Математички факултет
Универзитет у Београду

Раде Лукић

Циклотомични полиноми у настави средње школе

Мастер рад

Ментор: др Ђорђе Кртинић

Београд,
2015.

Садржај

Глава 1

УВОД

У овом мастер раду обрађени су циклотомични полиноми и појмови неопходни за њихово увођење и разумевање. Основна намера била је да се осим самих дефиниција, тврђења и њихових доказа, обради и задовољавајући број примера, како би се ова тема приближила циљаном аудиторијуму - средњошколцима и њиховим професорима. Наиме, редак је случај да се поменута тематика обрађује на додатној настави, а још ређе редовној, ван специјализованих гимназија. Стога на овај мастер рад, у случају реалног остваривања жељеног циља, можемо гледати и као на озбиљан покушај обогаћивања литературе за припрему средњошколских такмичења и мотивације средњошколаца да уче и примењују математику.

Друга глава садржи основне појмове везане за мултипликативне функције, примитивне корене из јединице, основне ставове и бројне примере, који уводе читаоца у материјал, обрађен у трећој глави. Одабир примера је првенствено окренут илустровању дефинисаних појмова, а потом и доказивању неких озбиљнијих тврђења које их повезују. Ово и јесте разлог зашто најпре наводимо примере са врло конкретним вредностима одговарајућих параметара, а тек онда ширимо слику о дубљој вези појмова које обрађујемо.

Трећа глава је нешто конкретнија, јер обрађујемо највећи број тврђења која касније користимо и која и представљају срж овог рада. Ипак, да останемо при примарној сврси, увод у тему започињемо обнављањем неопходног стандардног градива из средњошколске наставе, који се при овоме користи. При том, очекујући познавање потребне материје, ову рекапитулацију вршимо кроз примере, омогућавајући увид читаоца у директну примену.

Четврта глава доноси већи број сложенијих примера, који непосредно користе тврђења детаљно обрађена у претходном поглављу. Са основом припремљеном теоријским разматрањима у овом раду, ова прилика је, према надањима аутора, и искоришћена па је обрађен знатан број примера какви

се појављују на средњошколским такмичењима. Још већи значај лежи у чињеници да се аргументација из ових примера врло често без већих проблема преноси и на општије алгебарске структуре и да се њеним разумевањем, код ученика може мотивисати даљи напредак и жеља за стицањем нових знања на обрађену тему.

Велики број тврђења је доказан, па материјал може бити користан за учење основних ствари на ову тему. Међутим, за заинтересованог читаоца, рад је, пре свега, прилика за упознавање са овом тематиком и могућностима ове технике. Ни у ком случају нису постојале претензије за исцрпним обрађивањем овако озбиљне и дубоке математике. За даље продубљивање знања, читаоца можемо упутити на наведену литературу.

Овај рад, наравно није само дело аутора, озбиљну улогу одиграо је и ментор др Ђорђе Кртинић, корисним сугестијама које су сигурно утицале да рад добије естетски прихватљивији облик и форму примерену циљаној публици. На овом месту му се аутор и срдачно захваљује. Коначно, могуће и сигурно присутне грешке припадају одговорности само аутора и никог другог.

Глава 2

Примитивни корени и циклотомични полиноми

Ово поглавље је уводног карактера. У њему ћемо дефинисати основне појмове које користимо у раду, навести формулације и доказе ставова који ове појмове повезују и тако дати основу за проучавање циклотомичних полинома. Испоставиће се да овим добијамо врло важну технику, често врло мало, а понекад нимало обрађивану на редовној и додатној настави у средњој школи. Овде се мање-више детаљно уводе и кроз примере обрађују неке најважније мултипликативне функције, затим централни појмови примитивног корена и циклотомичног полинома и основна тврђења. Овим добијамо неопходну основу за разматрања у наредном поглављу. Кренућемо од примитивног корена, будући да се и сам појављује у дефиницији циклотомичног полинома, који је предмет изучавања.

2.1 Примитивни корен и мултипликативне функције

У жељи да се што брже припремимо за врло конкретна разматрања, наводимо уводну дефиницију n-тог корена.

Дефиниција 2.1.1. Нека је $n \in \mathbb{N}$. Комплексан број ω називамо n-тим кореном из јединице ако задовољава једнакост

$$\omega^n = 1.$$

Да ствар буде јаснија, израчунаћемо n-те корене за дати $n \in \mathbb{N}$.

Пример 2.1. Решења једначине $x^n - 1 = 0$ су

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

Решење. Наиме, x_k и рачунамо, применом Муаврове формуле као:

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

а како, према Основној теореми алгебре, полином n-тог степена има тачно n комплексних нула, рачунајући и њихову вишеструкост, то су x_k-ови и све нуле полинома x^n-1. □

Занимљиво је приметити и како скуп n-тих корена изгледа представљен у комплексној равни.

Пример 2.2. Наћи геометријску интерпретацију скупа нула полинома x^n-1.

Решење. Видели смо да су корени полинома x^n-1 дати са

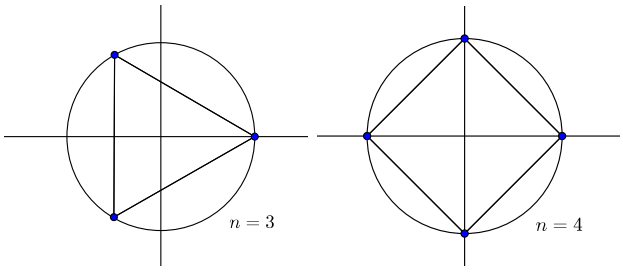
$$x_k = \cos\frac{2k\pi}{n}+i\sin\frac{2k\pi}{n}.$$

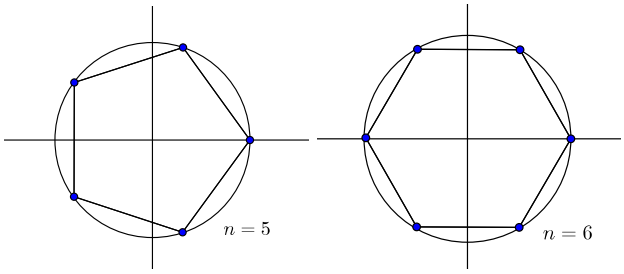
Будући да су сви n наведених бројева облика $\cos\theta+i\sin\theta$, $\theta\in\mathbb{R}$, њихов модуо је $\sqrt{\cos^2\theta+\sin^2\theta}=1$. Стога се сви налазе на јединичном кругу. Прецизнију информацију о њиховом распореду на јединичном кругу добијамо из чињенице да је растојање суседних елемената у низу $x_0, x_1, \ldots, x_{n-1}$ константно.

Наиме, за $1\leqslant k\leqslant n$

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

Знајући и да је $x_0=1$, добијамо да су x_k-ови тачке на јединичној кружници такве да су суседне међу њима међусобно подједнако удаљене међу којима је $x_0=1$ прва у низу, па наведени корени јесу темена правилног n-тоугла.
За конкретне вредности, слика 2.1 илуструје поменуте скупове n-тих корена.





Слика 2.1: Слика уз пример 2.2

Обојене тачке на кружници су корени полинома $x^n - 1$. □

А сад, још један неопходан појам.

Дефиниција 2.1.2. Нека је ω n-ти корен из јединице, за произвољно $n \in \mathbb{N}$. Тада најмањи број k такав да важи $\omega^k = 1$ називамо редом броја ω и означавамо са $r(\omega)$.

Једна очекивана веза реда броја ω и n, дата је следећом лемом.

Лема 2.1.1. Нека је n природан број и ω произвољан n-ти корен из јединице. Тада за неки цео број k важи $\omega^k = 1$ ако и само ако $r(\omega) \mid k$. Специјално $r(\omega) \mid n$.

Доказ. Нека је $t = r(\omega)$. Ако $t \mid k$, тада важи $\omega^k = (\omega^t)^{\frac{k}{t}} = 1$. За други смер нека важи $\omega^k = 1$, и нека је $k = at + b$, где је $0 \leqslant b \leqslant t - 1$. Одавде имамо да је $1 = \omega^{at+b} = (\omega^t)^a \omega^b = \omega^b$, одакле добијамо $\omega^b = 1$, па пошто је $b < t = r(\omega)$, то је $b = 0$, то јест $k = at$ што је и требало добити. □

Последица. Лако се види и да је $\omega^k = \omega^l$ ако и само ако $k \equiv l \pmod{t}$. Специјално за $1 \leqslant k, l \leqslant t$ важи и $k = l$.

Међу n-тим коренима од посебног интереса за нас су већ најављивани примитивни корени. Сада смо у могућности и да их уведемо.

Дефиниција 2.1.3. Нека је ω n-ти корен из јединице, за неко $n \in \mathbb{N}$. Уколико важи $r(\omega) = n$, онда ω називамо примитивним n-тим кореном из јединице.

Ови корени имају "генеришуће" својство. Тачан смисао овог својства даје следећа лема.

Лема 2.1.2. Нека је ω примитивни n-ти корен из јединице, за неко $n \in \mathbb{N}$. Тада је скуп $\{\omega, \omega^2, \ldots, \omega^n\}$, скуп свих n-тих корена из јединице.

Доказ. Како је $(\omega^k)^n = (\omega^n)^k = 1$ то је и ω^k n-ти корен из јединице. Како су бројеви $\omega, \omega^2, \ldots, \omega^n$ међусобно различити (што се види из последице леме 2.1.1 и дефиниције 2.1.3) и има их n, то они представљају све n-те корене. □

Примитивни корени из јединице имају врло специфичан облик и могу бити генерисани познавањем једног таквог. Наиме, важи следећа лема.

Лема 2.1.3. Ако је ω примитиван корен из јединице реда n, тада је сваки примитивни корен из јединице облика ω^a, где је $(a, n) = 1$.

Доказ. Нека је $(a, n) = 1$. Тада је $(\omega^a)^b = 1$ ако и само ако $n \mid ab$, јер је ω корен реда n. Но, како је $(a, n) = 1$, то мора $n \mid b$, па је $b = 0$ или $b \geqslant n$.
То значи да је ред елемента ω^a једнак n, па ω^a јесте примитиван корен.

За доказ другог смера леме, узмимо примитивни корен ω^a, $1 < a < n$. Означимо $(a, n) = d$ и претпоставимо да је $d > 1$. Како је $d > 1$, постоје a_1 и n_1 такви да је

$$a = da_1,\ n = dn_1 \text{ и } (a_1, n_1) = 1.$$

Тада имамо

$$(\omega^a)^{n_1} = \omega^{da_1 n_1} = \omega^{na_1} = (\omega^n)^{a_1} = 1^{a_1} = 1,$$

и $n_1 = \frac{n}{d} < n$, па је ω^a реда највише n_1 и $n_1 < n$, па ω^a није примитивни корен, супротно претпоставци. Зато је $d = 1$, то јест $(a, n) = 1$. □

Теорија којом тренутно располажемо омогућава и доказивање првих дубљих теорема.

Теорема 2.1.1. Ако су ε_1 и ε_2 примитивни корени из јединице респективно m-тог и n-тог реда, при чему су m и n узајамно прости, тада је $\varepsilon = \varepsilon_1\varepsilon_2$ примитиван корен mn-тог реда из јединице.

Доказ. Нека су ε_1 и ε_2, редом, примитивни корени из јединице, m-тог и n-тог реда. Тада је, према леми 2.1.3,

$$\varepsilon_1 = \omega_1^k,\ (k, m) = 1,$$

где је $\omega_1 = \cos\frac{2\pi}{m} + i\sin\frac{2\pi}{m}$, и

$$\varepsilon_2 = \omega_2^l,\ (l, n) = 1,$$

где је $\omega_2 = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$.
Да $\varepsilon_1\varepsilon_2$ јесте корен из јединице реда mn, следи једноставно из:

$$(\varepsilon_1\varepsilon_2)^{mn} = \varepsilon_1^{mn}\varepsilon_2^{mn} = (\varepsilon_1^m)^n(\varepsilon_2^n)^m = 1^n 1^m = 1.$$

Како је $\omega_1 = \omega^n$, а $\omega_2 = \omega^m$, за $\omega = \cos\frac{2\pi}{mn} + i\sin\frac{2\pi}{mn}$, то је

$$\varepsilon_1\varepsilon_2 = \omega_1^k\omega_2^l = (\omega^n)^k(\omega^m)^l = \omega^{nk+ml},$$

па да докажемо да је $\varepsilon_1\varepsilon_2$ примитиван корен реда mn, према леми 2.1.3 је довољно показати да је

$$(nk + ml, mn) = 1.$$

Међутим, ово једноставно следи на основу низа импликација:

$$\left.\begin{array}{l}(k,m)=1\\(n,m)=1\end{array}\right\}\Rightarrow (kn,m)=1\Rightarrow (kn+ml,m)=1$$

$$\left.\begin{array}{l}(l,n)=1\\(m,n)=1\end{array}\right\}\Rightarrow (lm,n)=1\Rightarrow (lm+kn,n)=1$$

Најзад, из

$$\left.\begin{array}{ll}(kn+ml,m)=1 & \text{и}\\(kn+ml,n)=1 & \end{array}\right\}\Rightarrow (kn+ml,mn)=1$$

што је и требало доказати. □

Дефиниција 2.1.4. Број природних бројева који нису већи од датог природног броја m и релативно су прости са њим, то јест број елемената произвољног сведеног система остатака по модулу m означава се са $\varphi(m)$. Функција φ зове се *Ојлерова функција*.

У наредном примеру израчунаћемо вредност Ојлерове φ функције за неке природне бројеве. Користићемо при том формулу

$$\varphi(n)=n\Big(1-\frac{1}{p_1}\Big)\Big(1-\frac{1}{p_2}\Big)\cdot\ldots\cdot\Big(1-\frac{1}{p_k}\Big),$$

за $n=p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_k^{\alpha_k}$, чији доказ ћемо посредно спровести кроз наредне теореме.

Пример 2.3. Израчунати $\varphi(21),\ \varphi(50),\ \varphi(342),\ \varphi(57),\ \varphi(1002),\ \varphi(1024)$.

Решење.

$\varphi(21)=\varphi(3\cdot 7)=21\cdot(1-\frac{1}{3})\cdot(1-\frac{1}{7})=3\cdot(1-\frac{1}{3})\cdot 7\cdot(1-\frac{1}{7})=2\cdot 6=12,$

$\varphi(50)=\varphi(2\cdot 5^2)=2\cdot(1-\frac{1}{2})\cdot 25\cdot(1-\frac{1}{5})=1\cdot 20=20,$

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

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

$\varphi(1002)=\varphi(2\cdot 3\cdot 167)=2\cdot(1-\frac{1}{2})\cdot 3\cdot(1-\frac{1}{3})\cdot 167\cdot(1-\frac{1}{167})=1\cdot 2\cdot 166=332,$

$\varphi(1024)=\varphi(2^{10})=2^{10}\cdot(1-\frac{1}{2})=2^9=512.$

□

Примитивни корен је знатно општији појам. Ми ћемо радити са комплексним примитивним коренима из јединице, а овде наводимо и дефиницију и пример рачунања примитивног корена по модулу природног броја.

Дефиниција 2.1.5. Ако је ред броја ω по модулу m једнак $\varphi(m)$, број ω се назива примитивним кореном по модулу m.

Размотримо и један једноставан пример са „малом“ провером, у циљу илустрације и бољег разумевања.

Пример 2.4. Одредити примитивне корене по модулу 19 и 8.

Решење. За прост број 19 имамо 18 узајамно простих бројева не већих од 19, како је $18 = 2 \cdot 3^2$ треба да одредимо елементе реда 2 и реда 3^2 у групи $1, 2, \ldots, 18$.
Како за први елемент мора важити

$$x^2 \equiv 1 \pmod{19},\ x \not\equiv 1 \pmod{19}$$

што због $x^2 - 1 = (x+1)(x-1)$ даје $x + 1 \equiv 0 \pmod{19}$, добијамо да је то број 18. Следећи број x_2 мора имати ред 9, то јест мора бити решење конгруенције

$$x^9 \equiv 1 \pmod{19}.$$

Провером добијамо да су решења једначине $1, 4, 5, 6, 7, 9, 11, 16, 17$. Свако ово решење има ред $1, 3$ или 9, па самим тим испадају бројеви $1, 7$ и 11. Множењем преосталих вредности са првим елементом 18 добијамо следећих шест примитивних корена по модулу 19, а то су $2, 3, 10, 13, 14$ и 15.

За сложен број 8 имамо 4 узајамно проста броја $1, 3, 5$ и 7. Како мора важити

$$x^2 \equiv 1 \pmod{8},\ x \not\equiv 1 \pmod{8},$$

и имамо да

$$3^2 \equiv 1 \pmod{8},$$

$$5^2 \equiv 1 \pmod{8},$$

$$7^2 \equiv 1 \pmod{8},$$

следи да $3, 5$ и 7 нису примитивни корени по модулу 8, јер је $\varphi(8) = 4$, и $2 < 4$. □

Показује се да по модулу природног броја примитиван корен постоји ако и само ако је он облика p^α, $2p^\alpha$, $\alpha \geqslant 1$, $p > 2$ или $n = 2$ и $n = 4$, а доказ истог изостављамо. Сада је јасније зашто у случају $n = 8$ нисмо имали примитиван корен. Но ово је било само информативног карактера. Настављамо рад са комплексним кореним из јединице.

Теорема 2.1.2. Ако је $(m, n) = 1$, тада се сваки корен једначине $x^{mn} = 1$ може једнозначно приказати као $\varepsilon = \varepsilon_1\varepsilon_2$, где је ε_1 корен једначине $x^m = 1$, а ε_2 корен једначине $x^n = 1$.

Доказ. Ако је ε посматрани корен једначине $x^{mn} = 1$, тада је $\varepsilon = \omega^k$ за неко $k \in \{0, 1, 2, \ldots, mn-1\}$ и $\omega = \cos\frac{2\pi}{mn} + i\sin\frac{2\pi}{mn}$.
Представимо k на јединствен начин по модулу mn као

$$k \equiv na + mb \pmod{mn},$$

где

$$a \in \{0, 1, 2, \ldots, m-1\},$$
$$b \in \{0, 1, 2, \ldots, n-1\}.$$

Ово је заиста могуће, а и представљање мора бити јединствено, јер је због $(m, n) = 1$, $k \equiv na + mb \pmod{mn}$ еквивалентно конјункцији $k \equiv na + mb \pmod{m}$ и $k \equiv na + mb \pmod{n}$ то јест $k \equiv na \pmod{m}$ и $k \equiv mb \pmod{n}$, а последње конгруенције имају решење, због $(m, n) = 1$ и оно је јединствено.

Наиме, $an \equiv k \pmod{m}$ има решење по a, јер $(m, n) = 1$ повлачи постојање $x, y \in \mathbb{Z}$ таквих да је $mx + ny = 1$, што даје $ny \equiv 1 \pmod{m}$, па $a = ky$ има жељено својство:

$$an \equiv kyn \equiv k \cdot 1 = k \pmod{m}.$$

Ако би и a_1 било решење горње конгруенције имали бисмо

$$a_1 n \equiv k \equiv an \pmod{m}$$

то јест

$$(a_1 - a)n \equiv 0 \pmod{m}$$

што због $(m, n) = 1$ даје

$$a_1 \equiv a \pmod{m}$$

што је и требало доказати.
Потпуно слично разматра се и конгруенција $bm \equiv k \pmod{n}$.
Сада, на основу горње репрезентације k по модулу mn имамо:

$$\varepsilon = \omega^k = \omega^{na+mb} = (\omega^n)^a(\omega^m)^b = \omega_1^a\omega_2^b = \varepsilon_1\varepsilon_2,$$

за $\varepsilon_1 = \omega_1^a$, $a \in \{0, 1, 2, \ldots, m-1\}$, $\varepsilon_2 = \omega_2^b$, $b \in \{0, 1, 2, \ldots, n-1\}$.

Јединственост a и b, у одговарајућим скуповима повлачи јединственост тражених ε_1 и ε_2.

Приметимо да коришћење својстава Ојлерове функције φ, чију мултипликативност посредно доказују теореме 2.1.1 и 2.1.2 и наредна теорема 2.1.3, директно даје решење конгруенције

$$an \equiv k \pmod{m}$$

као

$$a \equiv kn^{\varphi(m)-1} \pmod{m}$$

Наиме,

$$na \equiv n^{\varphi(m)}k \equiv 1 \cdot k = k \pmod{m},$$

јер је на основу Ојлерове теореме

$$n^{\varphi(m)} \equiv 1 \pmod{m},\ (m,n) = 1.$$

□

Теорема 2.1.3. Ако су m и n узајамно прости бројеви, тада је производ примитивног корена m-тог степена из јединице и примитивног корена n-тог степена из јединице примитиван корен mn-тог степена из јединице и обратно.

Доказ. Прво, $\varepsilon_1\varepsilon_2$ је примитивни корен из јединице реда mn, важи на основу теореме 2.1.1, јер је ε_1 примитивни корен из јединице реда m, а ε_2 примитивни корен из јединице реда n.

Обратно, ако је ε примитивни корен реда mn из јединице, тада према теореми 2.1.2 $\varepsilon = \varepsilon_1\varepsilon_2$, $\varepsilon_1^m = 1$, $\varepsilon_2^n = 1$. Ако ε_1 не би био примитивни корен реда m из јединице, тада би за неко $l < m$ било $\varepsilon_1^l = 1$. Тако би важило

$$\varepsilon^{nl} = (\varepsilon_1\varepsilon_2)^{nl} = (\varepsilon_1^l)^n(\varepsilon_2^n)^l = 1^n \cdot 1^l = 1$$

и $nl < mn$, што је немогуће, јер је ε примитиван корен реда mn из јединице. Слично, и ако ε_2 не би био примитиван корен реда n из јединице, за $k < n$ би било $\varepsilon_2^k = 1$ и

$$\varepsilon^{mk} = (\varepsilon_1\varepsilon_2)^{mk} = (\varepsilon_1^m)^k(\varepsilon_2^k)^m = 1^k \cdot 1^m = 1,$$

што је немогуће, јер је $mk < mn$.

□

Теорема 2.1.4. Број примитивних корена n-тог реда из јединице је паран за свако $n > 2$.

Доказ. Број примитивних корена из јединице реда n, је на основу теорема 2.1.1, 2.1.2, 2.1.3:

1° број бројева мањих од n и узајамно простих са n,

2° мултипликативна функција:

$$(m,n) = 1 \Rightarrow \varphi(mn) = \varphi(m)\varphi(n),$$

3° за степене простих се, према 1°, лако рачуна као:

$$\varphi(p^\alpha) = p^{\alpha-1}(p-1) = p^\alpha - p^{\alpha-1}.$$

Према 2° и 3°, за $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$ важи $\varphi(n) = \varphi(p_1^{\alpha_1}) \cdot \ldots \cdot \varphi(p_k^{\alpha_k})$, то јест

$$\varphi(n) = p_1^{\alpha_1 - 1}(p_1 - 1) \cdot \ldots \cdot p_k^{\alpha_k - 1}(p_k - 1).$$

За $n > 2$, број са бар једним непарним делиоцем p има за чинилац $p - 1$, који је паран, па $2 \mid \varphi(n)$. Ако је $n = 2^k$, $k > 1$ (јер је $n > 2$), тада, према 3°, $\varphi(n) = 2^{k-1}$, што је за $k > 1$ паран број. □

2.2 Мебијусова функција

Дефиниција 2.2.1. Мебијусова функција $\mu(n)$ је функција дефинисана за све природне бројеве на следећи начин:

$$\mu(n) = \begin{cases} 1, & \text{ако је } n = 1 \\ 0, & \text{ако је број } n \text{ дељив квадратом простог броја} \\ (-1)^{\nu}, & \text{иначе, где је } \nu \text{ број различитих простих делитеља броја } n. \end{cases}$$

Теорема 2.2.1. Ако су a и b узајамно прости бројеви, тада важи једнакост $\mu(ab) = \mu(a)\mu(b)$ (мултипликативност *Мебијусове функције*).

Доказ. Ако за неки прост p, $p^2 \mid ab$, тада $p^2 \mid a$ или $p^2 \mid b$, јер не може $p \mid a$, $p \mid b$, због претпоставке да су a и b узајамно прости. Тада $\mu(ab) = 0$ повлачи $\mu(a) = 0$ или $\mu(b) = 0$, зависно да ли $p^2 \mid a$ или $p^2 \mid b$, па горња једнакост важи.

Ако је $ab = p_1 p_2 \cdot \ldots \cdot p_k$, тада је $a = p_{i_1} \cdot \ldots \cdot p_{i_j}$ и $b = p_{i_{j+1}} \cdot \ldots \cdot p_{i_k}$, где је $(i_1, i_2, \ldots, i_j, i_{j+1}, \ldots, i_k)$ нека пермутација $(1, 2, \ldots, k)$ и важи $\mu(ab) = (-1)^k$, $\mu(a) = (-1)^j$, $\mu(b) = (-1)^{k-j}$ и $\mu(ab) = \mu(a)\mu(b)$ важи. За $a = 1$ тврђење важи јер је $\mu(1) = 1$. □

Теорема 2.2.2. За сваки природан број $n > 1$ важи да је

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

где је $\mu(n)$ Мебијусова функција.

Доказ. Нека је $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$, p_i-прости, $\alpha_i > 0$, $\alpha_i \in \mathbb{N}$. У збиру $\sum_{d \mid n} \mu(d)$ не-нула вредности долазе само од делилаца $d \mid n$ облика $d = p_1^{\beta_1} p_2^{\beta_2} \cdot \ldots \cdot p_k^{\beta_k}$, $0 \leqslant \beta_i \leqslant 1$, јер ако је за неко j, $\beta_j \geqslant 2$, тада $p_j^2 \mid d$ и $\mu(d) = 0$.

Из мултипликативности μ је

$$\mu(d) = \mu(p_1^{\beta_1} p_2^{\beta_2} \cdot \ldots \cdot p_k^{\beta_k}) = \mu(p_1^{\beta_1}) \cdot \ldots \cdot \mu(p_k^{\beta_k}),$$

а $\mu(1) = 1$ и $\mu(p_i) = (-1)^1 = -1$ за сваки прост p_i.
Тако је, користећи опет мултипликативност имамо

$$\sum_{d \mid n} \mu(d) = \sum_{0 \leq \beta_i \leq 1} \mu(p_1^{\beta_1}) \cdot \ldots \cdot \mu(p_k^{\beta_k})$$

а из

$$\mu(p_i^{\beta_i}) = \mu(p_i)^{\beta_i} \text{ за } p_i - \text{прост}, 0 \leq \beta_i \leq 1$$

је даље

$$\sum_{0\leq\beta_i\leq 1} \mu(p_1^{\beta_1}) \cdot \ldots \cdot \mu(p_k^{\beta_k}) = (\mu(1) + \mu(p_1)) \cdot \ldots \cdot (\mu(1) + \mu(p_k)) = 0 \cdot \ldots \cdot 0 = 0$$

□

Израчунајмо и вредност μ у неким природним бројевима.

Пример 2.5. Израчунати $\mu(1001)$, $\mu(1036)$, $\mu(10)$, $\mu(625)$, $\mu(14)$.

Решење. Број 1001 је производ три различита проста броја 7, 11 и 13, па је по дефиницији Мебијусове функције,

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

Број 1036 је дељив са $4 = 2^2$, па је

$$\mu(1036) = 0.$$

За $n = 10$ је

$$\mu(10) = \mu(2 \cdot 5) = (-1)^2 = 1.$$

Број 625 је четврти степен броја 5, па

$$\mu(625) = 0.$$

Слично случајевима 1001 и 10, и број 14 је производ различитих простих бројева 2 и 7, па је

$$\mu(14) = \mu(2 \cdot 7) = (-1)^2 = 1.$$

□

Теорема 2.2.3. Нека је функција f дефинисана на скупу $\mathbb{N}$ природних бројева и нека је

$$F(n) = \sum_{d|n} f(d) \text{ за свако } n \in \mathbb{N}.$$

Тада је

$$f(n) = \sum_{d|n} \mu(d) F\Big(\frac{n}{d}\Big),$$

(ова фурмула позната је и под називом *Мебијусова формула инверзије*).

Доказ. Срачунајмо горњи збир узимајући у обзир већ доказано $\sum_{d|n}\mu(d)=0$ за $n>1$:

$$\sum_{d|n}\mu(d)F\Big(\frac{n}{d}\Big)=\sum_{n=d_1d_2}\mu(d_1)F(d_2)\overset{(\text{деф. } F)}{=}\sum_{n=d_1d_2}\mu(d_1)(\sum_{d_3|d_2}f(d_3))=$$

$$\sum_{n=d_1d_2,\ d_3|d_2}\mu(d_1)f(d_3)\overset{(\text{замена поретка у збиру})}{=}\sum_{d_3|n}f(d_3)(\sum_{d_1|\frac{n}{d_3}}\mu(d_1))\overset{(1)}{=}$$

$$\sum_{d_3|n}f(d_3)\delta\Big(\frac{n}{d_3}\Big)\overset{(\text{ненула је само за } n=d_3)}{=}f(n),$$

што је и требало доказати.

(1)
$\sum_{d|n}\mu(d)=0,\ n>1$
$\delta(n)=0,\ n>1$
$\delta(1)=1$
$\delta(n)=\sum_{d|n}\mu(d)$ (има ове вредности према теореми 2.2.2) □

Теорема 2.2.4. Збир свих примитивних корена n-тог степена из јединице једнак је $\mu(n)$.

Доказ. Означимо збир свих примитивних n-тих корена из јединице са $f(n)$. Да докажемо да се $\mu(n)$ поклапа са $f(n)$, показаћемо да је и f мултипликативна (за μ смо то већ показали), као и да се поклапају на јединици и степенима простих. На основу ранијих разматрања је

$$f(n)=\sum_{1<k\leqslant n,\ (k,n)=1}e^{\frac{2\pi ik}{n}}.$$

Као прво, свих $\varphi(mn)$ сабирака у $f(m)f(n)$ су различити. Наиме, претпоставимо ли да су нека два једнака, то јест

$$e^{\frac{2\pi ip}{n}}\cdot e^{\frac{2\pi iq}{m}}=e^{\frac{2\pi ir}{n}}\cdot e^{\frac{2\pi is}{m}}$$

добијамо

$$pm+qn\equiv rm+sn\pmod{mn}\Leftrightarrow m(p-r)+n(q-s)\equiv 0\pmod{mn}$$

што даје

$$m\mid n(q-s),\ n\mid m(p-r),$$

односно због

$$(m,n)=1,\ m\mid q-s,\ n\mid p-r,$$

што је немогуће, јер q и s, односно p и r бирамо као различите по модулима, редом, m и n и који су, редом, са истима и узајамно прости.
Јасно, сваки од наведених сабирака се појављује у $f(mn)$, јер је

$$e^{\frac{2\pi ip}{n}} \cdot e^{\frac{2\pi iq}{m}} = e^{\frac{2\pi i(pm+qn)}{mn}}$$

и $(pm+qn, mn) = 1$ због $(p,n) = (q,m) = 1$

$$\left.\begin{array}{l}(p,n)=1,\ (m,n)=1 \Rightarrow (mp,n)=1 \Rightarrow (mp+nq,n)=1 \\ (q,m)=1,\ (n,m)=1 \Rightarrow (nq,m)=1 \Rightarrow (nq+mp,m)=1\end{array}\right\} \overset{(m,n)=1}{\Rightarrow}$$

$$(pm+qn, mn) = 1.$$

Дакле,

$$f(m)f(n) = \sum_{(p,n)=1,\ (q,m)=1,\ 1\leqslant p<n,\ 1\leqslant q<m} e^{\frac{2\pi i(pm+qn)}{mn}} =$$

$$\sum_{(k,n)=1,\ 1\leqslant k<n} e^{\frac{2\pi ik}{n}} = f(mn).$$

Али,

$$f(p^k) = \sum_{1\leqslant l<p^k,\ p\nmid l} e^{\frac{2\pi il}{p^k}} = \sum_{1\leqslant l<p^k} e^{\frac{2\pi il}{p^k}} - \sum_{l'\in\{1,2,\ldots,p^k-2\}} e^{\frac{2\pi ipl'}{p^k}} =$$

$$-1 - \Big(\sum_{1\leqslant l'\leqslant p^k-2} e^{\frac{2\pi il'}{p^{k-1}}}\Big) = (-1) - (-1) = 0.$$

$$f(p) = e^{\frac{2\pi i}{p}} + \ldots + e^{\frac{2\pi i(p-1)}{p}} + 1 - 1 = \frac{1-(e^{\frac{2\pi i}{p}})^p}{1-e^{\frac{2\pi i}{p}}} - 1 = 0 - 1 = -1$$

и

$$f(1) = \mu(1) = 1, \text{ па је } f(n) \equiv \mu(n).$$

□

За неке бројеве $n \in \mathbb{N}$, користећи горњи резултат, добијамо и нетривијалне тригонометријске идентитете.

Узимајући да је $n = 10$, у формули коју смо добили као резултат претходне теореме добијамо:

$$\cos\frac{2\cdot 1}{10}\pi + i\sin\frac{2\cdot 1}{10}\pi + \cos\frac{2\cdot 3}{10}\pi + i\sin\frac{2\cdot 3}{10}\pi + \cos\frac{2\cdot 7}{10}\pi + i\sin\frac{2\cdot 7}{10}\pi +$$

$$\cos\frac{2\cdot 9}{10}\pi + i\sin\frac{2\cdot 9}{10}\pi = \mu(10) = 1$$

Тако имамо, узимајући реални део горњег израза:

$$\cos\frac{\pi}{5} + \cos\frac{3\pi}{5} + \cos\frac{7\pi}{5} + \cos\frac{9\pi}{5} = 1,$$

па имајући у виду да је

$$\cos\frac{9\pi}{5} = \cos(2\pi - \frac{\pi}{5}) = \cos\frac{\pi}{5}$$

и слично,

$$\cos\frac{7\pi}{5} = \cos\frac{3\pi}{5}.$$

Имамо да је

$$\cos\frac{\pi}{5} + \cos\frac{3\pi}{5} = \frac{1}{2}.$$

Слично, за $n = 14$, издвајајући као и горе реални део израза добијеног директном применом теореме 2.2.4:

$$\cos\frac{2\cdot 1}{14}\pi + \cos\frac{2\cdot 3}{14}\pi + \cos\frac{2\cdot 5}{14}\pi + \cos\frac{2\cdot 9}{14}\pi + \cos\frac{2\cdot 11}{14}\pi + \cos\frac{2\cdot 13}{14}\pi = 1$$

то јест пошто су

$$\cos\frac{\pi}{7} \text{ и } \cos\frac{13\pi}{7},\ \ \cos\frac{3\pi}{7} \text{ и } \cos\frac{11\pi}{7},\ \ \cos\frac{5\pi}{7} \text{ и } \cos\frac{9\pi}{7}$$

једнаки, имамо да је

$$\cos\frac{\pi}{7} + \cos\frac{3\pi}{7} + \cos\frac{5\pi}{7} = \frac{1}{2}.$$

Занимљив идентитет добијамо и за $n = 30 = 2\cdot 3\cdot 5$:

$$\cos\frac{\pi}{15} + \cos\frac{7\pi}{15} + \cos\frac{11\pi}{15} + \cos\frac{13\pi}{15} = \frac{\mu(30)}{2} = -\frac{1}{2}.$$

Пример 2.6. Одредити вредност суме

$$S = \sum_{i,j=1}^{\varphi(n)} \varepsilon_i\varepsilon_j,$$

где су ε_i, $i = 1, 2, ..., \varphi(n)$, примитивни корени n-тог степена из јединице.

Решење. На основу теореме 2.2.4 је

$$\sum_{i,j=1}^{\varphi(n)} \varepsilon_i\varepsilon_j = (\sum_{i=1}^{\varphi(n)} \varepsilon_i)(\sum_{j=1}^{\varphi(n)} \varepsilon_j) = \mu(n)\cdot\mu(n) =$$

$$\mu^2(n) = \begin{cases} 1, & n = 1 \text{ или } n = p_1\cdot p_2\cdot \ldots \cdot p_k \\ 0, & \text{иначе} \end{cases}$$

□

Теорема 2.2.5. Нека су k и n међусобно прости природни бројеви. Означимо са P_n скуп свих примитивних корена n-тог реда из јединице, а са $P_n^k = \{\varepsilon^k \mid \varepsilon \in P_n\}$. Тада је

$$\text{(а) } P_n = P_n^k,$$

$$\text{(б) } \sum_{k=0}^{n-1} \varepsilon^{km} = 0 \text{ за свако } m \in \mathbb{Z} \ (n \nmid m) \text{ и свако } \varepsilon \in P_n \text{ (ако } n \mid m, \text{ збир је } n).$$

Доказ. а) Ако је $\theta \in P_n$, то јест θ неки од примитивних корена из јединице n-тог реда, тада је

$$\theta = e^{\frac{2\pi i l}{n}},$$

где је $(l, n) = 1$.
Но, $\theta^k = e^{\frac{2\pi i l k}{n}}$, а како је $(l, n) = 1$, и према услову теореме $(k, n) = 1$, имамо $(kl, n) = 1$, па и $\theta^k \in P_n$. Дакле, степеновањем свих елемената из P_n са k, $(k, n) = 1$ и даље добијамо елементе из P_n. Али, да покажемо и да сваки елемент из P_n јесте добијен на овај начин, довољно је доказати да за различите $l,\ m$, $(l, n) = 1$, $(m, n) = 1$, не може важити

$$(e^{\frac{2\pi i l}{n}})^k = (e^{\frac{2\pi i m}{n}})^k.$$

Ово повлачи

$$e^{\frac{2\pi i (lk - mk)}{n}} = 1,$$

то јест

$$\frac{(l-m)k}{n} = r \in \mathbb{Z}$$

односно

$$n \mid k(l-m).$$

Међутим, $(k, n) = 1$ па $n \mid (l - m)$, али ово је немогуће, по избору l и m, који су различити и узајамно прости са n, и $\leqslant n - 1$, и већи од 0.
Дакле, сви θ^k су различити и јесу примитивни корени из јединице n-тог реда.

б) Напишимо $m = rs$, где је $r = (m, n)$ и $(s, n) = 1$.
Тада је, према делу под а) за $r < n$:

$$\sum_{k=0}^{n-1} \varepsilon^{km} = \sum_{k=0}^{n-1} \varepsilon^{krs} = \sum_{k=0}^{n-1} (\varepsilon^s)^{rk} \overset{a)}{=}$$

$$\sum_{k=0}^{n-1} \theta^{rk} = 1 + \theta^r + \ldots + \theta^{r(n-1)} = \frac{1 - \theta^{rn}}{1 - \theta^r} \overset{(\theta^n = 1)}{=}$$

$$\frac{1 - (\theta^n)^r}{1 - \theta^r} = 0,$$

а) $\varepsilon^s = \theta \in P_n$
$\theta^r \neq 1$, јер $1 \leqslant (m,n) \leqslant n$.
Али, ако је $r = (m,n) = n$, онда $n \mid m$, и тада је

$$\sum_{k=0}^{n-1} \varepsilon^{km} = \sum_{k=0}^{n-1} 1 = n.$$

□

Глава 3

Основне особине циклотомичних полинома

3.1 Растављивост и примене на циклотомичне полиноме

Претходна глава даје нам и више него задовољавајућу подлогу за даље обрађивање материје. Пре самих тврђења, рекапитулирајмо основне појмове из дељивости полинома, као припрему за теорију која следи. Наиме, скраћујемо непотребно увођење познатих појмова и ставова, које ћемо брже обновити на конкретним примерима.

Навешћемо пар примера везаних за растављање полинома у $\mathbb{Z}[x]$.

Пример 3.1. Раставити полином $p(x) = x^4 + 5x^3 + 3x^2 - 19x - 30$ у $\mathbb{Z}[x]$.

Решење. Целобројне нуле потражићемо међу делиоцима броја 30, а то су:

$$\pm 1, \pm 2, \pm 3, \pm 5, \pm 6, \pm 10, \pm 15, \pm 30.$$

Једноставним рачуном добијамо:

$p(1) = -40 \neq 0,$

$p(-1) = -12 \neq 0,$

$p(2) = 0.$

Након добијања прве нуле, делимо $p(x)$ са $(x-2)$ што даје

$$(x^4 + 5x^3 + 3x^2 - 19x - 30) : (x - 2) = x^3 + 7x^2 + 17x + 15.$$

Целобројне нуле новодобијеног полинома тражимо међу бројевима $\pm 1, \pm 3, \pm 5, \pm 15$:

$p(1) = 40 \neq 0,$

$p(-1) = 4 \neq 0,$

$p(3) = 156 \neq 0,$

$p(-3) = 0.$

Одавде је

$$(x^3 + 7x^2 + 17x + 15) : (x + 3) = x^2 + 4x + 5,$$

а из представљања

$$x^2 + 4x + 5 = (x + 2)^2 + 1$$

видимо да последњи квадратни трином нема реалних корена, па се он не може даље раставити у $\mathbb{Z}[x]$.
Дакле,

$$x^4 + 5x^3 + 3x^2 - 19x - 30 = (x - 2)(x + 3)(x^2 + 4x + 5).$$

□

Горња техника некад може бити од користи и у доказивању нерастављивости полинома нижег степена.

Пример 3.2. Испитати растављивост полинома $p(x) = x^4 + 4x^3 + 4x^2 + 1$ у $\mathbb{Z}[x]$.

Решење. Будући да је слободан члан једнак 1, а водећи коефицијент полинома 1, једине могуће целобројне нуле су 1 и -1. Како је

$$p(1) = 10 \text{ и } p(-1) = 2,$$

то $p(x)$ нема фактора степена 1, а самим тим ни степена 3 при растављању у $\mathbb{Z}[x]$.
Нека је, зато,

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

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

где су a, b, c, $d \in \mathbb{Z}$.
Тада је

$$a + c = 4,$$

$$b + d + ac = 4,$$

$$ad + bc = 0, \text{ и}$$

$$bd = 1,$$

$b,\ d \in \mathbb{Z}$. Из последње једначине добијамо да је $b = d = \pm 1$. Из првог и трећег реда, за $b = d = 1$ следи

$$4 = a + c = 0$$

па овај случај не доводи до решења.
Из првог и трећег реда, за $b = d = -1$ следи

$$4 = a + c = 0$$

па опет нема решења у $\mathbb{Z}$.
Зато се дати полином не може раставити у $\mathbb{Z}[x]$. □

Наредни критеријум је нешто убојитије и типично средњошколско оруђе у задацима овог типа, за чији доказ је потребна *Гаусова Лема*.

Теорема 3.1.1. *(Гаусова Лема)* Претпоставимо да $f(x) \in \mathbb{Z}[x]$ има узајамно просте коефицијенте, тако да

$$f(x) = c_n x^n + \ldots + c_1 x + c_0.$$

Претпоставимо да се $f(x)$ може свести на $\mathbb{Q}[x]$, тако да је

$$f(x) = A(x)B(x)$$

где $A(x),\ B(x) \in \mathbb{Q}[x]$ имају позитивне степене. Тада је $f(x)$ растављив у $\mathbb{Z}[x]$, заправо

$$f(x) = a(x)b(x)$$

где је $a(x) = \mu A(x)$, $b(x) = \mu^{-1}B(x)$, $\mu \in \mathbb{Q}$ и $a(x),\ b(x) \in \mathbb{Z}[x]$.

Доказ. Нека је m заједнички садржалац имениоца коефицијената $A(x)$, тако да је $m_1 A(x) \in \mathbb{Z}[x]$. Нека је l највећи заједнички делилац коефицијената $m_1 A(x)$, тако да је $m_1 A(x) = l_1 a(x)$, где су коефицијенти $a(x)$ релативно прости.

Слично налазимо целе бројеве различите од нуле $m_2,\ l_2$ тако да је $m_2 B(x) = l_2 b(x)$, где су коефицијенти $b(x)$ релативно прости.
Нека је $\mu = m_1/l_1$ и $\nu = m_2/l_2$. Тада је

$$f(x) = \mu\nu a(x)b(x)$$

где су $a(x)b(x) \in \mathbb{Z}[x]$ дати као

$$a(x) = a_r x^r + \ldots + a_1 x + a_0,\ b(x) = b_s x^s + \ldots + b_1 x + b_0,$$

за $(a_0,\ a_1, \ldots,\ a_r) = (b_0,\ b_1, \ldots,\ b_s) = 1$ и $n = r + s$.
Заменимо $b(x)$ и ν са $-b(x)$ и $-\nu$ ако је потребно, па можемо претпоставити да је $\mu\nu > 0$. Тада морамо показати да је $\mu\nu = 1$.
Напишимо да је $\mu\nu = l/m$, где су $m,\ l \in \mathbb{Z}$, $m,\ l > 0$, и $(m,\ l) = 1$. Тада је

$$mf(x) = la(x)b(x).$$

Сада $l \mid mc_k$ за $k = 0,\ 1, \ldots,\ n$ и $(m, l) = 1$, па $l \mid c_k$ за $k = 0,\ 1, \ldots,\ n$. Како су $c_0,\ c_1, \ldots,\ c_n$ узајамно прости имамо да је $l = 1$.

Претпоставимо да је $m > 1$. Изаберимо прост p који дели m. Како је $(a_0,\ a_1, \ldots,\ a_r) = 1$, p не може делити све коефицијенте у $a(x)$. Стога мора постојати цео број i, где је $0 \leqslant i < r$, тако да p дели сваки $a_0,\ a_1, \ldots,\ a_{i-1}$ и p не дели a_i. Слично, мора постојати цео број j, где је $0 \leqslant j < s$ тако да p дели сваки од $b_0,\ b_1, \ldots,\ b_{j-1}$ и p не дели b_j. Али

$$mc_{i+j} = \cdots + a_{i-1}b_{j+1} + a_ib_j + a_{i+1}b_{j-1} + \cdots .$$

Сада p дели чланове са леве стране a_ib_j (то јест $p \mid a_0,\ p \mid a_1, \ldots, p \mid a_{i-1}$), p дели чланове са десне стране a_ib_j (то јест $p \mid b_0,\ p \mid b_1, \ldots, p \mid b_{j-1}$), и p дели mc_{i+j} (то јест $p \mid m$). Према томе $p \mid a_ib_j$ је контрадикција са чињеницом да $p \nmid a_i$ и $p \nmid b_j$. □

Теорема која следи даје најпознатији и најављени критеријум растављивости.

Теорема 3.1.2. *(Ајзенштајнов критеријум)* Претпоставимо да је $f(x) \in \mathbb{Z}[x]$ дато као

$$f(x) = c_nx^n + \ldots + c_1x + c_0$$

и нека је p прост, који задовољава следеће

(1) p не дели c_n,

(2) p дели $c_{n-1}, \ldots,\ c_1,\ c_0$,

(3) p^2 не дели c_0.

Тада је $f(x)$ нерастављив у $\mathbb{Q}[x]$.

Доказ. Претпоставимо да коефицијенти $c_0\ , c_1, \ldots,\ c_n$ немају заједничких простих чинилаца. Тада на основу Гаусове Леме и претпоставке да је $f(x)$ растављив у $\mathbb{Q}[x]$ имамо да је

$$f(x) = a(x)b(x)$$

где су $a(x),\ b(x) \in \mathbb{Z}[x]$ и оба имају позитивне степене. Записаћемо да је

$$a(x) = a_rx^r + \ldots + a_1x + a_0,\ b(x) = b_sx^s + \ldots + b_1x + b_0.$$

На основу (2) $p \mid c_0$, $c_0 = a_0b_0$, као и $p \mid a_0$ или $p \mid b_0$. Док из (3) имамо да $p^2 \nmid c_0$. Сада

$$c_k = a_0b_k + a_1b_{k-1} + \ldots + a_kb_0$$

и $p \mid a_k$ за $k = 0\ , 1, \ldots,\ r$ (у овом кораку смо користили да је $r < n$). Како p дели све коефицијенте $a(x)$ добијамо да p дели и све коефицијенте од $f(x)$ што је контрадикција са (1). □

Моћ горњег критеријума проверићемо и кроз пар примера.

Пример 3.3. Доказати да су полиноми $x^7+48x-24$, $x^p+px+(p-1)$, $p\geq 3$, $p-$ прост, x^5+4x^4+2x+2 нерастављиви у $\mathbb{Z}[x]$.

Решење. За полином
$$f(x)=x^7+48x-24$$
узмимо $p=3$, тада $3\mid -24$, $3\mid 48$, али $3^2\nmid -24$, па је овај полином нерастављив у $\mathbb{Z}[x]$.
За полином
$$f(x)=x^5+4x^4+2x+2$$
узмимо $p=2$, тада $2\mid 2$, $2\mid 2$, $2\mid 4$, али $2^2\nmid a_0=2$, па је овај полином нерастављив у $\mathbb{Z}[x]$.
За полином
$$f(x)=x^p+px+(p-1)$$
узмимо $p\geqslant 3$, p-прост.
Имамо да је

$$f(x+1)=(x+1)^p+p\cdot(x+1)+p-1=\sum_{k=1}^{p}x^k+1+px+p+p-1=$$

$$\sum_{k=1}^{p}\binom{p}{k}x^k+px+2p=x^p+\sum_{k=2}^{p-1}\binom{p}{k}x^k+2px+2p.$$

Како је

$$\binom{p}{k}=\frac{p!}{k!\cdot(p-k)!}=\frac{1\cdot 2\cdot\ldots\cdot p}{1\cdot 2\cdot\ldots\cdot k\cdot(p-k)\cdot(p-k-1)\cdot\ldots\cdot 1}$$

дељив са p, јер бројилац има чинилац p, а у имениоцу су бројеви мањи од p, па их p не дели, то $p\mid\binom{p}{k}$. Зато је $p\mid 2p$, $p\mid p$, $p\mid\binom{p}{k}$, $2\leqslant k\leqslant p-1$, али $p^2\nmid 2p$ за $p\geqslant 3$. Примена Ајзенштајновог критеријума омогућава закључак да је $f(x)$ нерастављив. □

Коначно, у прилици смо и да видимо корист од овог критеријума у циклотомичном „окружењу“.

Теорема 3.1.3. Нека је p прост број и $\varepsilon=\cos\frac{2\pi}{p}+i\sin\frac{2\pi}{p}$. Ако су $a_0,a_1,\ldots,a_{p-1}$ цели бројеви различити од нуле, тада ће једнакост

$$a_0+a_1\varepsilon+\ldots+a_{p-1}\varepsilon^{p-1}=0$$

важити онда и само онда ако је $a_0=a_1=\ldots=a_{p-1}$.

Доказ. Ако је

$$a_0 + a_1\varepsilon + \ldots + a_{p-1}\varepsilon^{p-1} = 0,$$

из

$$\frac{\varepsilon^p - 1}{\varepsilon - 1} = 1 + \varepsilon + \ldots + \varepsilon^{p-1} = 0$$

следи

$$a_0 + a_1\varepsilon + \ldots + a_{p-1}\varepsilon^{p-1} - a_0(1 + \varepsilon + \ldots + \varepsilon^{p-1}) = 0$$

то јест

$$(a_1 - a_0)\varepsilon + \ldots + (a_{p-1} - a_0)\varepsilon^{p-1} = 0 \Leftrightarrow (a_1 - a_0)\cdot 1 + \ldots + (a_{p-1} - a_0)\varepsilon^{p-2} = 0$$

односно ε анулира полином степена $p-2$, што је немогуће, па је

$$a_1 - a_0 = \ldots = a_{p-1} - a_0 = 0$$

то јест

$$a_0 = a_1 = \ldots = a_{p-1}.$$

Ако би ε било нула полинома степена $\leqslant p-2$, тада би тај полином делио

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

Но, $F(x)$ је нерастављив по Ајзенштајновом критеријуму, јер

$$F(x+1) = \frac{(x+1)^p - 1}{x} = \frac{\sum_{k=1}^{p}\binom{p}{k}x^k}{x} = \sum_{k=1}^{p}\binom{p}{k}x^{k-1} =$$

$$p + \binom{p}{2}x^1 + \ldots + \binom{p}{p}x^{p-1}$$

и $p \mid p,\ p \mid \binom{p}{2},\ \ldots,\ p \mid \binom{p}{p-1}$, али $p^2 \nmid p$. Како је

$$\binom{p}{k} = \frac{p(p-1)\cdot\ldots\cdot(p-k+1)}{1\cdot 2\cdot\ldots\cdot k}.$$

дељив са p, јер бројилац има чинилац p, а у имениоцу су бројеви мањи од p, па их p не дели, то $p \mid \binom{p}{k}$. □

Пример 3.4. Ако су m и n узајамно прости, доказати да полиноми $x^m - 1$ и $x^n - 1$ имају јединствен заједнички корен.

Решење. Скуп решења $x^n - 1$ је скуп корена из јединице n-тог реда, који јесте једна циклична група, па је пресек решења $x^m - 1 = 0$ и $x^n - 1 = 0$ подгрупа обе цикличне групе m-тог и n-тог реда, те њен ред r дели, према Лагранжовој теореми, редове обе групе, то јест $r \mid m$, $r \mid n$. Како је

$$r \mid m,\ r \mid n \Leftrightarrow r \mid (m,n) = 1$$

то је $r = 1$, па је тражени корен јединствен. □

Појам од централне важности, сада можемо и коректно дефинисати.

Дефиниција 3.1.1. Нека је n произвољан природан број. Тада n-тим циклотомичним полиномом називамо моничан полином чији су корени примитивни n-ти корени из јединице (и при томе нема двоструких нула):

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

Теорема 3.1.4. Нека је $\Phi_n(x)$ циклотомични полином, тада важи једнакост

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

Доказ. Све нуле полинома $x^n - 1$ су корени n-тог реда из јединице. Нека је θ један од тих корена, и нека је $r(\theta) = d$. Тада је θ примитивни корен d-тог реда из јединице, па је самим тим и нула полинома $\Phi_d(x)$, а такође, пошто $d \mid n$, то је θ нула и полинома $\prod_{d|n} \Phi_d(x)$, па пошто су полиноми $x^n - 1$ и $\prod_{d|n} \Phi_d(x)$ монични, и имају све једнаке нуле, то су и они сами једнаки, па је једнакост задовољена. Упоређивањем степена најстаријих чланова добијамо да је $n = \sum_{d|n} \varphi(d)$. □

Наведимо и првих двадесет циклотомичних полинома:

$$\Phi_1(x) = x - 1,$$

$$\Phi_2(x) = x + 1,$$

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

$$\Phi_4(x) = x^2 + 1,$$

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

$$\Phi_6(x) = x^2 - x + 1,$$

$$\Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1,$$

$$\Phi_8(x) = x^4 + 1,$$

$$\Phi_9(x) = x^6 + x^3 + 1,$$

$$\Phi_{10}(x) = x^4 - x^3 + x^2 - x + 1,$$

$$\Phi_{11}(x) = x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1,$$

$$\Phi_{12}(x) = x^4 - x^2 + 1,$$

$$\Phi_{13}(x) = x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1,$$

$$\Phi_{14}(x) = x^6 - x^5 + x^4 - x^3 + x^2 - x + 1,$$

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

$$\Phi_{16}(x) = x^8 + 1,$$

$$\Phi_{17}(x) = x^{16} + x^{15} + x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1,$$

$$\Phi_{18}(x) = x^6 - x^3 + 1,$$

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

$$\Phi_{20}(x) = x^8 - x^6 + x^4 - x^2 + 1.$$

Применом горе наведеног критеријума доказаћемо нерастављивост полинома $\Phi_n(x)$ за просто n.

Теорема 3.1.5. Ако је p прост број, онда је

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

Доказ. Према теореми 3.1.4 је

$$x^p - 1 = \prod_{d|p} \Phi_d(x) = \Phi_1(x)\Phi_p(x),$$

јер је p прост.
Али, $\Phi_1(x) = x - 1$, па је

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

□

Случај општег $n \in \mathbb{N}$ третира се нешто сложенијом техником и излази из оквира теме овог рада. Зато ћемо доказ истог овде изоставити.

Теорема 3.1.6. Полином $\Phi_n(x)$, $n > 2$, је нерастављив у пољу рационалних бројева.

Интуитивно очекивана, и горњим резултатима „потврђена“ важи и следећа теорема.

Теорема 3.1.7. Коефицијенти полинома $\Phi_n(x)$ су цели бројеви.

Доказ. За доказ ове теореме неопходно је најпре доказати следећу теорему:

Теорема Нека су f и g два монична полинома са рационалним коефицијентима. Ако су сви коефицијенти полинома $f \cdot g$ цели бројеви, онда су то и сви коефицијенти полинома f и g.

Доказ. Нека су $f(x) = x^m + a_{m-1}x^{m-1} + \ldots + a_0$ и $g(x) = x^n + b_{n-1}x^{n-1} + \ldots + b_0$ дати полиноми. Нека су M и N најмањи природни бројеви такви да су $Mf(x)$ и $Ng(x)$ полиноми са целобројним коефицијентима (очигледно је да такви M и N постоје, то су најмањи заједнички садржаоци од имениоца бројева $a_m, a_{m-1}, \ldots, a_0$, то јест $b_n, b_{n-1}, \ldots, b_0$, у скраћеном облику). Нека је даље $A_i = Ma_i$, за $0 \leqslant i \leqslant m-1$, и $B_j = Mb_j$, за $0 \leqslant j \leqslant n-1$, и нека је $A_m = M$, то јест $B_n = N$. Тада је

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

Како је по претпоставци $f(x)g(x) \in \mathbb{Z}[x]$, то су сви коефицијенти полинома $MNf(x)g(x)$ дељиви са MN.
Претпоставимо да је $MN > 1$ (у супротном би било $M = 1$, $N = 1$, чиме би тврђење било доказано). Нека је p прост број такав да $p \mid MN$. Покажимо да тада постоји $i \in 0, 1, \ldots, m$ такав да $p \nmid A_i$. Заиста, ако $p \nmid M$, тада и $p \nmid A_m$. У супротном, ако $p \mid M$, опет не може да важи $p \mid A_i$, за све $i \in 0, 1, \ldots, m$ јер би тада важило да је $\left(\frac{M}{p}\right)a_i = \frac{A_i}{p} \in \mathbb{Z}$, па бисмо имали контрадикцију са минималности броја M. Аналогним поступком показује се и да постоји $j \in 0, 1, \ldots, n$, такво да $p \nmid B_j$. Нека су I, J највећи од свих бројева i, j, за које је задовољено $p \nmid A_i$, $p \nmid B_j$. Тада је коефицијент уз члан x^{I+J}, у полиному $MNf(x)g(x)$, број облика $A_I B_J + S$, и притом ћемо показати да $p \mid S$. Заиста, како је

$$S = \sum_{k+l=I+J,\ k\neq I,\ l\neq J} A_k B_l$$

то мора за сваки сабирак у тој суми да важи или $k > I$, или $l > J$, па тада важи $p \mid A_k$, то јест $p \mid B_l$, односно сваки сабирак је дељив са p, па $p \mid S$. Дакле, добили смо да коефицијнет уз x^{I+J} није дељив са MN. Из те контрадикције следи да не може важити $MN > 1$, из чега следи тврђење. □

Докажимо тврђење индукцијом.

За $n = 1$ је очигледно тачно, јер је $\Phi_1(x) = x - 1$.
Претпоставимо да је тврђење тачно за све бројеве мање од n. Тада је применом теореме 3.1.4

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

па су коефицијенти полинома $\Phi_n(x)$ рационални бројеви, а према претходно доказаној теореми, самим тим и цели.

□

Глава 4

Даља својства циклотомичних полинома

4.1 Корисни идентитети и сложенији примери

Развијена теорија омогућава одређивање циклотомичних полинома вишег степена помоћу одговарајућих полинома нижег степена, по правилима које утврђујемо наредним теоремама. Прва таква сводиће $n = p^\alpha$ на случај самог простог броја p.

Теорема 4.1.1. Ако је $n = p^\lambda$ степен простог броја p, онда је

$$\Phi_n(x) = \Phi_p(x^{p^{\lambda-1}}).$$

Доказ. За $\lambda = 1$, очигледно важи. За $\lambda > 1$ је, на основу теореме 3.1.4

$$\Phi_{p^{\lambda+1}}(x) = \frac{x^{p^{\lambda+1}} - 1}{\prod_{d|p^\lambda} \Phi_d(x)} = \frac{x^{p^{\lambda+1}} - 1}{x^{p^\lambda} - 1},$$

према $((x^{p^\lambda} - 1) = \prod_{d|p^\lambda} \Phi_d(x))$, па је ово

$$= \frac{(x^{p^\lambda})^p - 1}{x^{p^\lambda} - 1} = 1 + x^{p^\lambda} + \ldots + (x^{p^\lambda})^{p-1} = \Phi_p(x^{p^\lambda}),$$

према теореми 3.1.5. □

Видимо и како то функционише за конкретне степене простих.

Пример 4.1. Израчунати $\Phi_{16}(x)$, $\Phi_{625}(x)$, $\Phi_{27}(x)$, $\Phi_{49}(x)$, $\Phi_{1331}(x)$.

Решење. Користећи закључак претходне теореме добијамо:

$$\Phi_{16}(x) = \Phi_2(x^8) = x^8 + 1,$$

$$\Phi_{625}(x) = \Phi_5(x^{125}) = x^{500} + x^{375} + x^{250} + x^{125} + 1,$$

$$\Phi_{27}(x) = \Phi_3(x^9) = x^{18} + x^9 + 1,$$

$$\Phi_{49}(x) = \Phi_7(x^7) = x^{42} + x^{35} + x^{21} + x^{14} + x^7 + 1,$$

$$\Phi_{1331}(x) = \Phi_{11}(x^{121}) = x^{1210} + x^{1089} + x^{968} + x^{847} + x^{726} + x^{605} + x^{484} + x^{363} + x^{242} + x^{121} + 1.$$

□

Занимљива веза постоји и између Φ_n и Φ_{2n}. Управо она је у садржају наредне теореме.

Теорема 4.1.2. За сваки непаран број n већи од 1 једнакост $\Phi_{2n}(x) = \Phi_n(-x)$ је задовољена.

Доказ. Према теореми 3.1.4 је:

$$x^{2n} - 1 = \prod_{d|2n} \Phi_d(x) = \prod_{d|n} \Phi_d(x) \prod_{d|n} \Phi_{2d}(x) \overset{\text{теорема 3.1.4}}{=}$$

$$(x^n - 1) \prod_{d|n} \Phi_{2d}(x) = (x^n - 1)(x + 1) \prod_{d|n,\ d>1} \Phi_{2d}(x),$$

па је

$$\prod_{d|n,\ d>1} \Phi_{2d}(x) = \frac{x^{2n} - 1}{(x^n - 1)(x + 1)} = \frac{x^n + 1}{x + 1} = x^{n-1} - x^{n-2} + \ldots + 1 \ (*)$$

Тврђење доказујемо потпуном индукцијом.

За $\Phi_6(x)$ имамо, према теореми 3.1.4,

$$x^6 - 1 = \Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_6(x) = (x - 1)(x + 1)(x^2 - x + 1)\Phi_6(x) =$$

$$(x - 1)(x^3 + 1)\Phi_6(x)$$

$$\Rightarrow \Phi_6(x) = \frac{x^6 - 1}{(x - 1)(x^3 + 1)} = \frac{x^3 - 1}{x - 1} = x^2 + x + 1 = \Phi_3(-x).$$

Претпоставимо да тврђење важи за непарне бројеве између 1 и датог броја n; тада $(*)$ даје

$$\prod_{d|n,\ d>1} \Phi_{2d}(x) = \frac{x^n + 1}{x + 1}$$

то јест

$$\Phi_{2n}(x) \cdot \prod_{d|n,\ 1<d<n} \Phi_d(-x) = \frac{x^n + 1}{x + 1} = \frac{-(-x)^n + 1}{-(-x) + 1} = \frac{(-x)^n - 1}{(-x) - 1}$$

док из

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

имамо

$$(-x)^n - 1 = \prod_{d|n} \Phi_d(-x) = \Phi_1(-x)\Phi_n(-x) \prod_{d|n} \Phi_d(-x) =$$

$$((-x) - 1)\Phi_n(-x) \prod_{d|n,\ 1<d<n} \Phi_d(-x)$$

одакле је

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

што коначно даје

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

□

Функционисање горњег правила видећемо у примеру који следи.

Пример 4.2. Израчунати $\Phi_{10}(x)$, $\Phi_{14}(x)$, $\Phi_6(x)$, $\Phi_{18}(x)$.

Решење. Користећи теорему 4.1.2, претходне резултате добијамо:

$$\Phi_{10}(x) = \Phi_5(-x) = x^4 - x^3 + x^2 - x + 1,$$

$$\Phi_{14}(x) = \Phi_7(-x) = x^6 - x^5 + x^4 - x^3 + x^2 - x + 1,$$

$$\Phi_6(x) = \Phi_3(-x) = x^2 - x + 1.$$

Применом теорема 4.1.1 и 4.1.2 добијамо и

$$\Phi_{18}(x) = \Phi_9(-x) = \Phi_3(-x^3) = x^6 - x^3 + 1.$$

□

Сетимо се Мебијусове формуле инверзије. Њен аналогон међу циклотомичним полиномима је наредна теорема.

Теорема 4.1.3. За природан број n важи

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

Доказ. Уочимо сличност ове теореме са теоремама 2.2.3 и 3.1.4, заправо је ово инверзија формуле у теореми 3.1.4 само мултипликативног облика за разлику од оног у теореми 2.2.3. Срачунајмо десну страну то јест производ

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

$$\prod_{d|n,\ n=dk}\Big(\prod_{s|\frac{d}{l},\ d=ls}\Phi_l(x)\Big)^{\mu(k)}=$$

$$\prod_{l|n}(\Phi_l(x))^{\sum_{k|\frac{n}{l}}\mu(k)}=\prod_{l|n}\Phi_l(x)^{\delta(\frac{n}{l})}=\Phi_n(x)$$

јер је $\delta(n)=\sum_{d|n}\mu(d)=0$, за $n>0$ и $\delta(1)=1$. □

Наведено, коначно, омогућава и сукцесивно спуштање степена код одређивања циклотомичних полинома, те у теореми дајемо поступак којим се ово и спроводи за ма које n.

Теорема 4.1.4. Ако је $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdot\ldots\cdot p_k^{\alpha_k}$, где су $p_1,p_2,\ldots,p_k$ различити прости бројеви, тада је $\Phi_n(x)=\Phi_{n'}(x^{n''})$, где је $n'=p_1p_2\cdot\ldots\cdot p_k$, а $n''=n/n'$.

Доказ. Делиоци од n' су бројеви $d=\prod_{j=1}^k p_j^{\varepsilon_j}$, $\varepsilon_j\in\{0,1\}$. Означимо скуп ових делитеља са D. Тада је, према теореми 4.1.3

$$\Phi_{n'}(x)=\prod_{d\in D}(x^d-1)^{\mu(\frac{n'}{d})}.$$

Делиоци s од n за које је $\mu(\frac{n}{s})\neq 0$ су бројеви $s=\prod_{j=1}^k p_j^{\beta_j}$ где је $\beta_j\geqslant\alpha_j-1$ за свако j, а то су тачно бројеви $n''d$, $d\in D$, и $\frac{n}{n''d}=\frac{n'}{d}$.
Отуда

$$\Phi_n(x)=\prod_{d\in D}(x^{n''d}-1)^{\mu(\frac{n'}{d})}=\Phi_{n'}(x^{n''}).$$

□

Алат којим се служимо, омогућава увиђање следеће везе $\Phi_n(x)$ и $\Phi_{pn}(x)$, $n\in\mathbb{N}$, p-прост.

Теорема 4.1.5. Ако је p прост број, тада је

$$\Phi_{pn}(x)=\begin{cases}\Phi_n(x^p), & \text{ако је } (n,p)=p,\\ \Phi_n(x^p)/\Phi_n(x), & \text{ако је } (n,p)=1.\end{cases}$$

Доказ. Размотримо прво случај када $p \mid n$.
Примена (теорема 4.1.3) даје:

$$\Phi_{pn}(x) = \prod_{d|pn}(x^{\frac{pn}{d}} - 1)^{\mu(d)} = \Big(\prod_{d|n}(x^{\frac{pn}{d}} - 1)^{\mu(d)}\Big)\Big(\prod_{d|pn,\ d\nmid n}(x^{\frac{pn}{d}} - 1)^{\mu(d)}\Big) =$$

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

У последњој загради важи $d \mid pn$, и $d \nmid n$, па одатле следи $p \mid d$, али пошто $p \mid n$ то важи и $p^2 \mid d$. Заиста, ако би било $d = pd_0$, где $p \nmid d_0$, тада би из $d \mid pn$ следило $d_0 \mid n$, то јест због $(d_0, p) = 1$ је $d_0 \mid \frac{n}{p}$, одакле следи $d_0 p \mid n$ то јест $d \mid n$, што је немогуће. Дакле, $p^2 \mid d$, и самим тим по дефиницији Мебијусове функције је $\mu(d) = 0$, па је

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

одакле је $\Phi_{pn}(x) = \Phi_n(x^p)$, што се тврдило.

Други случај теореме се може показати аналогно првом:

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

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

□

Као илустрацију примене доказаних тврђења, урадићемо следећа три занимљива примера.

Пример 4.3. Израчунати $\Phi_{15}(x)$.

Решење.

$$\Phi_{15}(x) = \frac{\Phi_3(x^5)}{\Phi_3(x)} = \frac{x^{10} + x^5 + 1}{x^2 + x + 1} = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1.$$

□

Пример 4.4. Израчунати $\Phi_n(1)$.

Решење. Примена (теорема 4.1.4) даје

$$\Phi_n(1) = \Phi_{n'}(1) = \Phi_{p_1 p_2 \cdot \ldots \cdot p_k}(1),\ n > 1.$$

Међутим, (теорема 3.1.4) важи

$$\prod_{d|n,\ d>1} \Phi_d(x) = \frac{x^n - 1}{x - 1} = 1 + x + \ldots + x^{n-1},$$

па у случају $n' = p_1 p_2 \cdot \ldots \cdot p_k$ имамо

$$\prod_{d|n',\ d>1} \Phi_d(x) = 1 + x + \ldots + x^{p_1 p_2 \cdot \ldots \cdot p_k - 1},$$

што даје

$$\prod_{d|n'=p_1 p_2 \cdot \ldots \cdot p_k,\ d>n} \Phi_d(1) = p_1 p_2 \cdot \ldots \cdot p_k.$$

Но, (теорема 3.1.5)

$$\Phi_{p_i}(1) = 1 + 1^1 + 1^2 + \ldots + 1^{p_i - 1} = p_i,$$

па је

$$\prod_{\varnothing \subsetneq \{i_1,\ldots,i_l\} \subseteq \{1,2,\ldots,k\}} \Phi_{p_{i_1} \cdot \ldots \cdot p_{i_l}}(1) = p_1 p_2 \cdot \ldots \cdot p_k$$

и

$$\prod_{i=1}^{k} \Phi_{p_i}(1) = \prod_{i=1}^{k} p_i = p_1 p_2 \cdot \ldots \cdot p_k$$

па је, због теореме 3.1.7,

$$\Phi_{p_{i_1} \cdot \ldots \cdot p_{i_l}}(1) = \pm 1$$

за свако $l > 1$.
Али, према теореми 4.1.5 за $(p_{i_1}, p_{i_2} \cdot \ldots \cdot p_{i_l}) = 1$, $x = 1$

$$\Phi_{p_{i_1} p_{i_2} \cdot \ldots \cdot p_{i_l}}(1) = \frac{\Phi_{p_{i_2} \cdot \ldots \cdot p_{i_l}}(1)}{\Phi_{p_{i_2} \cdot \ldots \cdot p_{i_l}}(1)} = 1.$$

Дакле, ако је $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$, тада је

$$\Phi_n(1) = \begin{cases} 1, & \text{за } k \geq 2 \\ p, & n = p^\alpha \\ 0, & n = 1. \end{cases}$$

□

Пример 4.5. Израчунати $\Phi_n(-1)$.

Решење. Коришћење теореме 4.1.2 даје

$$\Phi_n(-1) = \Phi_{2n}(1),$$

па даљи рачун $\Phi_n(-1)$ настављамо коришћењем резултата добијених у примеру 4.4.
За $n = 1$ се тривијално добија

$$\Phi_1(-1) = (-1) - 1 = -2.$$

За $n > 1$ разликујемо случајеве:

1° $n = 2^\alpha$, $\alpha > 0$

2° $n = 2^\alpha p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$, $\alpha_1, \alpha_2, \ldots, \alpha_k > 0$, $\alpha \geqslant 0$.

У првом случају је

$$\Phi_n(-1) = \Phi_{2^{\alpha+1}}(1) = 2,$$

док у другом случају имамо

$$\Phi_n(-1) = \Phi_{2n}(1) = 1,$$

јер $2n$ има више од једног простог делиоца, према примеру 4.4.
Дакле,

$$\Phi_n(-1) = \begin{cases} -2, & \text{за } n = 1 \\ 2, & \text{за } n = 2^\alpha \\ 1, & \text{за } n = 2^\alpha p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k},\ \alpha \geqslant 0,\ \alpha_1, \ldots, \alpha_k > 0. \end{cases}$$

□

Техника рачуна са коренима из јединице може бити корисна и у неким задацима енумеративне комбинаторике. Такав је и наредни пример.

Пример 4.6. За коначан скуп A означимо са $|A|$ кардиналан број скупа A, а са $s(A)$ суму његових елемената. Нека је p прост број а $A = \{1, 2, \ldots, 2p\}$. Одредити број свих подскупова $B \subset A$ таквих да је $|B| = p$ и да $p \mid s(B)$.

Решење. Случај $p = 2$ разматра се једноставно јер су једине могућности одабира два броја из скупа $\{1, 2, 3, 4\}$ са збиром дељивим са 2 подскупови $\{1, 3\}$ и $\{2, 4\}$. Дакле, у овом случају имамо две могућности.
За $p > 2$ означимо $\varepsilon = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p}$. Нека x_j представља број подскупова X од A који имају p елемената и $s(X) \equiv j \pmod p$. Тада важи релација

$$\sum_{j=0}^{p-1} x_j \varepsilon^j = \sum_{X \subset A,\ |X|=p} \varepsilon^{s(X)} =$$

$$\sum_{1 \leqslant c_1 < c_2 < \ldots < c_p \leqslant 2p} \varepsilon^{c_1 + c_2 + \ldots + c_p} = \sum_{1 \leqslant c_1 < c_2 < \ldots < c_p \leqslant 2p} \varepsilon^{c_1} \cdot \varepsilon^{c_2} \cdot \ldots \cdot \varepsilon^{c_p}.$$

Последњи збир је међутим једнак коефицијенту уз x^p у полиному

$$(x + \varepsilon) \cdot (x + \varepsilon^2) \cdot \ldots \cdot (x + \varepsilon^{2p}).$$

Наиме, развијајући назначени полином добијамо сабирке у којима се појављују као чиниоци x или неки од ε^j, $j = 1, 2, \ldots, 2p$. Тако ће уз x^p бити збир свих могућих производа чинилаца облика ε^j, $j = 1, 2, \ldots, 2p$, што је кључна примедба која ће нас одвести до решења.
Но, како је

$$x^p - 1 = (x-1)(x-\varepsilon)\cdot\ldots\cdot(x-\varepsilon^{p-1}),$$

једноставно налазимо да је

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

$$(-1)^{2p}(-x-\varepsilon)\cdot\ldots\cdot(-x-1)\cdot(-x-\varepsilon)\cdot\ldots\cdot(-x-1) =$$

$$((-x-1)\cdot(-x-\varepsilon)\cdot\ldots\cdot(-x-\varepsilon^{p-1}))^2 = ((-x^p)-1)^2 =$$

$$(-x^p-1)^2 = (x^p+1)^2 = x^{2p} + 2x^p + 1,$$

што даје

$$\sum_{j=0}^{p-1} x_j\varepsilon^j = 2$$

то јест

$$x_0 - 2 + x_1\varepsilon + x_2\varepsilon^2 + \ldots + x_{p-1}\varepsilon^{p-1} = 0$$

па је на основу теореме 3.1.3

$$x_0 - 2 = x_1 = \ldots = x_{p-1}.$$

Са друге стране, укупан број подскупова са p елемената скупа A је $\binom{2p}{p}$, те коначно добијамо

$$x_0 = \frac{\binom{2p}{p} - 2}{p} + 2,$$

што је тражени број.
Свих осталих подскупова са p елемената чији збир елемената при дељењу са p даје остатак j, $j \in \{1, 2, \ldots, p-1\}$ има

$$x_0 = \frac{\binom{2p}{p} - 2}{p}.$$

□

Литература

[1] Andreescu T., Dospinescu G., *Problems from the Book*

[2] Каделбург З., Мићић В., *Увод у теорију бројева*, Београд 1989.

[3] Калајџић Г., *Алгебра*, Београд 1998.

[4] Yves Gallot, *Cyclotomic Polynomials and Prime Numbers*

[5] Yimin Ge, *Elementary Properties of Cyclotomic Polynomials*

[6] *http* : *//srb.imomath.com/dodatne/ciklotomicni_brkovic.pdf*

[7] *https* : *//www2.bc.edu/reederma/cyclosummary.pdf*