je $\Phi_4(x) = x^2 + 1$. Analognim postupkom dobijamo i ostale ciklotomične polinome. Predstavićemo prvih 20:
$\Phi_1(x) = x - 1$
$\Phi_2(x) = x + 1$
$\Phi_3(x) = x^2 + x + 1$
$\Phi_4(x) = x^2 + 1$
$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$
$\Phi_6(x) = x^2 - x + 1$
$\Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$

$\Phi_8(x) = x^4 + 1$
$\Phi_9(x) = x^6 + x^3 + 1$
$\Phi_{10}(x) = x^4 - x^3 + x^2 - x + 1.$
$\Phi_{11}(x) = x^10 + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1.$
$\Phi_{12}(x) = x^4 - x^2 + 1$
$\Phi_{13}(x) = x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
$\Phi_{14}(x) = x^6 - x^5 + x^4 - x^3 + x^2 - x + 1$
$\Phi_{15}(x) = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$
$\Phi_{16}(x) = x^8 + 1$
$\Phi_{17}(x) = x^{16} + x^{15} + x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
$\Phi_{18}(x) = x^6 - x^3 + 1$
$\Phi_{19}(x) = x^{18} + x^{17} + x^{16} + x^{15} + x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
$\Phi_{20}(x) = x^8 - x^6 + x^4 - x^2 + 1.$

Može se zaključiti da ako je p prost broj $\Phi_p(x) = 1 + x + ... + x^{p-1} = \sum_{i=0}^{p-1} x^i$.

Neka je n prirodan broj. Pogledajmo kako se polinom $x^n - 1$ rastavlja na činioce za $n = 2, 3, 4, 5$.
$x^2 - 1 = (x - 1)(x + 1) = \Phi_1(x) \cdot \Phi_2(x)$
$x^3 - 1 = (x - 1)(x^2 + x + 1) = \Phi_1(x) \cdot \Phi_3(x)$
$x^4 - 1 = (x^2 - 1)(x^2 + 1) = (x - 1)(x + 1)(x^2 + 1) = \Phi_1(x) \cdot \Phi_2(x) \cdot \Phi_4(x)$
$x^5 - 1 = (x - 1)(x^4 + x^3 + x^2 + x + 1) = \Phi_1(x) \cdot \Phi_5(x)$
Primetimo sada da se polinom $x^n - 1$ rastavlja kao proizvod ciklotomičnih polinoma i to onih koji dele n. Da to važi za svako n, dokazaćemo sledećom teoremom.

Teorema 3.1. *Neka je n prirodan broj. Tada je*

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

Dokaz. Dokazaćemo da su polinomi $x^n - 1$ i $\prod_{d|n} \Phi_d(x)$ jednaki tako što ćemo pokazati da polinomi nemaju višestrukih nula i da imaju sve iste nule, a kako su oba polinoma monički slediće da su oni i jednaki.
Na osnovu posledice 2.17 znamo da polinom sa leve strane jednakosti nema dvostrukih nula u C. Tačno je i da polinom sa desne strane jednakosti ne

može imati višestrukih nula, jer kompleksan broj ne može istovremeno biti d-ti i d'-ti primitivni koren iz jedinice za različite d i d'. Znamo da su sve nule polinoma $x^n - 1$ n-ti koreni jedinice. Neka je θ jedan od tih korena i neka je reda d. Tada je θ primitivni d-ti koren jedinice, pa je i nula polinoma $\Phi_d(x)$, a pošto $d|n$ onda je θ i nula polinoma $\prod_{d|n} \Phi_d(x)$. S druge strane, ako je θ nula proizvoda $\prod_{d|n} \Phi_d(x)$, onda je nula nekog od $\Phi_d(x)$, a samim tim $x^d - 1$. Kako $d \mid n$, onda $(x^d - 1) \mid (x^n - 1)$, pa je θ nula i od $x^n - 1$. Dakle, jednakost je zadovoljena. □

Za narednu teoremu treba nam par elementarnih činjenica o Ojlerovoj funkciji φ.

Lema 3.2. *Neka je n neparan prirodan broj. Tada je $\varphi(2n) = \varphi(n)$ i $\varphi(n)$ je paran broj.*

Dokaz. Ako je n neparno, znamo da je $\varphi(2n) = \frac{1}{2-1}\varphi(n) = \varphi(n)$, pa je prvo tvrđenje dokazano. Dalje, svaki $k < n$ ima isti NZD sa n kao i $n - k$, pa su ili oba uzajamno prosti sa n, ili oba nisu. Ako je n neparno, onda se skup $\{1, 2, \ldots, n-1\}$ može razbiti u parove oblika $\{k, n-k\}$, pa je podskup svih uzajamno prostih sa n disjunktna unija nekih od tih parova. Dakle, $\varphi(n)$ je parno za neparne n. □

Usput, nije teško dokazati analizom dva-tri slučaja da je $\varphi(n)$ paran broj za sve $n > 2$, ali nam to ne treba u ovom radu, pa dokazujemo samo za neparne brojeve i njihove proizvode sa 2.

Teorema 3.3. *Neka je $n > 1$ neparan prirodan broj. Tada je*

$$\Phi_{2n}(x) = \Phi_n(-x).$$

Dokaz. Tvrdimo da, ako su $\varepsilon_1, \varepsilon_2, ..., \varepsilon_{\varphi(n)}$ svi primitivni koreni stepena n, tada su $-\varepsilon_1, -\varepsilon_2, ..., -\varepsilon_{\varphi(n)}$ svi primitivni koreni stepena $2n$. Kako za neparno n znamo na osnovu leme 3.2 da je $\varphi(2n) = \varphi(n)$, onda je broj primitivnih n-tih korena jedinice jednak broju primitivnih $2n$-tih korena jedinice.

Ostaje nam da pokažemo da ako je ε primitivni n-ti koren jedinice, onda je $-\varepsilon$ primitivni $2n$-ti koren jedinice. Ako je $0 < k < n$, onda tvrdimo da je $\varepsilon^k \neq -1$. Zaista, ako bi ε^k bilo jednako -1, onda bi bilo $\varepsilon^{2k} = (\varepsilon^k)^2 = (-1)^2 = 1$ i $\varepsilon^{2n-2k} = 1$. Takođe znamo da $2k \neq n$ jer je n neparan broj, pa

važi ili $2k < n$, ili $2n - 2k < n$. Dakle, dobili bismo stepen manji od n (ili $2k$, ili $2n - 2k$) na koji dignemo ε i dobijemo 1. To je nemoguće, jer red od ε je n.

Prema tome, ako je $0 < k < n$, onda $(-\varepsilon)^k \neq 1$. Stoga ni za jedno $0 < k < n$ ne važi $(-\varepsilon)^k = 1$: za parne k bi sledilo da $\varepsilon^k = 1$, što ne važi, jer je n red od ε, a za neparne k bi važilo da $\varepsilon^k = -1$, što smo upravo pokazali da nije tačno. Takođe, za $0 < k < n$, kako $\varepsilon^k \notin \{-1, 1\}$, sledi da ni $(-\varepsilon)^{n+k} = -(-\varepsilon)^k \neq 1$. Kako je n neparno, $(-\varepsilon)^n = -1 \neq 1$, pa je red od $-\varepsilon$ jednak $2n$. Zbog toga je
$\Phi_n(-x) = (-x - \varepsilon_1)(-x - \varepsilon_2)...(-x - \varepsilon_{\varphi(n)})$, a
$\Phi_{2n}(x) = (x + \varepsilon_1)(x + \varepsilon_2)...(x + \varepsilon_{\varphi(n)})$.
Dokazali smo da je $\Phi_{2n}(x) = (-1)^{\varphi(n)}\Phi_n(-x)$, a na osnovu leme 3.2 znamo da je $\varphi(n)$ paran broj, pa sledi da $\Phi_{2n}(x) = \Phi_n(-x)$. □

Sledećom teoremom dat je zapis ciklotomičnih polinoma koji je pogodan za njihovo izračunavanje, a koristi se i za dokazivanje nekih teorema.

Teorema 3.4. *Neka je n proizvoljan prirodan broj. Tada važi*

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

Dokaz. Iz teoreme 3.1 znamo da je $x^n - 1 = \prod_{d|n} \Phi_d(x)$. Ako na ovo primenimo teoremu 2.3, tj. uzmemo da je $F(n) = x^n - 1$, onda je $f(d) = \Phi_d(x)$. Prema ovoj teoremi je $f(n) = \prod_{d|n} F(\frac{n}{d})^{\mu(d)}$, tj. $\Phi_n(x) = \prod_{d|n}(x^{\frac{n}{d}} - 1)^{\mu(d)}$ što je i trebalo pokazati. □

Definicija 3.2. Polinom $p(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$ je palindromičan ako je $a_n a_{n-1}...a_1 a_0$ palindrom, tj. ako je $a_k = a_{n-k}$, za sve $k = 0, 1, ..., n$.

Teorema 3.5. *Za svaki prirodan broj $n > 1$, polinom $\Phi_n(x)$ je palindromičan.*

Dokaz. Tvrđenje sledi indukcijom po n iz sledeće leme. Daćemo i njen dokaz.

Lema 3.6. *Neka su $p(x)$ i $q(x)$ polinomi takvi da su $p(x)$ i $p(x) \cdot q(x)$ palindromični. Onda je polinom $q(x)$ palindromičan.*

Dokaz. Neka je $p(x) = \sum_{i=0}^{m} a_i x^i$, $q(x) = \sum_{i=0}^{n} b_i x^i$ i $p(x)q(x) = \sum_{i=0}^{m+n} c_i x^i$. Na osnovu pretpostavke znamo da za sve $0 \leq i \leq m$ i sve $0 \leq j \leq m+n$ važi

$$a_i = a_{m-i} \textbf{ i } c_j = c_{m+n-j}. \tag{3.1}$$

Pretpostavimo da $q(x)$ nije palindromičan. To znači da postoji $k \geq 0$ takvo da

$$b_k \neq b_{n-k} \tag{3.2}$$

i ako je $k > 0$, onda za sve $0 \leq j < k$ važi

$$b_j = b_{n-j}. \tag{3.3}$$

Sada računamo c_k i c_{m+n-k}. Razlikovaćemo dva slučaja. Prvi kada je $k \leq m$ i drugi kada je $k > m$.
Za $k \leq m$

$$c_k = \sum_{i=0}^{k} a_i b_{k-i}$$

i

$$c_{m+n-k} = \sum_{i=0}^{m+n-k} a_i b_{m+n-k-i} = \sum_{i=0}^{m} a_i b_{m+n-k-i} = \sum_{i=m-k}^{m} a_i b_{m+n-k-i}.$$

Dalje uvodimo smenu $j := m - i$ i računamo c_{m+n-k}.

$$c_{m+n-k} = \sum_{i=m-k}^{m} a_i b_{m+n-k-i} = \sum_{j=0}^{k} a_{m-j} b_{n-k+j} \overset{3.1}{=} \sum_{j=0}^{k} a_j b_{n-k+j} = a_0 b_{n-k} +$$
$$\sum_{j=1}^{k} a_j b_{n-(k-j)} \overset{3.3}{=} a_0 b_{n-k} + \sum_{j=1}^{k} a_j b_{k-j} \overset{3.2}{\neq} a_0 b_k + \sum_{j=1}^{k} a_j b_{k-j} = \sum_{j=0}^{k} a_j b_{k-j} = c_k.$$

Upravo smo pokazali da je $c_k \neq c_{m+n-k}$ što je kontradikcija.
Za $k > m$ je skoro isto, jedina razlika je što su granice suma drugačije. Prvo, imamo

$$c_k = \sum_{i=0}^{k} a_i b_{k-i} = \sum_{i=0}^{m} a_i b_{k-i}.$$

Dalje,

$$c_{m+n-k} = \sum_{i=0}^{m+n-k} a_i b_{m+n-k-i} = \sum_{i=0}^{m} a_i b_{m+n-k-i} \overset{j:=m-i}{=} \sum_{j=0}^{m} a_{m-j} b_{n-k+j} \overset{3.1}{=}$$
$$\sum_{j=0}^{m} a_j b_{n-k+j} = a_0 b_{n-k} + \sum_{j=1}^{m} a_j b_{n-(k-j)} \overset{3.3}{=} a_0 b_{n-k} + \sum_{j=1}^{m} a_j b_{k-j} \overset{3.2}{\neq}$$
$$a_0 b_k + \sum_{j=1}^{m} a_j b_{k-j} = \sum_{j=0}^{m} a_j b_{k-j} = c_k.$$

I u ovom slučaju smo dobili $c_k \neq c_{m+n-k}$, što je kontradikcija. Pretpostavka da $q(x)$ nije palindromičan uvek vodi u kontradikciju, pa smo dokazali da $q(x)$ mora biti palindromičan. □

Vraćamo se na dokaz teoreme 3.5 i dokazujemo indukcijom po n.
Za $n = 2$, $\Phi_2(x) = x + 1$, pa je tvrđenje tačno.
Pretpostavimo da je tačno za sve $1 < k < n$ i dokažimo da važi i za n.
Kako je $x^n - 1 = \prod_{d|n} \Phi_d(x)$, onda iz $\frac{x^n-1}{x-1} = \prod_{\substack{d|n \\ d\neq 1}} \Phi_d(x) = \Phi_n(x) \cdot \prod_{\substack{d|n \\ 1<d<n}} \Phi_d(x)$ sledi da je i $\Phi_n(x)$ palindromičan polinom, pošto su $\prod_{\substack{d|n \\ 1<d<n}} \Phi_d(x)$ (po indukcijskoj hipotezi) i $\frac{x^n-1}{x-1} = x^{n-1}+x^{n-2}+\cdots+x+1$ palindromični polinomi. □

Pre nego što pređemo na dokaze nesvodljivosti ciklotomičnih polinoma i da su im svi koeficijenti celobrojni, definisaćemo nekoliko pomoćnih lema, a neke od njih i dokazati.

Definicija 3.3. Neka je $p(x) \in Z[x]$ dat sa $p(x) = \sum_{i=0}^{n} a_i x^i$. Mera polinoma $p(x)$ je

$$m(p(x)) := NZD(a_0, a_1, \ldots, a_n).$$

Ako je $m(p(x)) \sim 1$, onda je $p(x)$ primitivan polinom.

Teorema 3.7. *Ako $p(x) \in Z[x]$ i $k \in Z \setminus \{0\}$, onda je $m(k \cdot p(x)) = k \cdot m(p(x))$.*

Dokaz. Sledi direktno iz definicije mere polinoma i osobine najvećeg zajedničkog delioca, da je $NZD(ka_0, ka_1, \ldots, ka_n) = k \cdot NZD(a_0, a_1, \ldots, a_n)$. □

Lema 3.8 (Gausova lema o primitivnim polinomima)**.** *Ako su $p(x), q(x) \in Z[x]$ primitivni polinomi, onda je i polinom $p(x) \cdot q(x)$ primitivan.*

Dokaz ove teoreme može se naći u knjizi Algebra 4, prof. Milana Grulovića, dokaz Leme 8.17.

Sledeća lema povezuje polinome nad skupom celih brojeva sa polinomima nad njihovim količničkim poljem, skupom racionalnih brojeva. Daćemo njenu formulaciju bez dokaza.

Lema 3.9. *Ako je $p(x) \in Q[x]$ polinom, onda postoji primitivan polinom $p_1(x) \in Z[x]$ i $\alpha \in Q$ takvi da $p(x) = \alpha p_1(x)$. Štaviše, $p_1(x)$ je jedinstven do na proizvod sa ± 1.*

Sada ćemo formulisati i dokazati lemu koja je u neku ruku suprotan smer Gausove leme (jer se radi o deljenju, a ne množenju). Ona i njena posledica će nam koristiti u dokazu da su koeficijenti ciklotomičnih polinoma celobrojni, a i u dokazu nesvodljivosti ciklotomičnih polinoma u $Z[x]$.

Lema 3.10. *Neka su $p(x) \in Z[x]$, $q(x) \in Q[x]$ takvi da je $p(x) \cdot q(x) \in Z[x]$ i da su polinomi $p(x)$ i $p(x) \cdot q(x)$ oba primitivni. Onda je $q(x) \in Z[x]$ i primitivan je.*

Dokaz. Na osnovu leme 3.9 , postoji polinom $q_1(x) \in Z[x]$ i $\alpha = \frac{a}{b} \in Q$ takvi da je $q_1(x)$ primitivan i da $q(x) = \alpha q_1(x)$. Sledi da

$$bp(x)q(x) = b\tfrac{a}{b}p(x)q_1(x) = ap(x)q_1(x).$$

Tada
$b \sim bm(p(x)q(x)) = m(bp(x)q(x)) = m(ap(x)q_1(x)) = am(p(x))m(q_1(x)) \sim a$. Dakle, $a \sim b$, pa $\alpha = \frac{a}{b} = \pm 1$. Stoga je i polinom $q(x) = \pm q_1(x)$ primitivan polinom sa celobrojnim koeficijentima. □

Posledica 3.11. *Neka su $p(x) \in Z[x]$, $q(x) \in Q[x]$ takvi da je $p(x) \cdot q(x) \in Z[x]$ i da su polinomi $p(x)$ i $p(x) \cdot q(x)$ oba moničkи. Onda je $q(x) \in Z[x]$ i takođe je moničkи.*

Dokaz. Na osnovu leme 3.10, $q(x) \in Z[x]$, a vodeći koeficijent mu mora biti 1 jer su vodeći koeficijenti $p(x)$ i $p(x) \cdot q(x)$ oba 1. (Znamo da je vodeći koeficijent proizvoda dva polinoma proizvod njihovih vodećih koeficijenata.) □

Posledica 3.12. *Neka su $p(x) \in Z[x]$, $q(x) \in C[x]$ takvi da je $p(x) \cdot q(x) \in Z[x]$ i da su polinomi $p(x)$ i $p(x) \cdot q(x)$ oba moničkи. Onda je $q(x) \in Q[x]$ i takođe je moničkи.*

Dokaz. Znamo da je $p(x)q(x)$ deljiv sa $p(x)$ u $C[x]$, pa je svakako kompleksna nula polinoma $p(x)$ istovremeno i nula polinoma $p(x)q(x)$. Neka je $p(x)$ nesvodljiv polinom, sledi da je $p(x)$ minimalan (pošto je nesvodljiv i monički) za neku svoju kompleksnu nulu a. Tada iz $p(a)q(a) = 0$ i $p(x)q(x) \in Q[x]$ sledi da $p(x)$ deli $p(x)q(x)$ u $Q[x]$ (jer minimalni polinom za algebarski element a deli svaki polinom kojem je a nula). Indukcijom, ako je $p(x) = f_1(x)...f_k(x)$ rastavljanje polinoma na nesvodljive faktore u $Q[x]$ takvo da su svi $f_i(x)$ monički, onda je svaki od $q(x)f_1(x)...f_k(x)$ monički polinom sa racionalnim koeficijentima. Dakle, potrebno je da na polinome $q(x)f_1(x)f_2(x)...f_i(x)$ i $q(x)f_1(x)f_2(x)...f_i(x)f_{i+1}(x)$ primenimo bazu indukcije pa dobijamo da, ako je $q(x)f_1(x)f_2(x)...f_i(x)f_{i+1}(x)$ monički polinom sa racionalnim koeficijentima, a znamo da je $f_{i+1}(x)$ nesvodljiv monički polinom sa racionalnim koeficijentima, onda je i polinom sa kompleksnim koeficijentima $q(x)f_1(x)f_2(x)...f_i(x)$ ustvari monički polinom sa racionalnim koeficijentima. Dakle, $q(x)$ je u $Q[x]$ i monički je. □

Teorema 3.13. *Neka je n prirodan broj. Tada polinom $\Phi_n(x)$ ima celobrojne koeficijente.*

Dokaz. U proizvodu $\prod_{d|n}(x^d - 1)^{\mu\left(\frac{n}{d}\right)}$ grupišemo faktore sa $\mu = 1$ i posebno faktore sa $\mu = -1$. Kao rezultat dobijamo polinom $\Phi_n(x) = \frac{P(x)}{Q(x)}$, gde su P i Q monički polinomi sa celobrojnim koeficijentima. Po posledici 3.12, $\Phi_n(x)$ je polinom sa racionalnim koeficijentima, a posledica 3.11 daje da su koeficijenti od $\Phi_n(x)$ celobrojni. □

Osvrnućemo se i na koeficijente ciklotomičnih polinoma. Na početku glave navedeni primeri polinoma $\Phi_n(x)$ pokazuju da su njihovi koeficijenti 0 ili ± 1 za male vrednosti n. Ali ovo nije uvek slučaj. Bilo koji broj može se naći kao koeficijent ciklotomičnih polinoma.

Primer 3.1. Zanimljivo je da se u $\Phi_{105}(x)$ prvi put javljaju koeficijenti različiti od $1, 0$ i -1.
$\Phi_{105}(x) = x^{48} + x^{47} + x^{46} - x^{43} - x^{42} - 2x^{41} - x^{40} - x^{39} + x^{36} + x^{35} + x^{34} + x^{33} + x^{32} + x^{31} - x^{28} - x^{26} - x^{24} - x^{22} - x^{20} + x^{17} + x^{16} + x^{15} + x^{14} + x^{13} + x^{12} - x^9 - x^8 - 2x^7 - x^6 - x^5 + x^2 + x + 1$

3.0.1 Nesvodljivost ciklotomičnih polinoma

U narednim teoremama videćemo kako se ciklotomični polinom $\Phi_{mn}(x)$ može predstaviti pomoću polinoma Φ_n. Posmatraćemo slučajeve kada je $m = p$. tj. kada je m prost broj.

Teorema 3.14. *Za prirodan broj n i prost broj p važi*

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

Dokaz. Prvo ćemo pokazati slučaj kada p deli n, analogno se pokazuje i kada p ne deli n. Prema teoremi 3.4 znamo da je

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

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

$$\Phi_n(x^p) \cdot \prod_{\substack{d|pn \\ d\nmid n}} \left(x^{\frac{pn}{d}} - 1\right)^{\mu(d)}.$$

Trebalo bi da pogledamo čemu je jednak proizvod $\prod_{\substack{d|pn \\ d\nmid n}} \left(x^{\frac{pn}{d}} - 1\right)^{\mu(d)}$. Kako d deli pn, a ne deli n, onda mora p da deli d. Znamo i da $p|n$, pa će p^2 deliti d. Zaista, ako bi samo p delilo d, onda bi bilo $d = pd_0$, gde p ne deli d_0, pa bi iz $d|pn$ sledilo da $d_0|n$, tj. $d_0|\frac{n}{p}$, odnosno, $pd_0|n$, tj. $d|n$, što je nemoguće. Dakle, $p^2|d$, pa je po definiciji Mebijusove funkcije $\mu(d) = 0$, a stoga $\prod_{\substack{d|pn \\ d\nmid n}} \left(x^{\frac{pn}{d}} - 1\right)^{\mu(d)} = 1$. Time smo dobili da je $\Phi_{pn}(x) = \Phi_n(x^p)$.

Pogledajmo slučaj kada n nije deljivo sa p. U ovom slučaju se delioci od pn sastoje od delilaca broja n i njihovog proizvoda sa p.

$$\Phi_{pn}(x) = \prod_{d|pn} \left(x^{\frac{pn}{d}} - 1\right)^{\mu(d)} = \left(\prod_{d|n} \left(x^{\frac{pn}{d}} - 1\right)^{\mu(d)}\right) \left(\prod_{d|n} \left(x^{\frac{pn}{pd}} - 1\right)^{\mu(pd)}\right).$$

Zbog jednakosti $\mu(pd) = -\mu(d)$, dobijamo da je

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

Time je dokaz završen. □

Posledica 3.15. *Neka su n i k prirodni brojevi, a p prost broj. Tada važi jednakost*

$$\Phi_{p^k n}(x) = \begin{cases} \Phi_n(x^{p^k}), \textit{kada } p \textit{ deli } n \\ \frac{\Phi_n(x^{p^k})}{\Phi_n(x^{p^{k-1}})}, \textit{kada } p \textit{ ne deli } n. \end{cases}$$

Dokaz. Dokaz se svodi na primenu prethodne teoreme $k-1$ put.

$$\Phi_{p^k n}(x) = \Phi_{p^{k-1}n}(x^p) = \Phi_{pn}(x^{p^{k-1}}) = \begin{cases} \Phi_n(x^{p^k}), \text{kada } p \text{ deli } n \\ \frac{\Phi_n(x^{p^k})}{\Phi_n(x^{p^{k-1}})}, \text{kada } p \text{ ne deli } n. \end{cases}$$ □

Primer 3.2. Izračunati $\Phi_n(\pm 1)$.
Izračunaćemo prvo $\Phi_n(1)$. Ako je n deljivo sa p^2, po prethodnoj teoremi je $\Phi_n(1) = \Phi_{\frac{n}{p}}(1^p) = \Phi_{\frac{n}{p}}(1)$. Zaista, ako je $n = p_1^{\alpha_1}p_2^{\alpha_2}...p_k^{\alpha_k}$ i $m = p_1p_2...p_k$, tada je $\Phi_n(1) = \Phi_m(1)$. Ostaje da izračunamo $\Phi_m(1)$. Ako je $m = p$ prost broj, onda je $\Phi_p(1) = 1^{p-1} + 1^{p-2} + ... + 1^1 + 1 = p$. Ako je $m = p_1p_2...p_k$ gde je $k > 1$ stavićemo da je $p = p_1$ i $n = \frac{m}{p}$. Po prethodnoj teoremi, znamo da je $\Phi_m(1) = \frac{\Phi_n(1)}{\Phi_n(1)} = 1$. Prema tome, ako je $n > 1$ onda je

$$\Phi_n(1) = \begin{cases} p, \text{ako je } n = p^\lambda \\ 1, \text{ako je } n \neq p^\lambda. \end{cases}$$

Sada izračunajmo $\Phi_n(-1)$. Sledeći slučajevi su mogući:
1) $n > 1$ je neparan broj. Tada je $\Phi_n(-1) = \Phi_{2n}(1) = 1$.

2) $n = 2^k$. Tada je na osnovu posledice 3.15 $\Phi_n(x) = \frac{x^n-1}{x^{\frac{n}{2}}-1} = x^{\frac{n}{2}} + 1$. Odatle je $\Phi_n(-1) = 0$ za $n = 2$ i $\Phi_n(-1) = 2$ za $n = 2^k$, gde je $k > 1$.
3) $n = 2m$, gde je $m > 1$ neparan broj. U ovom slučaju je $\Phi_n(-1) = \Phi_m(1)$. Iz izračunatog $\Phi_n(1)$ sledi da je $\Phi_n(-1) = p$ ako $m = p^\alpha$ i $\Phi_n(-1) = 1$ ako m ima više od jednog prostog delioca.
4) $n = 2^k m$, kada je $k > 1$ i $m > 1$ neparno. Neka je $m = p_1^{\alpha_1} p_2^{\alpha_2} ... p_t^{\alpha_t}$. Tada je $\Phi_n(x) = \Phi_{2r}(x^s)$ gde je $r = p_1 p_2 ... p_t$ i $s = 2^{k-1} p_1^{\alpha_1 - 1} ... p_t^{\alpha_t - 1}$. Stoga je $\Phi_n(-1) = \Phi_{2r}(1) = 1$.

Teorema 3.16. *Za uzajamno proste prirodne brojeve a i n važi*

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

Dokaz. Dokazaćemo jednakost tako što ćemo pokazati da polinomi imaju sve iste nule, a kako su oba polinoma monička slediće jednakost.
Polinom $\Phi_n(x^a)$ je stepena $a\varphi(n)$, a stepen polinoma $\prod_{d|a} \Phi_{nd}(x)$ je $\sum_{d|a} \varphi(dn) = \varphi(n) \sum_{d|a} \varphi(d) = \varphi(n)a$, tj. polinomi su istog stepena. Sada pokazujemo da je svaki a-ti koren primitivnog n-tog korena jedinice ujedno i koren polinoma $\prod_{d|a} \Phi_{nd}(x)$. Uzmimo da je ε n-ti primitivni koren jedinice. Tada je $\Phi_n(x^a) = \prod_{(n,k)=1} (x^a - \varepsilon^k)$. Svaka nula polinoma sa leve strane jednakosti je oblika ε^k, gde je ε an-ti primitivni koren jedinice i $(k, n) = 1$. Ako je $h = (k, a)$, onda je ε^k primitivni $\frac{an}{h}$-ti koren jedinice. Ako uzmemo da je $\frac{a}{h} = d$ onda je ε^k primitivni nd-ti koren jedinice, pa je koren polinoma $\Phi_{nd}(x)$. Ovim je dokaz završen. □

Sledeće dve teoreme koje smo radili na kursu Prstena, polja i teorije Galoa daju nesvodljivost nekih ciklotomičnih polinoma. Ponavljamo njihove dokaze, a usput pokazujemo da su polinomi čiju nesvodljivost dokazuju ciklotomični.

Teorema 3.17. *Za prost broj p polinom $\Phi_p(x)$ je nesvodljiv.*

Dokaz. Ako pokažemo da je $\Phi_p(x + 1)$ nesvodljiv, onda je $\Phi_p(x)$ nesvodljiv. Na osnovu teoreme 3.14 znamo da važi jednakost

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

Kako p^2 ne deli slobodan član ovog polinoma i p ne deli koeficijent uz najveći stepen broja x, a deli svaki drugi koreficijent uz x, po Ajzenštajnovom kriterijumu sledi da je $\Phi_p(x+1)$ nesvodljiv. □

Teorema 3.18. *Za prost broj p polinom $\Phi_{p^2}(x)$ je nesvodljiv.*

Dokaz. Neka je ε primitivni p^2-ti koren iz jedinice. Znamo da je $x^{p^2}-1 = (x^p-1)(x^{p(p-1)}+x^{p(p-2)}+...+x^{2p}-x^p+1)$. Radi lakšeg zapisa ćemo $(x^{p(p-1)}+x^{p(p-2)}+...+x^{2p}-x^p+1)$ obeležiti sa $q(x)$. Kako je $\varepsilon^{p^2}=1$ i $\varepsilon^p \neq 1$ (jer je ε primitivni koren), iz jednakosti $(\varepsilon^p-1)q(\varepsilon)=0$, mora biti $q(\varepsilon)=0$. Dakle, $q(x)$ je stepena $\varphi(p^2)=p(p-1)$ i ima kao nule sve primitivne p^2-te korene iz jedinice, pa $q(x)=\Phi_{p^2}(x)$.

Sada ćemo pokazati da je $q(x)$ nesvodljiv polinom, tačnije, kao u dokazu prethodne teoreme pokazaćemo Ajzenštajnovim kriterijumom primenjenim na prost broj p da je polinom $q(x+1) = \sum_{i=0}^{p(p-1)} a_i x^i$ nesvodljiv u $Z[x]$, pa pošto je Q količničko polje prstena Z, iz nesvodljivosti u $Z[x]$ sledi nesvodljivosti u $Q[x]$.
Sva tri polinoma (x^p-1), $q(x)$ i $x^{p^2}-1$ su monički, pa p ne deli $a_{p(p-1)}$. Ako bi za neko $0 \leq i < p(p-1)$ važilo da p ne deli a_i, onda je koeficijent uz x^{p+i} u polinomu $((x+1)^p-1)q(x+1)$ jednak
$a_i + \sum_{j=1}^{p-1} \binom{p}{j} a_j + (1-1)a_{i+p}$, što je zbir a_i i članova koji su deljivi sa p, tj. koeficijent uz x^{p+i} nije deljiv sa p. Sa druge strane, koeficijent uz x^{p+i} u $(x+1)^{p^2}-1$ je $\binom{p^2}{p+i}$. Sada ćemo pokazati da $p|\binom{p^2}{p+i}$. Maksimalni stepen broja p koji deli $(p^2)!$ je $\lfloor \frac{p^2}{p} \rfloor + \lfloor \frac{p^2}{p^2} \rfloor = p+1$, a maksimalni stepen p koji deli $(p+i)!(p^2-(p+i))!$, gde je $0 \leq p+i < p^2$, jeste $\lfloor \frac{p+i}{p} \rfloor + \lfloor \frac{p^2-(p+i)}{p} \rfloor \leq \frac{p+i}{p} + \frac{p^2-(p+i)}{p} = \frac{p+i+p^2-(p+i)}{p} = \frac{p^2}{p} = p$. Kako p^{p+1} deli $p^2!$ i ne deli $(p+i)!(p^2-(p+i))!$ sledi da je $\binom{p^2}{p+i} = \frac{p^2!}{(p+i)!(p^2-(p+i))!}$ deljivo sa p. Dakle, koeficijent uz x^{p+i} u polinomu $(x+1)^{p^2}-1$ jeste deljiv sa p, a u $((x+1)^p-1)q(x+1)$ nije. Ovim dolazimo u kontradikciju sa $x^{p^2}-1=(x^p-1)q(x)$. Još nam je ostalo da pokažemo da slobodan član polinoma nije deljiv sa p^2. To ćemo uraditi direktnim računanjem slobodnog člana polinoma $q(x+1) = \sum_{i=0}^{p-1} (x+1)^{pi}$. Svaki $(x+1)^{p(p-i)}$ ima slobodan član jednak 1, a suma ide od 0 do $p-1$,

pa je slobodan član od $q(x+1)$ jednak p. Dakle, slobodan član nije deljiv sa p^2. Sada su ispunjeni svi uslovi za primenu Ajzenštajnovog kriterijuma, pa je $q(x+1)$ nesvodljiv u $Z[x]$. Onda je i $q(x)$ nesvodljiv u $Z[x]$, pa na osnovu Gausove leme i u $Q[x]$, jer je Q količničko polje domena jednoznačne faktorizacije Z, a $q(x)$ je primitivan polinom stepena većeg od 0. □

Pokazaćemo i da nesvodljivost važi za bilo koji prirodan broj n, a ne samo za proste brojeve p. Taj dokaz je teorijski dosta zahtevniji nego u slučaju p i p^2.

Teorema 3.19. *Polinom $\Phi_n(x)$ je nesvodljiv nad Z.*

Dokaz. Neka je $\varepsilon = \cos\frac{2k\pi}{n} + i \cdot \sin\frac{2k\pi}{n}$ n-ti primitivni koren iz jedinice. Definišimo prvo polinom $P_n(x) \in C[x]$ sa

$$P_n(x) = \prod_{\substack{1\le k\le n\\(k,n)=1}} (x - \varepsilon^k).$$

Naravno, ε može biti bilo koji od $\varphi(n)$ primitivnih korena (jer znamo da pozitivni celi brojevi manji od n i uzajamno prosti sa n formiraju grupu po modulu n sa operacijom množenja). Iz leme 2.8 polinom $P_n(x)$ ima kao korene sve primitivne n-te korene jedinice. Sledi da su polinomi $P_n(x)$ i $\Phi_n(x)$ oba istog stepena $\varphi(n)$. Dalje, svi primitivni n-ti koreni iz jedinice su nule oba polinoma, a njih ima tačno $\varphi(n)$, pa su to sve nule oba polinoma, i svi primitivni n-ti koreni iz jedinice su jednostruke nule u oba polinoma. Stoga su $P_n(x)$ i $\Phi_n(x)$ asocirani u $C[x]$. No, oba su moničkи, pa sledi da $P_n(x) = \Phi_n(x)$. Na osnovu teoreme 3.13, sledi da $P_n(x)$ ima celobrojne koeficijente.
Dalje ćemo pokazati da je $P_n(x)$ nesvodljiv polinom nad Q. Dokaz će ići u tri tvrđenja.
Prvo tvrđenje: Neka je ε primitivni n-ti koren iz jedinice i $f(x)$ minimalni polinom nad Q za ε, tj. $f(x)$ je moničkи sa racionalnim koeficijentima i nesvodljiv, i $f(\varepsilon) = 0$. Tvrdimo da $f(x)$ ima celobrojne koeficijente. Kako je ε koren od $x^n - 1 = 0$, onda $f(x)$ deli $x^n - 1$. Neka je $x^n - 1 = f(x)g(x)$. Dakle, $g(x) \in Q[x]$ i moničkи je, jer su i $f(x)$ i $x^n - 1$ moničkи. Iz leme 3.9 (gde smo prebacili konstante na drugu stranu) sledi da postoje primitivni polinomi $f_1(x), g_1(x) \in Z[x]$ i nenula racionalni brojevi $a, b \in Q$ takvi da $f_1(x) = af(x)$ i $g_1(x) = bg(x)$. Iz leme 3.8 dobijamo

$$1 \sim m(f_1(x)g_1(x)) = m(af(x)bg(x)) = m(ab(x^n - 1)) \sim ab.$$

Dakle $ab = \pm 1$. Međutim, kako je $f(x)$ monički, sledi da je a vodeći koeficijent polinoma $f_1(x) \in Z[x]$, pa a mora biti ceo broj. Analogno i b mora biti ceo broj, pa $a = \pm 1$ i $b = \pm 1$. Dakle, $f(x) = \pm f_1(x) \in Z[x]$, pa $f(x)$ ima celobrojne koeficijente.
Drugo tvrđenje: Ako je p prost broj koji ne deli n, onda je ε^p koren od $f(x) = 0$. Pošto je ε koren od $P_n(x)$ sledi da $f(x)$ deli $P_n(x)$, tj. $P_n(x) = f(x)h(x)$, gde je $h(x)$ monički polinom i po posledici 3.12 ima celobrojne koeficijente. Pošto je p uzajamno prost sa n sledi da je ε^p isto primitivni n-ti koren od jedinice, tj. $P_n(\varepsilon^p) = 0$. Trebalo bi da pokažemo da je ε^p koren od $f(x)$. Pretpostavimo suprotno, da ε^p nije koren od $f(x)$, onda mora biti koren od $h(x)$. Dakle, ε je koren od $h(x^p) = 0$. Pošto je $f(x)$ minimalni polinom za ε (nad Q), sledi da $f(x)$ deli $h(x^p)$, tj. $h(x^p) = f(x)q(x)$, gde je $q(x)$ monički polinom sa celobrojnim koeficijentima (po posledici 3.12). Takođe, pošto je $P_n(x)$ faktor od $x^n - 1$ imamo $x^n - 1 = P_n(x)d(x)$, gde je $d(x)$ monički sa celobrojnim koeficijentima. Dakle, imamo sledeće jednakosti:

$$x^n - 1 = f(x)h(x)d(x) \tag{3.4}$$

$$h(x^p) = f(x)q(x) \tag{3.5}$$

Pogledajmo šta se dešava sa ovim jednačinama po modulu p, tačnije, sve koeficijente polinoma zamenićemo njihovim ostatkom pri deljenju sa p. Tako dobijeni polinomi biće u $F_p[x]$, ali oznake nećemo menjati. Jednačina (3.5) biće ekvivalentna sa

$$(h(x))^p = f(x)q(x) \tag{3.6}$$

u $F_p[x]$. Neka je $k(x)$ u $F_p[x]$ nesvodljiv faktor od $f(x)$. Iz jednačine (3.6) $k(x)$ deli $(h(x))^p$, pa deli i $h(x)$. Zbog jednakosti (3.4) $(k(x))^2$ deli $x^n - 1$. Pošto $x^n - 1$ ima dvostruki koren, onda $x^n - 1$ i njegov izvod nx^{n-1} imaju zajednički koren. Kako su n i p uzajamno prosti i izvod je nenula polinom, nx^{n-1} ne sme imati isti koren kao $x^n - 1$. Ovo nas je dovelo u kontradikciju, pa je početna pretpostavka da ε^p nije koren od $f(x)$ pogrešna.
Treće tvrđenje: $f(x)$ je minimalni polinom nad Q za svaki primitivni n-ti koren iz jedinice. Na osnovu drugog tvrđenja, za svaki prost broj p koji ne deli n, ε^p (koji je opet primitivni n-ti koren iz jedinice) je i koren od $f(x) = 0$.

Pošto je $f(x)$ monički i nesvodljiv, on će biti minimalan i za primitivni koren ε^p. Istu logiku možemo primeniti više puta i kao rezultat ćemo dobiti da je $f(x)$ minimalni polinom za $\varepsilon^{p_1 \cdots p_m}$, gde su $p_1, p_2 ... p_m$ prosti brojevi uzajamno prosti sa n. Iz toga sledi da je ε^k (gde je k uzajamno prost sa n) isto koren od $f(x)$.

Dakle, $f(x)$ ima sve nule koje ima $P_n(x)$, a u $P_n(x)$ je svaka od njih jednostruka. Stoga $P_n(x) \mid f(x)$. Pošto je $f(x)$ nesvodljiv sledi da je $f(x) = P_n(x)$ (jer su asocirani i oba monički). Dakle, $\Phi_n(x) = P_n(x)$ je nesvodljiv. □

3.0.2 Ciklotomični polinomi i red broja po prostom modulu

Lema 3.20. *Neka je n prirodan broj i d delilac broja n. Ako je x ceo broj i p prost broj koji deli $\Phi_n(x)$ i $\Phi_d(x)$, onda p deli n.*

Dokaz. Prema teoremi 3.1 važi da je $x^n - 1 = \prod_{q|n} \Phi_q(x)$, pa je $x^n - 1$ deljivo sa $\Phi_n(x)\Phi_d(x)$. Kako je p prost broj koji deli i $\Phi_n(x)$ i $\Phi_d(x)$ onda polinom $x^n - 1$ ima dvostruku nulu po modulu p, što po teoremi 2.18 znači da p deli n. □

Posledica 3.21. *Neka su m i n prirodni brojevi, a p prost broj koji ne deli mn. Tada ne mogu i $\Phi_m(x)$ i $\Phi_n(x)$ biti deljivi sa p za istu vrednost broja x.*

Dokaz. Pretpostavimo suprotno, da su oba polinoma $\Phi_m(x)$ i $\Phi_n(x)$ deljiva sa p za neko x. Tada polinom $x^{mn} - 1$ ima dvostruku nulu po modulu p, što bi po teoremi 2.18 značilo da p deli mn, a to je u kontradikciji sa uslovom teoreme. □

Lema 3.22. *Neka su m i n prirodni brojevi, a p prost broj koji ne deli ni m ni n. Tada su u Z_p polinomi $\Phi_m(x)$ i $\Phi_n(x)$ uzajamno prosti.*

Dokaz. Pretpostavimo suprotno, da polinomi $\Phi_m(x)$ i $\Phi_n(x)$ nisu uzajamno prosti, odnosno da postoji polinom $g(x) \neq 1$ koji deli oba ova polinoma. Kako $\Phi_m(x)\Phi_n(x)$ deli polinom $x^{mn} - 1$, onda i $g^2(x)$ deli $x^{mn} - 1$, što je zbog posledice 2.17 nemoguće u Z_p. □

Podsećamo na Definiciju 2.5 reda broja a po modulu p i oznake $o_p(a)$ kojom smo ga označavali.

Teorema 3.23. *Neka je p prost broj. Tada za sve prirodne brojeve n i cele brojeve a, pri čemu su a i p uzajamno prosti, važi ekvivalencija*

$$p|\Phi_n(a) \Leftrightarrow o_p(a) = n.$$

Dokaz. Dokazaćemo indukcijom po n. Tvrđenje je tačno za $n = 1$, jer je $\Phi_1(x) = x - 1$. Pretpostavimo da važi za svako $k < n$ i dokažimo za n.
($\Rightarrow$) Pretpostavimo da za neko a važi da $p|\Phi_n(a)$. Tada je $a^n - 1 \equiv 0 \ (mod\ p)$, odnosno $a^n \equiv 1 \ (mod\ p)$. Pretpostavimo da je $o_p(a) = k \neq n$. Tada iz indukcijske hipoteze imamo da je $\Phi_k(a) \equiv 0 \ (mod\ p)$. Međutim, tada je $\Phi_n(a) \equiv \Phi_k(a) \equiv 0$ po modulu p, što znači da $k|n$, pa po lemi 3.20 sledi da $p|n$, što je u kontradikciji sa uslovom teoreme.
($\Leftarrow$) Neka je $o_p(a) = n$. Tada je $a^n \equiv 1$ po modulu p, tj. $a^n - 1 \equiv 0 \ (mod\ p)$, odnosno $\prod_{k|n} \Phi_k(a) \equiv 0$ po modulu p, pa sledi da $p|\Phi_k(a)$ za neko k koje deli n. Međutim, takvo $k < n$ ne postoji, jer bi u slučaju da postoji važilo da $p|a^k - 1$, što je nemoguće jer je n najmanji broj za koji važi da je $a^n \equiv 1 \ (mod\ p)$. Dakle, $k = n$ i time je dokaz završen. □

Teorema 3.24. *Neka je n prirodan broj i x ceo broj. Tada za svaki prost delilac p polinoma $\Phi_n(x)$ važi ili da je $p \equiv 1$ po modulu n ili da p deli n.*

Dokaz. Ako $p|\Phi_n(x)$, onda p ne deli x. To je zbog toga što $p|\Phi_n(x)$, a $\Phi_n(x)|x^n - 1$, tj. $p|x^n - 1$, pa ne može da deli x. Neka je $k = o_p(x)$. Pošto $p|x^n - 1$, to je $x^n \equiv 1 \ (mod\ p)$, pa k deli n :
1) $k = n$. Tada iz Male Fermaove teoreme važi da je $x^{p-1} \equiv 1 \ (mod\ p)$, odnosno da $n|p - 1 \Leftrightarrow p \equiv 1 \ (mod\ n)$.
2) $k < n$. Pošto važi

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

sledi da za neko d koje deli k važi da $p|\Phi_d(x)$. Međutim, pošto $p|\Phi_n(x)$, $d|k$ i $k|n$, to iz leme 3.20 sledi da $p|n$. □

Lema 3.25. *Neka su a i b prirodni brojevi, a x ceo broj. Tada važi da je $NZD(x^a - 1, x^b - 1) =\mid x^{(a,b)} - 1 \mid$.*

Dokaz. Neka je $T = (x^a - 1, x^b - 1)$ i $t = (a, b)$. Pošto $x^t - 1|x^a - 1$ i $x^t - 1|x^b - 1$ sledi da $x^t - 1|T$. Iz $T|x^a - 1$ sledi da je $(x, T) = 1$. Neka je $o_T(x) = d$, tj. $x^d \equiv 1 \ (mod\ T)$. Tada $d|a$ i $d|b$, pa $d|t$. Dakle, $x^d - 1|x^t - 1$. Kako $T|x^d - 1$, a $x^d - 1|x^t - 1$ sledi da $T|x^t - 1$. Pošto $x^t - 1|T$ i $T|x^t - 1$ to je $T =\mid x^t - 1 \mid$. □

Teorema 3.26. *Neka su m i n prirodni brojevi takvi da $m > n$. Ako za neko celo x važi da je $NZD(\Phi_m(x), \Phi_n(x)) > 1$, onda su i $NZD(\Phi_m(x), \Phi_n(x))$ i $\frac{m}{n}$ stepeni istog prostog broja p.*

Dokaz. Pretpostavimo da je p prost broj koji deli i $\Phi_m(x)$ i $\Phi_n(x)$. Pokazaćemo da je tada $\frac{m}{n}$ stepen broja p. Tačnije, pokazaćemo da ako je $m = p^\alpha M$ i $n = p^\beta N$,gde su $(p, M) = (p, N) = 1$, onda je $M = N$. Kako $p|\Phi_m(x)$, a $\Phi_m(x)|x^m - 1$ sledi da $p|x^m - 1$, odnosno x i p su uzajamno prosti. Pokažimo da $p|\Phi_M(x)$. Ako je $\alpha = 0$, onda je tvrđenje dokazano, jer je onda $m = p^0 M = 1 \cdot M$, pa $p|\Phi_M(x)$. Ako je $\alpha \neq 0$ iz posledice 3.15 važi

$$0 \equiv \Phi_m(x) = \Phi_{p^\alpha M}(x) = \Phi_M(x^{p^\alpha}) \ (mod\ p),$$

pa $p|\Phi_M(x^{p^\alpha})$. Međutim, $x^{p^\alpha} \equiv x \cdot x^{p^\alpha - 1} \equiv x \cdot x^{p-1} \equiv x \ (mod\ p)$. Odatle sledi

$$0 \equiv \Phi_M(x^{p^\alpha}) \equiv \Phi_M(x) \ (mod\ p).$$

Slično, $p|\Phi_N(x)$.
Pretpostavimo sada da je $M > N$ i neka je $t = (M, N)$, $t < M$. Pošto $p|\Phi_M(x)|x^M - 1$ i $p|\Phi_N(x)|x^N - 1$, onda $p|(x^M - 1, x^N - 1)$. Iz prethodne leme sledi $p|x^t - 1 = \prod_{d|t} \Phi_d(x)$. Dakle, postoji delilac d broja t takav da p deli $\Phi_d(x)$. Međutim, $d|t$ i $t|M$ i $p|\Phi_M(x)$, pa po lemi 3.20 sledi da $p|M$, što je kontradikcija. Dakle, nije $M > N$. Analogno, ne važi ni $N > M$, pa sledi da $M = N$.

Konačno, ako bi $NZD(\Phi_m(x), \Phi_n(x))$ imao i neki drugi prost faktor $q \neq p$, isti dokaz bi se mogao primeniti i na q, pa bismo dobili da je $\frac{m}{n}$ takođe i stepen broja q. No, to je nemoguće zbog $m > n$, $p \neq q$ i jednoznačne faktorizacije u Z. □

Glava 4

Vederburnova teorema

Jedna od najznačajnih primena ciklotomičnih polinoma je dokaz Vederburnove teoreme o komutativnosti konačnih tela.

Definicija 4.1. Telo je prsten u kom su jednakosti $ax = b$ i $bx = a$ jedinstveno rešive za svako $a \neq 0$.

Naravno, ako $b \neq 0 \neq a$, rešenje jednačine $ax = b$ ne može biti $x = 0$, jer $a0 = 0$ važi u svakom prstenu. Slično za $xa = b$. Dakle, ako je R telo, $(R \setminus \{0\}; \cdot)$ je kvazigrupa.

Lema 4.1. *Ako je R prsten sa jedinicom 1 i $1 \in F \subseteq R$ potpolje od R, onda je R vektorski prostor nad F.*

Dokaz. $(R; +)$ je Abelova grupa, a ostale osobine vektorskog prostora slede iz asocijativnosti množenja, distributivnosti množenja prema sabiranju i činjenice da jedinica R pripada F. □

Treba nam još nekoliko činjenica o telima koje se ne uče na standardnim kursevima algebre, ali se dokazuju isto kao poznate teoreme o poljima. Samo ih navodimo bez dokaza. Ako je R telo, kažemo da je M modul nad tim telom ako je $(M; +)$ Abelova grupa, a elementi R množe elemente M sa osobinama kao u slučaju vektorskog prostora (sem što međusobno množenje elemenata tela ne mora biti komutativno). Tada M ima bazu nad R, dakle linearno nezavisan skup elemenata $B \subseteq M$ takav da se svaki element M može na jedinstven način napisati kao linearna kombinacija elemenata iz B. Sve baze M nad R imaju istu kardinalnost i ako je baza B konačna, $|B| = n$ onda

$|M| = |R|^n$. Sve ovo se dokazuje potpuno analogno kao u Linearnoj algebri, a ne mora da važi ako je M modul nad prstenom R koji nije telo.

Konačno, podsećamo se nekih činjenica iz Teorije grupa.

Lema 4.2. *Neka je G konačna grupa i $x \in G$. Sa*

$$C_G(x) = \{y \in R \mid xy = yx\}$$

obeležavamo centralizator *elementa x, dok sa*

$$O_x = \left\{yxy^{-1} \mid y \in R^*\right\}$$

obeležavamo klasu konjugacije *ili* orbitu *elementa x [konkretnije, orbitu u odnosu na konjugaciju]. Tada je $C_G(x)$ podgrupa od G i važi*

$$|O_x| = [G : C_G(x)] = \frac{|G|}{|C_G(x)|}.$$

Skica dokaza. Dokaz da je $C_G(x)$ podgrupa od G ide po definiciji, gde zatvorenost za inverze dobijamo tako što jednakost $gx = xg$ pomnožimo sa obe strane sa g^{-1}. Preslikavanje $\varphi : G \mapsto O_x$ dato sa $\varphi(g) = gxg^{-1}$ je sirjektivno (očigledno), i važi $\varphi(g) = \varphi(h)$ akko $gxg^{-1} = hxh^{-1}$ akko $h^{-1}gx = xh^{-1}g$ akko $h^{-1}g \in C_G(x)$ akko $gC_G(x) = hC_G(x)$. Dakle, jezgro $\ker\varphi$ je desna kongruencija po modulu podgrupe $C_G(x)$, pa $|O_x| = [G : C_G(x)]$. □

Napominjemo da je $\{O_x : x \in G\}$ particija skupa G i da $|O_x| = 1$ akko $x \in Z(G)$.

Teorema 4.3. *Neka je G konačna grupa, a T transverzala svih klasa konjugovanosti koje imaju više od jednog elementa (dakle svih klasa konjugovanosti koje nisu u centru $Z(G)$). Tada*

$$|G| = |Z(G)| + \sum_{x \in T} [G : C_G(x)].$$

Dokaz. Kako je $Z(G)$ transverzala svih klasa konjugovanosti koje su jednoelementne (videti napomenu pre teoreme), a T transverzala svih klasa konjugovanosti koje imaju više od jednog elementa, i kako klase konjugovanosti čine particiju skupa G, dobijamo

$$|G| = \sum_{x \in T \cup Z(G)} |O_x| = \sum_{x \in Z(G)} |O_x| + \sum_{x \in T} |O_x| = |Z(G)| + \sum_{x \in T} [G : C_G(x)].$$

Poslednja jednakost važi na osnovu leme 4.2. □

Teorema 4.4. *Svako konačno telo R je komutativno.*

Dokaz. Kako je $R \setminus \{0\}$ kvazigrupa i polugrupa, onda je grupa. Dakle R ima jedinicu 1 i nema delitelje nule. Karakteristika je stoga prost broj p i za sve $a \neq 0$ važi $pa = 0$ i $red(a) = p$. Razmotrimo potprsten generisan sa 1. Taj potprsten je komutativno telo, dakle polje Z_p sa p elemenata. Lema 4.1 nam kaže da je telo R vektorski prostor nad F_p. Ako je r dimenzija ovog prostora, onda R sadrži p^r elemenata. Neka je Z centar polja R, tj. skup elemenata iz R koji komutiraju sa svim elementima iz R. Tada je Z polje koje sadrži F_p, što znači da Z ima $q = p^s$ elemenata. Telo R je takođe vektorski prostor nad Z. Ako je dimenzija polja R nad Z jednako t, onda R sadrži q^t elemenata, odnosno $p^r = q^t = p^{st}$. Hoćemo da pokažemo da je $R = Z$, tj. da je $t = 1$. Time ćemo pokazati da svi elementi iz R međusobno komutiraju.

Za svaki element x iz R, razmotrimo centralizator

$$C_R(x) = \{y \in R \mid xy = yx\}.$$

Jasno je da je $C_R(x)$ zatvoren za množenje i razliku, pa je $C_R(x)$ potprsten od R koje sadrži Z. Takođe, iz leme 4.2 sledi da je $C_R(x)$ zatvoren i za inverze svojih nenula elemenata, pa je $C_R(x)$ podtelo od R.

S jedne strane, telo $C_R(x)$ je vektorski prostor nad Z i sadrži q^{d_x} elemenata, gde je d_x prirodan broj koji zavisi od x, a sa druge strane, R je modul nad $C_R(x)$, pa je $q^t = (q^{d_x})^k = q^{d_x k}$, tj. $d_x | t$. Za svaku klasu konjugovanosti O_x elementa $x \in R^*$ imamo $\mid O_x \mid = \frac{|R^*|}{|C_R(x)\setminus\{0\}|} = \frac{q^t-1}{q^{d_x}-1}$. Klasovna jednačina primenjena na multiplikativnu grupu R^* daje

$$|R^*| = q^t - 1 = (q-1) + \sum \frac{q^t - 1}{q^{d_x} - 1}, \tag{4.1}$$

gde suma ide po orbitama za koje je $d_x < t$ ($d_x = t$ odgovara elementima Z kojih ima $q-1$ u R^*). Pomoću ciklotomičnih polinoma $\Phi_t(x)$ dokazujemo da je jednakost (4.1) moguća samo za $t = 1$. Zaista, polinom $x^t - 1$ je deljiv sa $\Phi_t(x)$. Pored toga, ako $d_x | t$ i $d_x < t$, onda $x^{d_x} - 1$ i $\Phi_t(x)$ nemaju zajedničkih korena (svi koreni $\Phi_t(x)$ su primitivni t-ti koreni iz jedinice, a koreni $x^{d_x} - 1$ nisu, jer $d_x < t$). Dakle, polinomi $\frac{x^t-1}{x^{d_x}-1}$ su deljivi sa $\Phi_t(x)$. Stoga, brojevi $q^t - 1$ i svi $\frac{q^t-1}{q^{d_x}-1}$ su deljivi sa $\Phi_t(q)$. Iz (4.1) sledi da $\Phi_t(q) \mid (q-1)$.
S druge strane, $\mid \Phi_t(q) \mid = \prod \mid q - \varepsilon_i \mid > q - 1$, jer je $\mid \varepsilon_i \mid = 1$ i $\varepsilon_i \neq 1$. □

Glava 5

Žigmondijeva teorema

Cilj ove glave je da dokažemo sledeću teoremu Žigmondija:

Teorema 5.1. *Neka su a i n prirodni brojevi veći od 1. Tada postoji prost delilac p od $a^n - 1$ takav da $o_p(a) = n$, sem u slučajevima kada je $n = 2$, $a = 2^s - 1$, gde je $s \geq 2$ ili $n = 6$, $a = 2$.*

Na osnovu teoreme 3.23, možemo posmatrati polinom $\Phi_n(a)$ i njegovu deljivost sa p. Pre nego što dokažemo samu teoremu, dokazaćemo dve leme koja će nam koristiti u dokazu. Za dokaz prve leme koristiće se i poznata Lema o podizanju stepena (Lifting the Exponent Lemma - LTE), pa ćemo prvo nju formulisati i dokazati. Budući da nas interesuje lema o podizanju stepena za neparan prost broj, nju ćemo dokazati, dok ćemo lemu vezanu za prost broj 2 samo formulisati.

Najveći stepen prostog broja p koji deli a označavaćemo sa $v_p(a)$, tj. ako je $v_p(x) = \alpha$ onda $p^\alpha | x$ i $p^{\alpha+1} \nmid x$.

Teorema 5.2. ***Lema o podizanju stepena za*** $p = 2$ *Neka su x i y neparni celi brojevi takvi da $4|x - y$. Tada*

$$v_2(x^n - y^n) = v_2(x - y) + v_2(n).$$

Teorema 5.3. ***Lema o podizanju stepena*** *Neka su x i y celi brojevi, n pozitivan ceo broj i p neparan prost broj takav da $p|x - y$ i $p \nmid x$ i $p \nmid y$. Tada*

$$v_p(x^n - y^n) = v_p(x - y) + v_p(n).$$

Dokaz. Dokazaćemo indukcijom po $v_p(n)$. Prethodno pokazujemo jedno tvrđenje koje će nam koristiti u dokazu baze:

$$p|x^{n-1}+x^{n-2}y+...+xy^{n-2}+y^{n-1} \text{ akko } p|n.$$

Kako je $x-y\equiv 0\ (mod\ p)$, tj. $x\equiv y\ (mod\ p)$ onda je $x^{n-1}+x^{n-2}y+...+xy^{n-2}+y^{n-1}\equiv x^{n-1}+x^{n-2}x+...+x\cdot x^{n-2}+x^{n-1}\equiv n\cdot x^{p-1}$. Znamo da važi $p\nmid x$, pa $p|x^{n-1}+x^{n-2}y+...+xy^{n-2}+y^{n-1}$ akko $p|n\cdot x^{p-1}$ akko $p|n$, čime je tvrđenje dokazano.

Treba nam sada baza indukcije $v_p(n)=0$, kao i specijalan slučaj $n=p$. Ako $v_p(n)=0$, onda $p\nmid n$, pa je

$$v_p(x^n-y^n)=v_p((x-y)(x^{n-1}+x^{n-2}y+...+xy^{n-2}+y^{n-1}))=$$
$$v_p(x-y)+v_p(x^{n-1}+x^{n-2}y+...+xy^{n-2}+y^{n-1})=v_p(x-y),$$

gde poslednja jednakost sledi na osnovu tvrđenja, pa je baza dokazana.

Sad dokazujemo $v_p(x^p-y^p)=v_p(x-y)+1$. Treba da dokažemo dve stvari, da

$$p|x^{p-1}+x^{p-2}y+...+xy^{p-2}+y^{p-1}$$

i da

$$p^2\nmid x^{p-1}+x^{p-2}y+...+xy^{p-2}+y^{p-1}.$$

Prvo smo dokazali u tvrđenju, pa preostaje drugo.

Neka je $y=x+kp$, gde je k ceo broj. Za ceo broj t, $1\leq t<p$ će biti

$$x^{p-1-t}\cdot y^t\equiv x^{p-1-t}\cdot(x+kp)^t\equiv x^{p-1-t}(x^t+t\cdot kp\cdot x^{p-1}+\tfrac{t(t-1)}{2}(kp)^2\cdot x^{t-2}+...)\equiv$$
$$x^{p-1-t}(x^t+t(kp)x^{t-1})\equiv x^{p-1}+t(kp)x^{p-2}\ (mod\ p^2).$$

Koristeći ovo, dobijamo

$$x^{p-1}+x^{p-2}y+...+xy^{p-2}+y^{p-1}\equiv x^{p-1}+(x^{p-1}+1\cdot kp\cdot x^{p-2})+(x^{p-1}+2kp\cdot x^{p-2})+...+(x^{p-1}+(p-1)kp\cdot x^{p-2})\equiv p\cdot x^{p-1}+(1+2+...+(p-1))kp\cdot x^{p-2}\equiv$$
$$px^{p-1}+\tfrac{p(p-1)}{2}kp\cdot x^{p-2}\equiv px^{p-1}+\tfrac{p-1}{2}kp^2\cdot x^{p-2}\equiv px^{p-1},$$

a to nije ekvivalento sa 0 po modulu p^2 jer $p\nmid x$. Dakle, dokazali smo da je $v_p(x^p-y^p)=v_p(x-y)+1$.

Prelazimo na dokaz induktivnog koraka. Pretpostavimo da je $n=p^\alpha\cdot b$, gde je $\alpha\geq 1$ i $(p,b)=1$. Tada je

$$v_p(x^n-y^n)=v_p((x^{p^\alpha})^b-(y^{p^\alpha})^b)=v_p(x^{p^\alpha}-y^{p^\alpha})=v_p((x^{p^{\alpha-1}})^p-(y^{p^{\alpha-1}})^p)=$$
$$v_p(x^{p^{\alpha-1}}-y^{p^{\alpha-1}})+1=v_p((x^{p^{\alpha-2}})^p-(y^{p^{\alpha-2}})^p)+1=v_p(x^{p^{\alpha-2}}-y^{p^{\alpha-2}})+2=$$
$$...=v_p((x^1)^p-(y^1)^p)+\alpha-1=v_p(x-y)+\alpha=v_p(x-y)+v_p(n)$$

U drugoj jednakosti koristili smo bazu indukcije, a u četvrtoj specijalan slučaj $n = p$. □

Lema 5.4. *Neka su a i n prirodni brojevi veći od 1. Ako su svi prosti delioci od $\Phi_n(a)$ ujedno i delioci broja n, tada je $\Phi_n(a)$ prost broj koji deli n ili je $n = 2$.*

Dokaz. Neka je p proizvoljan prost broj takav da $p|\Phi_n(a)$. Iz uslova leme sledi da $p|n$. Takođe, znamo da su p i a uzajamno prosti brojevi zato što je konstantan član u $\Phi_n(x)$ jedinica. Neka je $k = o_p(a)$. Dakle, $1 \leq k < p$, pa su k i p uzajamno prosti.

Kako važi $(k, p) = 1$, na osnovu teoreme 3.23 važi da $p|\Phi_k(a)$. Iz $k < p \leq n$ dobijamo da $k \neq n$, a znamo i da $p|\Phi_k(a)$ i $p|\Phi_n(a)$, pa su ispunjeni uslovi za primenu teoreme 3.26. Iz te teoreme sledi da je $\frac{n}{k} = p^t$ za neki prirodan broj $t > 0$. Dalje je

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

za neki polinom $Q(x)$. Primetimo da $x^{\frac{n}{p}} - 1 | Q(x)$, jer su svi koreni polinoma $x^{\frac{n}{p}} - 1$ n-ti koreni iz jedinice koji nisu primitivni.
Ako je p neparan prost broj tada tvrdimo da je $v_p(a^n - 1) = v_p(a^{\frac{n}{p}} - 1) + 1$. Naime, $p|a^k - 1$, a znamo da $k|\frac{n}{p}$, pošto su k i p uzajamno prosti (zato što $k|p - 1$), pa sledi da $p|a^{\frac{n}{p}} - 1$. Sa druge strane, naravno da $p \nmid 1$, a stoga i $p \nmid a^{\frac{n}{p}}$. Vidimo da su ispunjeni uslovi za primenu Leme o podizanju stepena koja za neparan prost broj p daje drugu jednakost u sledećem nizu:

$$v_p(a^n - 1) = v_p((a^{\frac{n}{p}})^p - 1^p) = v_p(a^{\frac{n}{p}} - 1) + v_p(p) = v_p(a^{\frac{n}{p}} - 1) + 1.$$

Kako $(a^{\frac{n}{p}} - 1)\Phi_n(a) | (a^n - 1)$, onda je stepen broja p koji deli $\Phi_n(a)$ najviše 1. Ali, mi znamo da $p|\Phi_n(a)$, pa je stepen broja p koji deli $\Phi_n(a)$ tačno 1.
Neka su p i q prosti brojevi takvi da i p i q dele $\Phi_n(a)$. Tada i p i q dele n, pa primenom gornjeg argumenta i na jednog i na drugog dobijamo da je

$$n = p^{a_1} k_1 = q^{a_2} k_2,$$

gde je $k_1 = o_p(a)$ i $k_2 = o_q(a)$.
Primetimo da $\frac{n}{p^{a_1}} = k_1 | p - 1$ i $\frac{n}{q^{a_2}} = k_2 | q - 1$. U tom slučaju, iz $q|k_1$ sledi da $q|(p - 1)$, a iz $p|k_2$ sledi da $p|(q - 1)$. Dakle, $q \leq p - 1$, a $p \leq q - 1$, što je nemoguće. Iz ovoga sledi da $\Phi_n(a)$ ima najviše jedan prost faktor i ako je neparan, onda je $\Phi_n(a)$ prost.

Pretpostavimo da je $\Phi_n(a)$ paran broj, dakle $\Phi_n(a)$ je stepen dvojke. Očigledno je da je $k = o_2(a) = 1$, pa sledi da je $n = 2^t$. U tom slučaju se indukcijom lako pokazuje da je $\Phi_{2^t}(a) = a^{2^{t-1}} + 1 \equiv 2$ po modulu 4, kada je $n \neq 2$. Dakle, kada je $n \neq 2$ važi da 4 ne deli $\Phi_n(a)$, odakle sledi tvrđenje. □

Lema 5.5. *Neka su a, n prirodni brojevi veći od 1. Neka je $n = p^k r$, gde je $k > 0$, a p je prost broj koji ne deli r. Tada je*

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

gde je $b = a^{p^{k-1}}$.

Dokaz. Na osnovu posledice 3.15 znamo da je

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

Prvo dokazujemo slučaj kad $n = p^k$, odnosno $r = 1$. Tada $\varphi(r) = 1$, $\Phi_r(x) = x - 1$ i

$$\Phi_n(a) = \frac{b^p - 1}{b-1} = \frac{a^{p^k} - 1}{a^{p^{k-1}} - 1} = \sum_{i=0}^{k-1} a^{ip^{k-1}} = 1 + a^{p^{k-1}} + \cdots + a^{(p-1)p^{k-1}} >$$
$$a^{(p-1)p^{k-1}} = b^{p-1} > b^{p-1} - b^{p-2} = (b^{p-2}(b-1))^{\varphi(r)}.$$

Sad pretpostavljamo da $r > 1$, tj. da n nije stepen prostog broja. Tada, znamo da je $\Phi_r(b^p) = \prod_{\substack{ord(\varepsilon)=r \\ \varepsilon^r=1}} (b^p - \varepsilon)$ i da u proizvodu ima $\varphi(r)$ činilaca (pošto ima $\varphi(r)$ primitivnih $r-$tih korena iz jedinice). Takođe, za sve te ε koji učestvuju u gornjem proizvodu znamo da $\varepsilon \neq 1$ jer $r > 1$, pa 1 nije primitivni r-ti koren iz jedinice. Dalje, moduo svakog od izraza $|b^p - \varepsilon|$ je veći od $b^p - 1$ (sledi iz nejednakosti trougla, jer $|\varepsilon| = 1$ i znamo da $\varepsilon \neq 1$). Iz neprekidnosti $\Phi_n(x)$, kako nema nula na realnom intervalu $[b^p, +\infty)$ i kako je $\lim_{x \to +\infty} \Phi_n(x) = +\infty$ (ovo poslednje jer je vodeći koeficijent polinoma $\Phi_n(x)$ jedinica, dakle pozitivan je), zaključujemo da je $\Phi_r(b^p) > 0$. Stoga dobijamo

$$\Phi_r(b^p) = |\Phi_r(b^p)| = \prod_{\substack{ord(\varepsilon)=r \\ \varepsilon^r=1}} |b^p - \varepsilon)| > (b^p - 1)^{\varphi(r)}.$$

Slično je $\Phi_r(b) < (b+1)^{\varphi(r)}$, jer $\Phi_r(b) = \prod_{\substack{ord(\varepsilon)=r \\ \varepsilon^r=1}} (b - \varepsilon)$, u proizvodu ima $\varphi(r)$ izraza i moduo svakog od njih je manji od $b+1$. Ubacivanjem $\Phi_r(b^p) > (b^p - 1)^{\varphi(r)}$ i $\Phi_r(b) < (b+1)^{\varphi(r)}$ u gornju jednakost dobijamo

$$\Phi_n(a) = \frac{\Phi_r(b^p)}{\Phi_r(b)} > \left(\frac{b^p-1}{b+1}\right)^{\varphi(r)}.$$

Ako iskoristimo da je $b^p - 1 > b^{p-2}(b^2-1)$ dobijamo sledeće

$$\Phi_n(a) \geq \left(\frac{b^p-1}{b+1}\right)^{\varphi(r)} > \left(\frac{b^{p-2}(b^2-1)}{b+1}\right)^{\varphi(r)} = \left(\frac{b^{p-1}(b-1)(b+1)}{b+1}\right)^{\varphi(r)} = \left(b^{p-2}(b-1)\right)^{\varphi(r)}.$$

□

Vratimo se na dokaz Žigmondijeve teoreme.

Dokaz. Za $n = 2$ proveravamo navedeni izuzetak ubacivanjem vrednosti. Znamo da je p prost broj koji deli $a^2 - 1 = (a-1)(a+1)$. Ako $p|a-1$, onda je $o_p(a) = 1$, pa $o_p(a) \neq 2 = n$. Dakle, mora biti $p|a+1$. Ako je a oblika $2^s - 1$, onda $p|(2^s-1)+1 = 2^s$. Jedini prost faktor koji deli ovaj izraz jeste $p = 2$, ali u tom slučaju nije $o_2(a) = 2$, jer je $(2^s-1)^1 \equiv 1$ po modulu $p = 2$, pa je $o_2(a) = 1$. Time je izuzetak potvrđen. Sa druge strane, ako a nije oblika $2^s - 1$ i $n = 2$, onda $a+1$ ima neki neparan prost faktor p i $a \equiv -1 \ (mod\ p)$, pa $o_p(a) = 2 = n$. Dakle, za $n = 2$ teorema važi za a koji nisu oblika $2^s - 1$, a ne važi za a koji su oblika $2^s - 1$.

Pretpostavimo da je $n > 2$. Ako pretpostavimo da postoji prost broj p takav da $p|\Phi_n(a)$ i p ne deli n, onda na osnovu teoreme 3.23 znači da je $o_p(a) = n$, što i treba da dokažemo.

Preostaje nam slučaj kada $n > 2$ i za svaki prost broj p za koji deli $\Phi_p(a)$ važi da p deli n. Tada na osnovu leme 5.4 važi da je $\Phi_n(a) = q$ za neki prost broj q koji deli n.

Neka je $n = q^k r$, gde q ne deli r. Na osnovu leme 5.5 znamo da je

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

gde je $b = a^{q^{k-1}}$. Ako je $q \geq 5$ tada važi da je $b^{q-2} > q$ za sve cele brojeve b. Ovo ćemo pokazati indkucijom po q, ali ćemo prvo pokazati da je $b > 1$. Znamo da je $a > 1$ i da je $k > 0$ (jer $p|n$), pa je $p^{k-1} \geq p^0 = 1$, iz čega sledi da je $b = a^{p^{k-1}} \geq a^1 = a > 1$. Vraćamo se na indukciju po q. Dokazujemo da

za sve prirodne brojeve $q \geq 5$ važi $b^{q-2} > q$. Za b znamo da je prirodan broj veći od 1, pa važi da je $b \geq 2$. Za $q = 5$ je

$$b^{q-2} = b^3 \geq 2^3 = 8 > 5,$$

pa baza $q = 5$ važi.
Pretpostavimo da važi $b^{q-2} > q$ i dokažimo da važi $b^{(q+1)-2} > q + 1$.

$$b^{(q+1)-2} = b^{(q-2)+1} = b \cdot b^{q-2} \geq 2 \cdot b^{q-2} > 2q \geq q + 5 \geq q + 1.$$

Ovim smo pokazali da je $b^{q-2} > q$, pa je i $(b^{q-2}(b-1))^{\varphi(r)} > q$. Ostaje samo da proverimo za $q = 3$. Ako je $q = 3$, izraz sa desne strane postaje $(b(b-1))^{\varphi(r)}$, gde je $b = a^{3^{k-1}}$. Pošto je a prirodan broj veći od 1, najmanje što može biti je 2. Ako uzmemo bilo koji veći broj od 2, imaćemo da desna strana nije manja od 3, pa a mora biti 2. Tada je $k = 1$ i $\varphi(r) = 1$, inače opet imamo da je desna strana veća od 3, dakle $k = 1$ i $r = 1$ ili $r = 2$. Sada računamo koliko je n. $n = q^k \cdot r$, tj. $n = 3^1 \cdot 1 = 3$ ili $n = 3^1 \cdot 2 = 6$. U slučaju kada je $n = 3$, proveravanjem dobijamo da $a^n - 1 = 2^3 - 1 = 7$ i za $p = 7$ $o_p(a) = o_7(2) = 3 = n$, pa tvrđenje važi. Međutim, u slučaju kada je $a = 2$ i $n = 6$ dobijamo da $a^n - 1 = 2^6 - 1 = 63$, prosti delioci od 63 su 7 i 3, $o_3(a) = o_3(2) = 2 \neq 6 = n$ i $o_7(a) = o_7(2) = 3 \neq 6 = n$, pa tvrđenje ne važi, čime je i drugi izuzetak dokazan. □

Navešćemo još samo generalizaciju tj. punu formu Žigmondijeve teoreme. Daćemo teoremu bez dokaza.

Teorema 5.6. *Neka su a, b i n prirodni brojevi takvi da je $n > 1$ i $a > b > 0$. Tada postoji prost broj q koji je delilac polinoma $a^n - b^n$ takav da q ne deli $a^j - b^j$ za svako j, $0 < j < n$, sem u slučajevima kad je $n = 2$, $a + b = 2^s$ gde je $s \geq 2$ i $n = 6$, $a = 2$ i $b = 1$.*

Literatura

[1] Vukašin Brković, *Ciklotomični polinomi*, Matematička gimnazija, Beograd, maturski rad, Jun 2013.
https://imomath.com/srb/dodatne/ciklotomicni_brkovic.pdf

[2] Victor V. Prasolov, *Polynomials* (2.izdanje), Springer 2010.

[3] Milan Z. Grulović, *Predavanja iz Algebre 4*, Departman za matematiku i informatiku PMF Novi Sad, 2017.
https://www.researchgate.net/publication/321151760_Predavanja_iz_Algebre_4

[4] Paramanand's Math Notes, *Gauss and Regular Polygons: Cyclotomic Polynomials*, 2009.
paramanands.blogspot.com/2009/12/gauss-and-regular-polygons-cyclotomic-polynomials.html#.XrLOS6gzZPY

Biografija

Jovana Tomik Ognjenović rođena je 21.9.1992. godine u Šapcu, Srbija. Osnovnu školu „Čaki Lajoš" u Bačkoj Topoli završila je 2007. godine kao nosilac Vukove diplome. Zatim je upisala opšti smer gimnazije u Gimnaziji i ekonomskoj školi „Dositej Obradović" u Bačkoj Topoli. Nakon završetka iste 2011. godine, upisala je osnovne akademske studije matematike na Departmanu za matematiku i informatiku, Prirodno-matematičkog fakulteta u Novom Sadu, smer Diplomirani profesor matematike. Studije je završila 2016. godine sa prosečnom ocenom 8.49. Master studije upisala je iste godine na istom fakultetu, smer Master profesor matematike. Godine 2017. dobija sina Luku, a 2019. sina Aleksu. Sve ispite predviđene planom i programom položila je 2019. godine sa prosečnom ocenom 8.05, čime je stekla uslov za odbranu master rada i završetak studija.

Novi Sad, 2020. Jovana Tomik Ognjenović

UNIVERZITET U NOVOM SADU
PRIRODNO–MATEMATIČKI FAKULTET
KLJUČNA DOKUMENTACIJSKA INFORMACIJA

Redni broj:
RBR

Identifikacioni broj:
IBR

Tip dokumentacije: Monografska dokumentacija
TD

Tip zapisa: Tekstualni štampani materijal
TZ

Vrsta rada: Master rad
VR

Autor: Jovana Tomik Ognjenović
AU

Mentor: dr Petar Marković, redovni profesor
MN

Naslov rada: Ciklotomični polinomi **NR**

Jezik publikacije: srpski (latinica)
JP

Jezik izvoda: srpski
JI

Zemlja publikovanja: Republika Srbija
ZP

Uže geografsko područje: Vojvodina
UGP

Godina: 2020.
GO

Izdavač: Autorski reprint
IZ

Mesto i adresa: Departman za matematiku i informatiku, Prirodno–matematički fakultet, Univerzitet u Novom Sadu, Trg Dositeja Obradovića 4, Novi Sad
MA

Fizički opis rada: (5, 49, 4, 0, 0, 0, 0)
FO

Naučna oblast: Matematika
NO

Naučna disciplina: Algebra
ND

Ključne reči: Primitivni koren, Ciklotomični polinom, Nesvodljivost, Vederburnova teorema, Žigmondijeva teorema
PO

UDK:

Čuva se: Biblioteka Departmana za matematiku i informatiku Prirodno–matematičkog fakulteta Univerziteta u Novom Sadu
ČU

Važna napomena:
VN

Izvod:
IZ

U ovom master radu bavimo se ciklotomičnim polinomima. U prvom delu rada podsetićemo se pojmova kao što su Mebijusova funkcija i nekih njenih osobina, pojma primitivnog korena, kao i nekih osnovnih osobina polinoma, radi lakšeg razumevanja teme. U drugom delu rada (od trećeg poglavlja pa nadalje) bavimo se isključivo ciklotomičnim polinomima i dokazivanju osobina i njihove nesvodljivosti. Biće reči i o vezi ciklotomičnih polinoma i reda broja po prostom modulu, kao i o primeni ciklotomičnih polinoma u dokazivanju poznatih teorema, kao što su Vederburnova i Žigmondijeva teorema

Datum prihvatanja teme od strane NN veća: 19.06.2020.
DP

Datum odbrane:
DO

Članovi komisije:
KO

Predsednik:	Dr Bojan Bašić, vanredni profesor, Prirodno-matematički fakultet, Univerzitet u Novom Sadu
Član:	dr Petar Đapić, vanredni profesor, Prirodno-matematički fakultet, Univerzitet u Novom Sadu
Član:	dr Petar Marković, redovni profesor, Prirodno-matematički fakultet, Univerzitet u Novom Sadu, mentor