Eötvös Loránd Tudományegyetem
Természettudományi Kar

KÖROSZTÁSI POLINOMOK

Szakdolgozat

Készítette: **Papp Ármin Péter**
Matematikai elemző szakirány

Témavezető: **Ágoston István**
egyetemi docens
Algebra és Számelmélet Tanszék

Budapest, 2019

Tartalomjegyzék

Köszönetnyilvánítás

Ezúton szeretném megköszönni témavezetőmnek, Ágoston Istvánnak a kitartó és hosszadalmas munkáját. Hasznos javaslatai, ötletei nagy mértékben hozzájárultak a szakdolgozat elkészüléséhez.

Külön köszönet Seres Ákos és Hojsza Kristóf szaktársaimnak, akik az évek során nagy segítséget nyújtottak a vizsgák és zárthelyik teljesítésében, valamint a szakdolgozat megírásához nélkülözhetetlen program megismerésében.

Továbbá, köszönöm édesanyámnak aki megtanította nekem, hogy bármilyen kilátástalan is legyen a helyzet soha ne adjam fel és bármilyen problémám is akadt hozzá bátran fordulhattam segítségért bármikor. A többi családtagomnak is köszönök mindenféle támogatást.

Végül, de nem utolsó sorban óriási köszönet illeti barátnőmet, Sánta Viktóriát, aki a legreménytelenebb pillanatokban is bátorított és ösztönző szavaival erőt adott a folytatásra.

Bevezetés

Szakdolgozatom témájának a körosztási polinomokat választottam. Ez egy roppant érdekes függvény család, számos érdekes tulajdonsága ismert a matematika csodálatos, szerte-ágazó világában. Néhány példa a körosztási polinomok felhasználhatóságának lehetőségeiről, melyekről szó lesz a dolgozatban.

A **számelméletben** a *Dirichlet-tétel* egy speciális esetének, a *Zsigmondy-tételnek* valamint a *Völgytételnek* bizonyítása a körosztási polinomok segítségével is végrehajtható. Az **absztrakt algebrában**, a *Galois-elméletben* is gyakran használjuk őket. Dolgozatomban a sokszögek szerkeszthetősége kapcsán szerepelnek, és felbukkannak a véges ferdetestek kommutativitását kimondó Wedderburn-tétel bizonyításában is.

Az érdeklődésemet a téma iránt tehát a téma sokszínűsége keltette fel. Ebből a sokféle alkalmazásból nyújtok egy kis ízelítőt az olvasónak az alapoktól kezdve egészen a kissé bonyolultabb bizonyításokig.

Az anyag feldolgozásban az irodalomjegyzékben feltüntetett forrásokat használtam.

1. Alapfogalmak: egységgyök, primitív egységgyök, körosztási polinom

Ebben a fejezetben néhány egyszerű definícióval alapozom meg a folyamatot, amik alapvető fontosságúak a körosztási polinomok előállításához, az ezekkel való számolásokhoz és a bizonyításokban való alkalmazáshoz.

1.1. Egységgyök

1.1.0.1. Definíció. ***(Egységgyök)*** *Azt mondjuk, hogy az $\varepsilon \in \mathbb{C}$-beli szám n-edik egységgyök, ha $\varepsilon^n = 1$. Az ε komplex szám egységgyök, ha $\exists n \in \mathbb{N}^+$, melyre ε n-edik egységgyök.*

1.1.0.2. Tétel. *Az n-edik egységgyökök a következő alakban írhatóak fel:*

$$\varepsilon_k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n} \quad (k = 0, 1, ...n-1)$$

Ezt a jelölést használva $\varepsilon_0 = 1$ és $\varepsilon_k = \varepsilon_1^k$ a Moivre-képlet alapján.

1.2. Primitív egységgyök

1.2.0.1. Definíció. ***(Primitív egységgyök)*** *Az ε komplex szám primitív n-edik egységgyök, ha n a legkisebb olyan természetes szám, melyre ε n-edik egységgyök, vagyis az összes olyan komplex szám, melynek a rendje n.*

1.2.0.2. Tétel. *Az $\varepsilon_k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}$ egységgyök akkor és csak akkor primitív n-edik egységgyök, ha k és n relatív prímek.*

1.3. Körosztási polinom definíciója és rekurzív kiszámítása

1.3.1. Definíció. ***(Körosztási polinom)*** *Az n-edik körosztási polinom alatt azt a normált polinomot értjük, melynek csak a primitív n-edik egységgyökök a gyökei és mindegyik egyszeres, más szóval a primitív n-edik egységgyökök minimálpolinomja. Ezt a polinomot Φ_n-nel jelöljük:*

$$\Phi_n(x) = \prod_{o(\varepsilon)=n} (x - \varepsilon),$$

A $\Phi_n(x)$ fokát könnyen meg tudjuk határozni. Mindegyik gyöktényező különböző és mindegyik komplex szám egyszeres gyöke, tehát a polinom gyöktényezőinek a száma megegyezik az n-edik primitív egységgyökök számával. Ezért $deg(\Phi_n(x)) = \varphi(n)$, ahol φ alatt az Euler-féle φ függvényt értjük.

A körosztási polinomok csak néhány n esetére számolható ki könnyen a fenti képlet felhasználásával. Csak egy darab primitív első egységgyök van (1) és második primitív egységgyökből is szintén csak egy darab van (-1). Az $n = 1$ és $n = 2$ esetben kifejezetten könnyen megkaphatjuk a körosztási polinomokat, de az $n = 4$ eset sem okozhat problémát, ugyanis a negyedik primitív egységgyökökből két darab van $(i, -i)$. Írjuk is fel ezeket a polinomokat:

$$\Phi_1(x) = x - 1 \qquad \Phi_2(x) = x + 1 \qquad \Phi_4(x) = (x - i)(x + i) = x^2 + 1$$

A nyolcadik primitív egységgyököket is meg tudjuk határozni egy kis elszántsággal $\left(\pm\frac{\sqrt{2}}{2} \pm \frac{\sqrt{2}}{2}i\right)$. Könnyen észrevehető, hogy a harmadik és hatodik primitív egységgyököket is érdemes lehet kiszámolni, hiszen a $\pi/6$ és $\pi/3$ szögfüggvényértékei is szépen felírhatók. Így a harmadik primitív egységgyököket $\left(-\frac{1}{2} \pm \frac{\sqrt{3}}{2}i\right)$ és a szintén két darab hatodik primitív egységgyököket beírva a képletbe kapunk meg további három körosztási polinomot:

$$\Phi_8(x) = \left(x - \frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i\right)\left(x - \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i\right)\left(x + \frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i\right)\left(x + \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i\right) =$$

$$= x^4 + 1$$

$$\Phi_3(x) = \left(x + \frac{1}{2} - \frac{\sqrt{3}}{2}i\right)\left(x + \frac{1}{2} + \frac{\sqrt{3}}{2}i\right) = x^2 + x + 1$$

$$\Phi_6(x) = \left(x - \frac{1}{2} - \frac{\sqrt{3}}{2}i\right)\left(x - \frac{1}{2} + \frac{\sqrt{3}}{2}i\right) = x^2 - x + 1$$

A polinomok gyökeit nézve és a kissé bonyolult kiszámítást figyelembe véve azt várnánk, hogy a polinom is hasonló alakú lesz, de a zárójeleket kibontva látjuk, hogy a kapott polinomok „szép”-ek, mert együtthatói egész számok. Az ötödik körosztási polinomnál viszont már nagyobb problémába ütközünk. Ennek a polinomnak az előállításához a $\cos 72°$ és $\sin 72°$ szögfüggvényértékek segítségével tudnánk csak felírni ezt a polinomot. Ezek pontos értéke kiszámolható, ám bonyolultabb eredményt ad mint az eddigiek, az $n = 7$ esetben tovább romlik a helyzetünk. Ez nem sok reménnyel kecsegtet, hogy bonyolultabb értékekre és kiszámolhassuk $\Phi_n(x)$ együtthatóit. Szerencsére a helyzetünk sokkal jobb, hiszen az előbb láttuk, hogy a kiszámolt körosztási polinomok együtthatói egészek. Később be fogjuk látni, hogy ez bármilyen $n \in \mathbb{N}$ számra igaz. Kezdetként vegyünk egy rekurzív kiszámítási módszert:

1.3.2. Állítás. *A körosztási polinomokat megkaphatjuk ezzel a rekurzív képlettel is:*

$$\Phi_n(x) = \frac{x^n - 1}{\prod\limits_{\substack{k|n \\ k \neq n}} \Phi_k(x)}$$

Ezért a körosztási polinomok egész együtthatósak.

Az állítás bizonyítása előtt, vizsgáljuk meg alaposan az állítást. Könnyen látható, hogy például az $n = 100$ esetre szeretnénk kiszámolni az ehhez tartozó körosztási polinomot, akkor egyszerűbb módja is van mint, hogy a bonyolult primitív egységgyökökkel és azok gyöktényezőinek összeszorzásával bajlódnánk. A képlet szerint a századik körosztási polinom konstruálásához elegendő a korábbi körosztási polinomokat ismernünk. Ezeknek a polinomoknak az ismeretében a polinomok maradékos osztási algoritmusával kevesebb munka árán is kiszámolható $\Phi_{100}(x)$. Sőt, elég csupán néhány $\Phi_k(x)$ polinom együtthatóinak az ismerete. Az $n = 100$ esetben például elég a $k = 1, 2, 4, 5, 10, 20, 25, 50$ eseteket ismernünk, azaz k valódi osztója 100-nak. Most következzen az állítás bizonyítása:

Bizonyítás. Az $x^n - 1$ gyökei csak az n-edik egységgyökök és mindegyik gyök multiplicitása 1. Ezeknek a komplex számoknak a rendje minden esetben osztja n-et. Az olyan számoknak, melyeknek a rendje nem n, az nem gyöke a Φ_n polinomnak. Amikor $\Phi_k(x)$-szel leosztunk, valójában ezekkel a tagokkal egyszerűsítünk le. A fenti rekurzív képletet ezt bizonyítja. A nevezőben lévő körosztási polinomokról tudjuk, hogy normáltak. Indukció alkalmazásával a kisebb fokú körosztási polinomokról láthatjuk, hogy együtthatóik egész számok, így $\mathbb{Z}[x]$-ben is végrehajtható a maradékos osztás algoritmusa.

A képletet más alakban is fel tudjuk írni, amelyből könnyebben észrevehető, miért is lesz igaz:

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

Összefoglalva tehát, ha minden $k \mid n$-re ismerjük $\Phi_k(x)$-et, akkoraz n-edik körosztási polinomot is ki tudjuk számolni könnyedén. Nézzünk néhány példát:

1.3.3. Példa. $\Phi_5(x) = \dfrac{x^5 - 1}{\Phi_1(x)} = \dfrac{x^5 - 1}{x - 1} = x^4 + x^3 + x^2 + x + 1$

$$\Phi_7(x) = \frac{x^7 - 1}{\Phi_1(x)} = \frac{x^7 - 1}{x - 1} = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$

$$\Phi_9(x) = \frac{x^9 - 1}{\Phi_1(x)\Phi_3(x)} = \frac{x^9 - 1}{(x-1)(x^2 + x + 1)} \frac{x^9 - 1}{x^3 - 1} = x^6 + x^3 + 1$$

$$\Phi_{10}(x) = \frac{x^{10}-1}{\Phi_1(x)\Phi_2(x)\Phi_5(x)} = \frac{x^{10}-1}{(x-1)(x+1)(x^4+x^3+x^2+x+1)} =$$

$$= \frac{x^{10}-1}{(x^5-1)(x+1)} = x^4 - x^3 + x^2 - x + 1$$

Az első két esetből, egyszerűen általánosíthatunk tetszőleges $n = p$ prím esetére, ugyanis ebben az esetben n-nek csak egyetlen osztója van ami nem önmaga, így csak egy taggal kell leosztani, hogy megkapjuk a keresett polinomot.

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

A Φ_9 és Φ_{10} kiszámolásakor a nevezőben az előbb tárgyalt esetet használtuk fel, $p = 3$ valamint $p = 5$ értékekre, így könnyen tudtuk egyszerűsíteni a hányadost.

Számoljuk ki $\Phi_{100}(x)$-et, de csak a korábbi körosztási polinomokat vesszük ehhez igénybe. A szükséges polinomok közül néhányat már fel is írtunk, ezért csak Φ_{20}, Φ_{25} és Φ_{50} együtthatói kellenek a századik körosztási polinom meghatározásához. Ahogy az előbb is, most is tudjuk egyszerűsíteni a számításainkat, de ettől még a számolások tovább bonyolódnak és a képletek is egyre csak hosszabbak lesznek.

$$\begin{aligned}
\Phi_{20}(x) &= \frac{x^{20}-1}{\Phi_1(x)\Phi_2(x)\Phi_4(x)\Phi_5(x)\Phi_{10}(x)} = \frac{x^{20}-1}{(x^{10}-1)\Phi_4(x)} = \frac{x^{10}+1}{x^2+1} = \\
&= x^8 - x^6 + x^4 - x^2 + 1 \\
\Phi_{25}(x) &= \frac{x^{25}-1}{\Phi_1(x)\Phi_5(x)} = \frac{x^{25}-1}{x^5-1} = x^{20} + x^{15} + x^{10} + x^5 + 1 \\
\Phi_{50}(x) &= \frac{x^{50}-1}{\Phi_1(x)\Phi_2(x)\Phi_5(x)\Phi_{10}(x)\Phi_{25}(x)} = \frac{x^{50}-1}{(x^{25}-1)\Phi_2(x)\Phi_{10}(x)} = \\
&= \frac{x^{25}+1}{(x+1)(x^4-x^3+x^2-x+1)} = x^{20} - x^{15} + x^{10} - x^5 + 1 \\
\Phi_{100}(x) &= \frac{x^{100}-1}{\Phi_1(x)\Phi_2(x)\Phi_4(x)\Phi_5(x)\Phi_{10}(x)\Phi_{20}(x)\Phi_{25}(x)\Phi_{50}(x)} = \\
&= \frac{x^{100}-1}{(x^{50}-1)\Phi_4(x)\Phi_{20}(x)} = \frac{x^{50}+1}{(x^2+1)(x^8-x^6+x^4-x^2+1)} = \\
&= x^{40} - x^{30} + x^{20} - x^{10} + 1
\end{aligned}$$

Egyéb képletek segítségével tovább csökkenthető a számolások bonyolultsága. Ilyen képletekre fogunk nézni most néhány példát.

1.3.4. Állítás. *Ha n páratlan, akkor $\Phi_{2n}(x) = \Phi_n(-x)$*

Bizonyítás. A képletet elemezve hamar rájövünk, hogy a két polinom foka megegyezik, ugyanis a definíció szerint $deg(\Phi_n(x)) = \varphi(n)$. A $\varphi(n)$ függvény multiplikatiyitását kihasználva $deg(\Phi_{2n}(x)) = \varphi(2n) = \varphi(2)\varphi(n) = \varphi(n)$. A $-x$ változó helyettesítésével a polinom foka nem változik: $deg(\Phi_n(-x)) = \varphi(n)$. A definícióból tudjuk, hogy a körosztási polinomok főegyütthatója 1, ezért a két polinomnak megegyezik a főegyütthatója. Ha megmutatjuk, hogy ugyanazok a gyökeik, akkor a két polinom azonos.

Legyen ε primitív $2n$-edik egységgyök. Tudjuk, hogy $\varepsilon^{2n} = 1$, ezért ε^n gyöke az $x^2 - 1$ polinomnak. Viszont $\varepsilon^n \neq 1$, mert ε primitív $2n$-edik egységgyök, ezért $\varepsilon^n = -1$. Vagyis $(-\varepsilon)^n = (-1)^n\varepsilon^n = (-1)(-1) = 1$, mivel n páratlan paritású. Ebből következik, hogy ha ε rendje $2n$, akkor n osztható $-\varepsilon$ rendjével. $o(\varepsilon) = 2n \Rightarrow o(-\varepsilon) = n_1 \mid n$. ε rendje $2n$, ezért n_1 nem lehet kisebb n-nél, mivel $(-\varepsilon)^{2n_1} = \varepsilon^{2n_1} = 1$, azaz a rendje $2n_1$ lenne ami kisebb mint $2n$, ez ellentmondana az állításnak. Mivel $-\varepsilon$ rendje n, ezért $\Phi_n(-\varepsilon) = 0$. A $\Phi_{2n}(x)$ polinom összes gyöke a $\Phi_n(-x)$ polinomnak is gyöke.

1.3.5. Állítás. *Vegyünk két természetes számot m, n, úgy hogy m osztója legyen n-nek és n minden prímosztója osztója legyen m-nek is. Ez esetben $\Phi_n(x) = \Phi_m(x^{n/m})$.*

Bizonyítás. Az *1.3.4* bizonyításához hasonlóan most is először a jobb és bal oldali polinom fokát hasonlítjuk össze. Itt $deg\Phi_n(x) = \varphi(n)$, és $deg\Phi_m(x^{n/m}) = \frac{n}{m}\varphi(m)$. Ugyanakkor a feltételek szerint $m \mid n$, és n minden prímosztója osztja m-et is, így egy jól ismert képlet szerint $\varphi(n) = \frac{n}{m}\varphi(m)$. Vagyis a két polinom foka egyenlő. Így ismét elegendő megmutatnunk, hogy a bal oldalon szereplő polinom gyökei gyökei lesznek jobb oldalnak is. Vegyük az ε n-edik egységgyököt és helyettesítsük be a jobb oldalon szereplő polinomba. A hatvány primitív rendjére vonatkozó $o(z^k) = \frac{o(z)}{(o(z),k)}$ képletet felhasználva kapjuk, hogy $o(\varepsilon^k) = \frac{o(\varepsilon)}{(o(\varepsilon),k)} = \frac{n}{(n,k)} = \frac{n}{k} = m$. Vagyis $\varepsilon^{n/m}$ gyöke $\Phi_m(x)$-nek, azaz $\Phi_m(\varepsilon^{n/m}) = 0$. Amiből következik, hogy a polinom az $x^{n/m}$ behelyettesítés után $\Phi_m(x)$ polinommal egyezik meg.

1.3.6. Példa. *Számítsuk ki ismét a $\Phi_{100}(x)$-et az utóbbi két képlettel. Reményeink szerint most egyszerűbben a végére jutunk. Először a 1.2.4. Állítás-t vesszük igénybe, $\Phi_{10}(x)$ kiszámításához:*

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

Most pedig a második összefüggés alapján számoljuk ki $\Phi_{100}(x)$-et, az $m = 10$ és $n = 100$ értékek helyettesítésével:

$$\Phi_{10}(x) = x^4 - x^3 + x^2 - x + 1 \quad \Longrightarrow \quad \Phi_{100}(x) = x^{40} - x^{30} + x^{20} - x^{10} + 1$$

Lényeges különbség van a két módszer között, ugyanis a második számolás során gyakorlatilag csak a $\Phi_5(x)$ polinomra volt szükségünk, ezért sokkal kevesebb információ tudatában is fel tudtuk írni a polinomot. Továbbá az sem utolsó szempont, hogy egyszerűbb, rövidebb a számítás.

Következzen egy kissé általánosabb képlet. Néhány korábbi tétel csak speciális esete ennek:

1.3.7. Állítás. *Legyen $n \in \mathbb{N}$ tetszőleges és p prím. Ekkor:*

1. $p \mid n \Longrightarrow \Phi_{np}(x) = \Phi_n(x^p)$
2. $p \nmid n \Longrightarrow \Phi_{np}(x) = \dfrac{\Phi_n(x^p)}{\Phi_n(x)}$

Észrevehető, hogy az *1.3.7.* első része tulajdonképpen egy speciális esete a korábban tárgyalt *1.3.5*-nek, viszont az *1.3.5* is gyorsan következik az *1.3.7.1*-ből.

Bizonyítás. Az első állítás következik az *1.3.5* Állításból.
A második állítás bizonyításához itt is vizsgáljuk meg a két polinom fokát: $\varphi(pn) = \varphi(p)\varphi(n) = (p-1)\varphi(n)$. A hányados számlálójának foka $p\varphi(n)$, míg a nevezőnek $\varphi(n)$, azaz a jobb oldali hányadospolinomnak szintén $(p-1)\varphi(n)$ a foka. Ezután ismét a hatvány rendjének képletét alkalmazzuk, mely szerint ε primitív np-edik egységgyök p-edik hatványa n-edik primitív egységgyök: $o(\varepsilon^p) = \frac{o(\varepsilon)}{o(\varepsilon),p} = \frac{np}{p} = n$. Tehát ε gyöke a $\Phi_n(x^p)$ körosztási polinomnak.

Könnyen észrevehető, hogy az *1.3.7* második esetének a $p = 2$ speciális esete már szerepelt az eddigiek során igaz, a képlet kicsit egyszerűbb volt. Viszont ez a megfogalmazás sokkal általánosabb mint az *1.3.4*, mivel így nem csak a $p = 2$ esetre igaz, hanem tetszőleges p prím esetén is.
Az *1.3.7* segítségével nagyon sok n érték esetén jóval könnyebben meg tudjuk határozni a körosztási polinomok együtthatóit. Vegyük az $n = 9000$ értéket és számoljuk ki $\Phi_{9000}(x)$-et. Először csak a módszer lépéseit, a felhasznált polinomokat és az alkalmazott képleteket ismertetem:

$$\Phi_3(x) \xrightarrow{1.3.7.2} \Phi_{3\cdot 5}(x) \xrightarrow{1.3.4} \Phi_{2\cdot 3\cdot 5}(x) \xrightarrow{1.3.5} \Phi_{2^3\cdot 3^2\cdot 5^3}$$

A fenti képleteket felhasználva az alábbi módon számolható ki $\Phi_{9000}(x)$.

$$\begin{aligned}
\Phi_3(x) &= \frac{\Phi_1(x^3)}{\Phi_1(x)} = \frac{x^3-1}{x-1} = x^2+x+1 \Longrightarrow \\
\Phi_{3\cdot 5}(x) &= \frac{\Phi_3(x^5)}{\Phi_3(x)} = \frac{x^{10}+x^5+1}{x^2+x+1} = x^8-x^7+x^5-x^4+x^3-x+1 \Longrightarrow \\
\Phi_{2\cdot 3\cdot 5}(x) &= \Phi_{3\cdot 5}(-x) = x^8+x^7-x^5-x^4-x^3+x+1 \Longrightarrow \\
\Phi_{9000}(x) &= \Phi_{2^3\cdot 3^2\cdot 5^3}(x) = \Phi_{2\cdot 3\cdot 5}(x^{300}) = x^{2400}+x^{2100}-x^{1500}-x^{1200}-x^{900}+x^{300}+1
\end{aligned}$$

1.3.8. Tétel. *Legyen $n \geq 2$-re a $\Phi_n(x) = a_k x^k + a_{k-1}x^{k-1} + ... + a_1 x + a_0$. Ekkor: $a_k = a_0, a_{k-1} = a_1, ...$ azaz $a_{k-l} = a_l$ minden $0 \leq l \leq k/2$-re.*

1. Megjegyzés. *A fenti tulajdonsággal rendelkező polinomok a reciprok polinomok egyik osztályát alkotják. Egy $f(x)$ polinomot pontosan akkor nevezzük reciprok polinomnak, ha α-ra, ami gyöke neki, $1/\alpha$ is gyöke, méghozzá ugyanakkora multiplicitással. Megmutatható, hogy egy $f(x) = a_k x^k + ...a_0$ polinom pontosan akkor reciprok polinom, ha $a_{k-l} = a_l$ $\forall 0 \leq l \leq k/2$-re vagy $a_{k-l} = -a_l$ $\forall 0 \leq l \leq k/2$-re. (Ez utóbbi esetben $a_{k/2} = 0$, feltéve, hogy $2 \mid k$.) Az első esetben az együtthatók szimmetrikusak, a másikban antiszimmetrikusak.*

Bizonyítás. A megjegyzés alapján elegendő megmutatnunk, hogy ε-nal együtt $1/\varepsilon$ is gyöke $\Phi_n(x)$-nek, ez viszont világos, hiszen $o(\varepsilon) = o(1/\varepsilon) = o(\overline{\varepsilon})$. Így $\Phi_n(x)$ reciprok polinom, és mivel $(x-\varepsilon)$-nal együtt $(x-\overline{\varepsilon})$ is gyöktényező, ezért $\Phi_n(x)$-ből kiemelhető $(x-\varepsilon)(x-\overline{\varepsilon}) = x^2 - 2Re\varepsilon + \varepsilon\overline{\varepsilon} = x^2 - 2Re\varepsilon + 1$. Ez egyetlen esetben nem tehető meg: $n = 2$ esetén -1 is gyök, és ilyenkor a megfelelő gyöktényező $(x+1)$. De ez azt jelenti, hogy $\Phi_n(x) = f_1(x)...f_k(x)$, ahol $k = \varphi(n)/2$, és $\forall f_i$ konstans tagja 1. Így $\Phi_n(x)$-re csak a szimmetrikus feltétel teljesülhet.

Az alábbi táblázatban felsorolom az első 20 körosztási polinomot:

$\Phi_1(x)$	$=$	$x-1$
$\Phi_2(x)$	$=$	$x+1$
$\Phi_3(x)$	$=$	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
$\Phi_{13}(x)$	$=$	$x^{12}+x^{11}+x^{10}+x^9+x^8+x^7+$ $x^6+x^5+x^4+x^3+x^2+1$
$\Phi_{14}(x)$	$=$	$x^6-x^5+x^4-x^3+x^2-x+1$
$\Phi_{15}(x)$	$=$	$x^8-x^7+x^5-x^4+x^3-x+1$
$\Phi_{16}(x)$	$=$	x^8+1
$\Phi_{17}(x)$	$=$	$x^{16}+x^{15}+x^{14}+x^{13}+x^{12}+x^{11}+x^{10}+x^9+$ $+x^8-x^7+x^5-x^4+x^3-x+1$
$\Phi_{18}(x)$	$=$	x^6-x^3+1
$\Phi_{19}(x)$	$=$	$x^{18}+x^{17}+x^{16}+x^{15}+x^{14}+x^{13}+x^{12}+x^{11}+x^{10}+$ $+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1$
$\Phi_{20}(x)$	$=$	$x^8-x^6+x^4-x^2+1$

A táblázatot elnézegetve hamar észrevehetjük, hogy a polinomok együtthatói csak ± 1 vagy 0. Ez nincs mindig így, ha kicsit nagyobb értékekre is meghatározzuk a polinom együtthatóit a 105-ödik körosztási polinom esetében feltűnik, hogy a hetedfokú tag együtthatója 2. Ez nem véletlenül van így, hiszen a körosztási

polinomokra igaz az alábbi tétel:

1.3.9. Tétel. *Ha p és q különböző prímek, akkor a $\Phi_{pq}(x)$ együtthatói $-1, 0, 1$*

Ezt a Tételt és a $2n$-edik körosztási polinomra vonatkozó képletet figyelembe véve, érthető hogy a 105 a legkisebb ilyen szám, hiszen egy olyan számra van szükségünk amely három páratlan prím szorzata. Nem lehet n páros, mert akkor alkalmaznánk rá a *1.3.4* Állítást, ami csak a $n/2$-edik körosztási polinom páratlan fokú tagjainak együtthatóit szorozza -1-gyel. Ezért a ± 1 együtthatók továbbra is ∓ 1 együtthatók maradnak. Ha nem $\pm 1, 0$ együtthatót szeretnénk, akkor n csak valamely három páratlan prím szorzata lehet. A legkisebb ilyen értéket akkor kapjuk, hogyha a három legkisebb páratlan prímszámot szorozzuk össze, azaz $n = 3 \cdot 5 \cdot 7 = 105$.

1.4. Explicit képletek

1.4.1. Definíció. ***(Möbius-féle inverz függvény)*** *Tekintsük az n pozitív szám prímfaktorizációját: $\prod_{i=1}^{m} p_i^{k_i}$, p_i különböző prímeket jelöl. A $\mu : \mathbb{N} \to \mathbb{N}$ függvény legyen az*

$$\mu(n) = \begin{cases} 1 & n = 1, \\ (-1)^m & n = p_1 p_2 ... p_{k_m}, \\ 0 & \textit{különben.} \end{cases}$$

1.4.2. Tétel. *Ha $n \in \mathbb{Z}^+$, akkor*

$$\sum_{k|n} \mu(k) = \begin{cases} 1 \textit{ ha } n = 1, \\ 0 \textit{ ha } n \neq 1. \end{cases}$$

Bizonyítás. Legyen $n = p_1^{\alpha_1} ... p_2^{\alpha_k} > 1$. Az produktumban nyilván csak a négyzetes k-kra lesz $\mu(k)$ értéke nem nulla, amik megfelelnek az n prímosztói egy-egy részhalmazának. Mivel ugyanannyi páros, mint páratlan részhalmaz van, ezért ugyanannyiszor kapunk $+1$-et és -1-et. Így az összeg 0.

1.4.3. Tétel. *A körosztási polinomot fel tudjuk írni a Möbius-féle inverz függvény segítségével is.*

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

Bizonyítás. Vezessük be a következő jelölést: $k \mid n$-re legyen $k' = \frac{n}{k}$. A bizonyítandó képlet tehát:

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

és világos, hogy a két felírás ekvivalens, mivel ha k végigfut n osztóin, akkor k' is ugyanazt teszi. Az is világos, hogy a „szorzatpolinom" gyöktényezői mind $(x-\varepsilon)$ alakúak, ahol $o(\varepsilon) \mid n$. Azt kell megmutatnunk, hogy az $(x-\varepsilon)$ gyöktényező multiplicitása egy, ha $o(\varepsilon) = n$, és 0 egyébként. (Azért beszélünk csak idézőjelesen szorzatpolinomról, mert a kitevők negatívak is lehetnek, azaz itt polinomok hányadosairól van szó.) Milyen (x^k-1) tényezőkben szerepel tehát egy $(x-\varepsilon)$ gyöktényező, ha $o(\varepsilon) = t^2$. Minden olyan k-nál, ahol $t \mid k$, méghozzá $\mu(k')$ kitevővel. Ezeket összeadva a kitevők összege $\sum_{k'|t'} \mu(k')$, ami az előző *1.4.2* Tétel szerint 0, ha $t' > 1$, azaz $t < n$, és 1, ha $t' = 1$, azaz $k = n$. És pontosan ezt akartuk bizonyítani.

2. Körosztási polinomok irreducibilitása

A körosztási polinomok sokoldalú alkalmazhatóságának egyik legfontosabb oka a Φ_n polinomok irreducibilitása. Mint ismeretes, $\mathbb{Z}[x]$-beli polinomok irreducibilitása ekvivalens $\mathbb{Z}$ és $\mathbb{Q}$ felett, feltéve, hogy a polinom legalább elsőfokú, és az együtthatóinak a legnagyobb közös osztója 1. Mivel $\Phi_n(x)$ minden n-re normált, nem konstans, a továbbiakban mindig $\mathbb{Q}[x]$-beli irreducibilitásról fogunk beszélni, de ez automatikusan $\mathbb{Z}[x]$-beli felbonthatóságot is jelent.
Most először egy speciális esetben mutatjuk meg, hogy $\Phi_n(x)$ irreducibilis $\mathbb{Q}[x]$-ben, mivel ennek az esetnek a bizonyítása könnyű és tanulságos.

2.1. A $\Phi_p(x)$ polinomok irreducibilitása

2.1.1. Tétel. *$\Phi_p(x)$ irreducibilis $\mathbb{Q}$ felett $\forall p$ prímre.*

Bizonyítás. Ismeretes, hogy $\Phi_p(x) = \dfrac{x^p-1}{x-1} = x^{p-1} + ... + 1$ Tekintsük most az $F(x) = \dfrac{(x+1)^p-1}{(x+1)-1} = \dfrac{\sum_{i=0}^{p}\binom{p}{i}x^{p-i}}{x} = \dfrac{x^p + \binom{p}{1}x^{p-1} + ... + \binom{p}{p-1}x + 1 - 1}{x} = x^{p-1} + \binom{p}{1}x^{p-2} + ... + \binom{p}{p-1}$. Alkalmazzuk $F(x)$-re a jól ismert Schönemann-Eisenstein-féle irreducibilitási kritériumot.

2.1.2. Tétel. ***Schönemann-Eisenstein-kritérium*** *Legyen $f = a_nx^n + a_{n-1}x^{n-1} + ... + a_1x + a_0 \in \mathbb{Z}[x]$ olyan polinom, melyhez $\exists p$ prímszám, hogy:*

- $p \nmid a_n$
- $p \mid a_i, \quad \forall 0 \leq i \leq n-1$
- $p^2 \nmid a_0$

Ekkor az f polinom irreducibilis $\mathbb{Q}[x]$ felett.

Mivel $p \mid \binom{p}{i}$ $\forall 1 \leq i \leq p-1$, hiszen a számlálóban szerepel p, viszont a nevezőben nem, továbbá $\binom{p}{p-1} = p$ nem osztható p^2-tel, ezért alkalmazhatjuk $F(x)$-re a Schönemann-Eisenstein-kritériumot. Azt kapjuk, hogy $F(x) = \Phi_p(x+1)$ irreducibilis $\mathbb{Q}$ felett. Ha Φ_p reducibilis lenne, azaz $\Phi_p(x) = g(x)h(x)$, ahol $g, h \in \mathbb{Q}[x]$ nem konstans polinomok, akkor $F(x) = \Phi_p(x+1) = g(x+1)h(x+1)$ egy nem triviális faktorizációját adva $F(x)$-nek. Így $\Phi_p(x)$ is irreducibilis $\mathbb{Q}$ felett.

2.2. $\Phi_n(x)$ irreducibilitása az általános esetben

Most egy lényegesen nehezebb bizonyítással megmutatjuk, hogy $\Phi_n(x)$ $\forall n$ esetén irreducibilis.

2.2.1. Tétel. *$\Phi_n(x)$ irreducibilis $\mathbb{Q}[x]$-ben $\forall n$-re.*

Bizonyítás. Tegyük fel, hogy $\Phi_n(x)$ szorzattá bontható.

$$\Phi_n(x) = f_1(x)...f_k(x),$$

ahol $f_i(x) \in \mathbb{Z}[x]$, és $f_i(x)$ irreducibilis $\mathbb{Q}[x]$-ben $\forall 1 \leq i \leq k$-re. Feltehető, hogy $\forall i$-re $f_i(x)$ normált, azaz a főegyütthatója 1, hiszen $\Phi_n(x)$ normált, és így a főegyütthatója, ami az $f_i(x)$-ek főegyütthatóinak a szorzata, csak ± 1-ek szorzataként írható fel. Így minden $f_i(x)$-et választhatjuk normáltnak.
A továbbiakban az alábbi segédállítást fogjuk felhasználni.

2.2.2. Lemma. *Legyen p prímszám, melyre $p \nmid n$. Ekkor ha $\varepsilon \in \mathbb{C}$-re: $f1_(\varepsilon) = 0$, akkor $f_1(\varepsilon^p) = 0$.*

Bizonyítás. Először megmutatjuk, hogyan következik ebből $\Phi_n(x)$ irreducibilitása. A feltevés szerint ugyanis $f_1(x)$ nem konstans, tehát $\exists \varepsilon \in \mathbb{C}$ primitív n-edik egységgyök, amire $f_1(\varepsilon) = 0$. Mivel ε primitív n-edik egységgyök, ezért $\forall$ primitív n-edik egységgyök előáll ε^k alakban, ahol $(k, n) = 1$. Ez azt jelenti, hogy $k = p_1 p_2 ... p_l$, ahol p_i-k nem feltétlenül különböző prímek, és $p_i \nmid n$. Ekkor a *3.2.2* Lemma ismételt alkalmazásával azt kapjuk, hogy $\varepsilon^{p_1}, \varepsilon^{p_1 p_2}, ..., \varepsilon^{p_1 p_2 ... p_l} = \varepsilon^k$ is gyöke f_1-nek. Vagyis $f_1(x)$-nek valamennyi primitív n-edik egységgyök gyöke, és így $f_1(x) = \Phi_n(x)$.

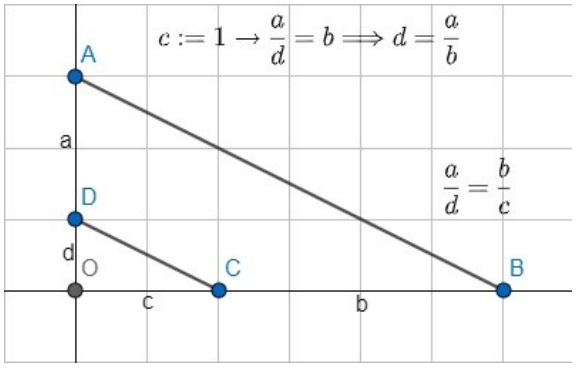
Most bizonyítsuk a *3.2.2* Lemmát. Indirekt módon, vizsgáljuk meg azt az esetet, amikor a lemma nem igaz. Tegyük fel, hogy ε gyöke az f_1 polinomnak, viszont ε^p nem gyöke. Az ε^p biztosan gyöke egy másik f_i polinomnak. A $\Phi_n(\varepsilon^p) = 0$ csak akkor lehetséges, ha valamelyik tényezője a szorzatnak 0. A szorzatot tetszőlegesen átrendezhetjük, attól nem fog változni a polinom értéke, ezért az egyszerűség kedvéért, válasszuk f_2-nek azt a polinomot, melynek a helyettesítési értéke a ε^p helyen 0.

Azt kaptuk tehát, hogy ε gyöke $f_1(x)$-nek és $f_2(x)$-nek is. Így $(f_1(x), f_2(x^p)) \neq 1$, és mivel $f_1(x)$ irreducibilis, ezért $f_1(x) \mid f_2(x^p)$ $\mathbb{Q}[x]$-ben. De f_1 normált polinom, így az oszthatóság $\mathbb{Z}[x]$-ben is fennáll, ezért $\exists g(x) \in \mathbb{Z}[x]$, hogy $f_1(x)g(x) = f_2(x^p)$. Feltesszük még most ezeknek a polinomoknak a modulo p vett változatát. $h(x) \in \mathbb{Z}[x]$ esetén jelölje $h^*(x)$ azt a $\mathbb{Z}_p[x]$-beli polinomot, melynek együtthatói a h együtthatóinak a maradéka modulo p. Ekkor ez a megfeleltetés művelettartó, így $f_1^*(x)g^*(x) =$

$f_2^*(x^p)$ $\mathbb{Z}_p[x]$-ben. De $\mathbb{Z}_p[x]$-ben minden együtthatóra igaz az $a^p \equiv a$ összefüggés, továbbá szabad tagonként p-edik hatványra emelni, így $f_2^*(x^p) = (f_2(x))^p$. Ezek szerint az $f_1^*(x)$ nem konstans polinom osztja $(f_2(x))^p$-t, és így van közös irreducibilis faktoruk: $h(x)$. Ez azt jelenti, hogy $h \mid f_1^*$ és $h \mid f_2^*$, és mivel $f_1^*, f_2^* \mid (x^n - 1)^*$, így $h^2 \mid (x^n - 1)^*$ $\mathbb{Z}_p[x]$-ben. Ez viszont nem lehetséges, mert $(x^n - 1)^*$-nak és a deriváltjának, nx^{n-1}-nek nincs közös faktora. Mivel ellentmondásra jutottunk, ezért a lemma állítása igaz, és ebből következik a tétel helyessége is.

3. Szabályos sokszögek szerkeszthetősége

Ebben a fejezetben arról szólunk, hogy mi módon kapcsolódnak a körosztási polinomok szerkesztési feladatokhoz. A tárgyalásmódunk nagyrészt meseszerű, vázlatos lesz, és a szabályos sokszögek szerkeszthetőségéről szóló állításunk csak az egyik irányát fogjuk bizonyítani (mert a másik irányhoz más, például komolyabb csoportelméleti ismeretek is kellenének, és az most nem tárgya a dolgozatnak). Szerkesztési feladatoknál az a kérdés, hogy adott alappontokból (alapobjektumokból) kiindulva meg tudunk-e szerkeszteni egy másik elvárt tulajdonságokkal rendelkező pontot (objektumot) csak körzőt és vonalzót használva. Ha nincsenek kiinduló pontjaink (például a feladat az, hogy szerkesszünk 20°-os szöget), akkor azt tesszük fel, hogy adva van egy egységhosszúságú szakasz két végpontjával. Így mindig feltehetjük, hogy adva van egy koordináta-rendszerünk, melynek $(0,0)$ és $(1,0)$ koordinátájú pontja két megadott pont. Elemi szerkesztési lépések mutatják, hogy ha az (a,b) szerkeszthető, akkor $(a,0)$ és $(0,b)$, sőt $(b,0)$ is szerkeszthető. És megfordítva, ha $(a,0)$ és $(b,0)$ szerkeszthető, akkor az (a,b) pont is szerkeszthető. Ily módon van értelme „szerkeszthető számról" beszélni. Az $a \in \mathbb{R}$ szerkeszthető, ha $(a,0)$ szerkeszthető. És (a,b) szerkeszthető, ha a és b szerkeszthető. Most megmutatjuk, hogy ha vesszük az alappontként megadott pontjaink koordinátáit - ezek szerkeszthetők -, akkor szerkeszthető lesz minden olyan $\alpha \in \mathbb{R}$ is, ami benne van az alappontok által generált $K \leq \mathbb{R}$ résztestben. Világos, hogy az x tengelyre nézve az $(a,0)$ pont után a b hosszúságú szakaszt, $a+b$ is szerkeszthető, s mivel az origó adott, ezért $(a,0)$ tükrözöttjét, $(-a,0)$-t is meg tudjuk szerkeszteni, ha a szerkeszthető. Igazolnunk kell még, hogy két szerkeszthető szám, a és b szorzatot, ab is szerkeszthető, illetve ha $b \neq 0$, akkor az a/b hányados is. Legyen $A = (0;a)$; $B = (b;0)$, valamint $O = (0;0)$ és ettől egységnyi távolságra lévő $C = (1;0)$. Húzzuk be az AB szakaszt, továbbá egy ezzel párhuzamos szakaszt, melynek a kezdőpontja C pont és a végpontja pedig legyen az y-tengellyel való metszéspontja, ezt jelöljük D-vel. Alkalmazzuk a párhuzamos szelők tételét.

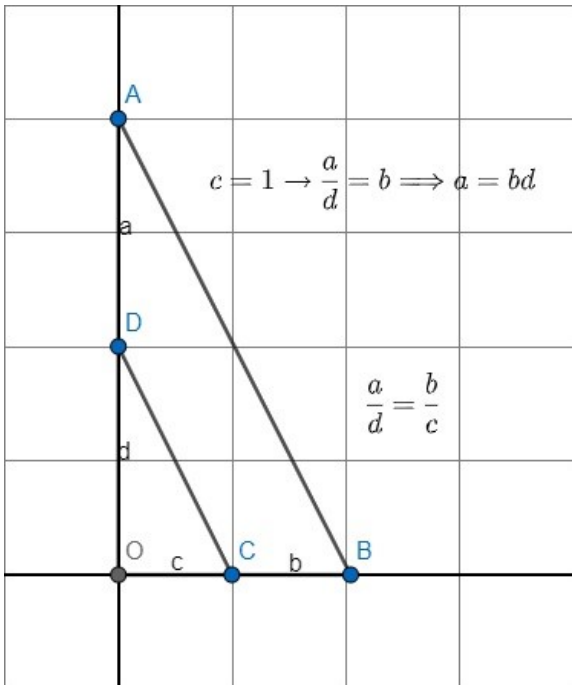


Az alábbi összefüggést kapjuk:

$$d/a = 1/b \Longleftrightarrow d = a/b.$$

Tehát meg tudjuk szerkeszteni két szám hányadosát.

Vegyünk ismét egy koordináta-rendszert, melyben az előző példához hasonlóképpen vesszük fel a pontokat. Szintén húzzunk egy párhuzamos szakaszt az AB szakasszal a C pont és a szakasz y-tengellyel való metszéspontja(D) között.



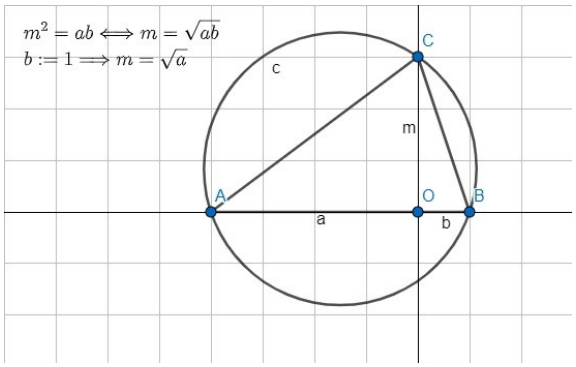
A párhuzamos szelők tételét újra alkalmazva z alábbi háromszögre:

$$c/a = b/1 \Longleftrightarrow c = ab.$$

Tehát két szerkeszthető szám szorzata is szerkeszthető.

Egy ügyes trükkel most azt is belátjuk, hogy bármely $a > 0$ szerkeszthető számok négyzetgyöke is szerkeszthető.

A $\sqrt{a}$ szerkesztéséhez vegyük az $A = (-a; 0)$ és a $B = (1; 0)$ pontokat. Az AB szakaszra rajzoljunk egy Thalész-kört, melynek köríve illeszkedik az A és B pontokra, középpontja pedig az AB szakasz felezőpontja. Ez a kör két helyen metszi az y-tengelyt, a pozitív oldalon vett metszéspontot jelöljük $C = (0; m)$-vel. Ilyen módon választott háromszög esetén az AB szakasz derékszögben látszik a C pontból. Az OC szakasz az ABC derékszögű háromszögnek az átfogóhoz tartozó magassága.



A magasságtétel kimondja, hogy $m^2 = ab$. Válasszuk $b := 1$, behelyettesítve $m^2 = a \Longleftrightarrow m = \sqrt{a}$. Vagyis egy szám négyzetgyökét is tudjuk szerkeszteni körzővel és vonalzóval.

Az elmondottak alapján indukcióval könnyen igazolható az alábbi tétel:

3.1. Tétel. *Legyen $K_0 \leq \mathbb{R}$ egy szerkesztési feladat alapadatai által generált résztest, és tegyük fel, hogy létezik $\mathbb{R}$ résztesteinek egy következő lánca:*

$$K_0 < K_1 < K_2 < ... < K_t \leq \mathbb{R}$$

méghozzá azzal a megkötéssel, hogy K_{i+1}, másodfokú bővítése K_i-nek minden $0 \leq i < t$-re.

Ekkor K_t minden eleme szerkeszthető.

1. Megjegyzés. *K_{i+1} foka K_i felett a K_{i+1} dimenziója K_i felett, és így kaphatjuk meg, hogy egy irreducibilis másodfokú, $K_i[x]$-beli polinom valamely α gyökét hozzávesszük K_i-hez. Mivel a másodfokú egyenlet megoldóképlete alapján α szerkeszthető, ezért K_{i+1} elemei is szerkeszthetők.*

Az az érdekes, hogy a fenti tétel állítása meg is fordítható: ha egy $\alpha \in \mathbb{R}$ szám szerkeszthető, akkor létezik hozzá egy ilyen testlánc. Ez szemléletesen azért igaz, mert a körzős-vonalzós szerkesztés során egyenesek, illetve körök metszéspontjait kapjuk új pontnak, és ezek mindig egy legfeljebb másodfokú egyenlet megoldásaként kaphatók meg. Így a meglevő pontok által generált résztestek egy bővülő testsorozatot adnak, ahol a bővítések foka legfeljebb 2.

A fenti tétellel egy csomó nevezetes szerkesztési problémáról be lehet bizonyítani, hogy nem megoldható.

Igaz ugyanis, hogy minden szerkeszthető pont fokának az alaptest felett 2-hatványnak kell lennie. Így például nem megoldható a kockakettőzés feladata, mert itt az 1 mellé $\sqrt[3]{2}$-t kellene szerkesztenünk, $\sqrt[3]{2}$ foka pedig a kiinduló alaptest, $\mathbb{Q}$ felett 3.

Térjünk most vissza a körosztási polinomokra. Az alábbi tétel egyik módját fogjuk igazolni.

3.2. Tétel. *A szabályos n-szög pontosan akkor szerkeszthető, ha* $n = 2^m p_1 p_2 ... p_k$, *ahol* $m \in \mathbb{N}$, *és* $p_1, p_2, ..., p_k$ *különböző Fermat-prímek (azaz* $p_i = 2^{2^{k_i}} + 1$ *valamilyen* $k_i \in \mathbb{N}$*-re).*

Bizonyítás. Először megmutatjuk, hogy egy szabályos n-szög pontosan akkor szerkeszthető, ha a $a = \cos\frac{2\pi}{n}$ szerkeszthető. Ha ugyanis szerkeszthető egy szabályos n-szög, akkor szerkesztéssel megkaphatjuk a szimmetriaközéppontját, majd ezt a csúcsokkal összekötve egy olyan egyenlő szárú háromszöget, amelynek a szárszöge $\alpha = \frac{2\pi}{n}$. Ha adva van az α szög, akkor az egyik szárra az egységszakaszt felvéve, majd ezt merőlegesen levetítve a másik szögszárra $\cos\frac{2\pi}{n}$ hosszúságú szakaszt kapunk.

Megfordítva, ha $\cos\frac{2\pi}{n}$ adott, akkor az előbbi módon tudunk szerkeszteni egy $\alpha = \frac{2\pi}{n}$ szöget, majd egy egyenlő szárú háromszöget α szárszöggel. Ezt n-szer egymáshoz illesztve a csúcsánál épp egy szabályos n-szöget kapunk.

Ez tehát azt jelenti, hogy ha szerkeszthető szabályos n-szög, akkor $a = \cos\frac{2\pi}{n}$ foka $\mathbb{Q}$ felett (ez az a minimálpolinomjának a foka) 2-hatvány.

A következő lépésben megmutatjuk, hogy $a = \cos\frac{2\pi}{n}$ foka pontosan akkor 2-hatvány, ha az $\varepsilon = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$ primitív n-edik egységgyök foka 2-hatvány. Ha ugyanis $\mathbb{Q}(a)$ foka 2-hatvány, akkor $\varepsilon \in \mathbb{Q}(a)(i\sin\frac{2\pi}{n})$, és $(i\sin\frac{2\pi}{n})^2 = -\sin^2\frac{2\pi}{n} = \cos^2\frac{2\pi}{n} - 1 = a^2 - 1$, így $b = i\sin\frac{2\pi}{n}$ foka legfeljebb 2 a $K(a)$ test felett. Ebből az adódik, hogy ε foka is 2-hatvány. Megfordítva, ha ε foka 2-hatvány, akkor $\overline{\varepsilon} \in \mathbb{Q}(\varepsilon)$, és $\varepsilon + \overline{\varepsilon} = 2\cos\frac{2\pi}{n}$ adott $a \in \mathbb{Q}(\varepsilon)$, vagyis az $a = \cos\frac{2\pi}{n}$ foka is 2-hatvány.

Végezetül azt mutatjuk meg, hogy $\varepsilon = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$ foka (ami éppen $\varphi(n)$, hiszen ε minimálpolinomja $\Phi_n(x)$), 2-hatvány, akkor $n = 2^m p_1 ... p_k$ a megadott feltételekkel.

Tegyük tehát fel, hogy $n = p_1^{\alpha_1} ... p_t^{\alpha_t}$, $\alpha_i \geq 1$.

A φ függvény multiplicitása alapján:

$$\varphi(n) = \varphi(p_1^{\alpha_1}) ... \varphi(p_i^{\alpha_i}) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) ... (p_t^{\alpha_t} - p_t^{\alpha_t - 1}) = p_1^{\alpha_1 - 1} ... p_t^{\alpha_t - 1}(p_1 - 1) ... (p_t - 1)$$

Ez pontosan akkor 2-hatvány, ha $p_i^{\alpha_i - 1}$ és $p_i - 1$ is 2-hatvány. Így a páratlan prímek legfeljebb elsőfokon szerepelhetnek a kanonikus polinom előállításában, és $p_i = 2^{l_i} + 1$ alakú minden szereplő páratlan prímre. Az ilyen alakú prímek viszont mind $2^{2^{k_i}} + 1$ alakúak, azaz Fermat-prímek.

Ezzel beláttuk, hogy csak az ilyen n-ekre lehetnek a szabályos n-szögek szerkeszthetők.

A megfordítás bizonyításához arra lenne szükség, hogy igazoljuk a korábban emlegetett testlánc létesítését, ehhez viszont Galois-elmélet és a 2-csoportok egyes tulajdonságai kellenének, így ezt a bizonyítást most elhagyjuk.

4. Számelméleti alkalmazás

A számelméletben mindig is fontos szerepet játszottak a prímszámok, és számos olyan tételt ismerünk, amely kimondja, hogy végtelen sorozatok végtelen sok prímszámot tartalmaznak. Először Euklidész bizonyította be, hogy a természetes számok halmaza végtelen sok prímszámot tartalmaz. Majd a *Dirichlet-tétel* szerint szintén végtelen sok prím kapható az $nk+1$ alakú számok között. Ennek egy speciális esetét a következőkben be is bizonyítjuk. Ennek a tételnek egy általánosabb formája a

4.1. Dirichlet tétel

4.1.1. Tétel. ***(Dirichlet)*** *Vegyük az $nk+1$ alakú számtani sorozatot, ahol az n rögzített pozitív egész számot tekintjük a differenciának és a sorozat első eleme az 1. A körosztási polinomok segítségével be fogjuk látni, hogy ennek a számtani sorozatnak végtelen sok prím tagja van.*

2. Megjegyzés. *Ez az általános Dirichlet-tétel egy speciális esete.*

Szükségünk lesz az alábbi lemmára:

4.1.2. Lemma. $o_p(c) = n \iff p \mid \Phi_n(c)$ *és* $p \nmid n$.

Bizonyítás. Tegyük fel, hogy $o_p(c) = n$. Ekkor $c^n \equiv 1(\mod p)$. Nullára rendezve az egyenletet kapjuk, hogy $c^n - 1 \equiv 0(\mod p)$. Tehát $c^n - 1 = a \cdot p$ alakban is felírható. A maradékosztályok száma $p-1$, ezért $n \mid p-1$, ebből kifolyólag $p \mid n$ feltétel nem teljesülhet. Az x helyére helyettesítsünk c-t. Tekintsük most az $x^n - 1$ polinom szorzatra bontását,és helyettesítsünk be c-t

$$c^n - 1 = \prod_{k|n} \Phi_k(c).$$

A $c^n - 1 \equiv 0(\mod p)$ egyenlőség miatt tudjuk, hogy a $c^n - 1$ értéknek osztója a p, de ha a jobb oldal osztható, akkor a bal oldalnak is oszthatónak kell lennie p-vel, vagyis valamelyik $k \mid n$: $\Phi_k(c)$ körosztási polinomnak is osztója lesz p. A feltétel alapján tudjuk, hogy c rendje n modulo p, vagyis semmilyen n-nél kisebb értékre nem lesz eggyel kongruens a hatvány. Mivel n a lehető legkisebb ezért $n = k$, hiszen $\Phi_k(c) \mid c^k - 1$, tehát $p \mid \Phi_n(c)$. A másik irány bizonyításához a $p \mid \Phi_n(c)$ és $p \nmid n$ feltételekből fogunk kiindulni. Az eddigiek szerint az n-edik körosztási polinom osztója a $c^n - 1$ polinomnak, de akkor $p \mid c^n - 1$ is teljesül, ezért $c^n \equiv 1(\mod p)$. Tegyük fel, hogy c rendje $t < n$; ekkor $c^t \equiv 1(\mod p)$, és $t \mid n$. A körosztási polinomok szorzataként előállított képletében helyettesítsünk n helyére

t-t: $c^t - 1 = \prod_{kmidt} \Phi_k(c)$. A p prím szintén osztja a bal oldalt, hiszen $c^t \equiv 1(\mod p)$, tehát biztosan osztja a jobb oldalon is valamelyik $\Phi_k(c)$ szorzattényezőt osztja p, és itt $k \mid t < n$. Ez azt jelenti, hogy $c^n - 1 = \prod_{k|n} \Phi_k(c)$ jobb oldalán már két tényezőnek is osztója, vagyis már két tényezőt is találtunk a jobb oldalon, melyre igaz, hogy p osztja.
Nézzük $\mathbb{Z}_p$ test felett az $x^n - 1 = \prod_{k|n} \Phi_k(x)$. Ha p osztja $\Phi_k(c)$-t, akkor $\Phi_k(c) \equiv 0(modp)$, vagy úgyis mondható, hogy c gyöke Φ_k polinomnak $\mathbb{Z}_p$ felett. Beláttuk, hogy két tényező is van a $\prod \Phi_k$ szorzatban, ami osztható p-vel, ezért c legalább két tényezőnek is gyöke. Ha az egyenlőség jobb oldalát osztja, akkor a bal oldalt is, vagyis az $x^n - 1$ polinomnak c legalább kétszeres gyöke. A polinomot deriválva kapjuk, hogy $nc^{n-1} = 0$ $\mathbb{Z}_p$-ben. A feltételek alapján tudjuk, hogy a $\mathbb{Z}_p$ testben $n \neq 0$ és $c \neq 0$, mert $p \nmid n$ és $p \nmid c$, ezért nc^{n-1} nem lehet 0. Tehát c nem gyöke az nx^{n-1} polinomnak, vagyis az $x^n - 1$ polinomnak nem lehet kétszeres gyöke. A lemma állítását ezzel beláttuk.

Most következzen a Dirichlet-tétel bizonyítása:

Bizonyítás. 5.1.1 Tétel(Dirichlet) A tétel azt mondja ki hogy végtelen sok $nk+1$ alakú prím létezik. Vizsgáljuk meg azt az esetet, amikor véges sok ilyen alakú prím található. Használjuk a $p_1, p_2, ..., p_s$ jelölést az összes ilyen prímre, ahol s a prímek számát jelöli. Konstruáljuk meg a $c = \lambda n p_1 ... p_s$ számot, λ egy tetszőleges pozitív számot jelöl és $s = 0$ esetre a prímek szorzata legyen 1. Amennyiben λ kellően nagy: $\Phi_n(c) > 1$. Vegyük $\Phi_n(c)$ egy tetszőleges p prímosztóját. $\Phi_n(c) \mid c^n - 1$

szerint $p \mid c^n - 1$. Ebből következik, hogy $p \nmid c^n$, ezért $p \nmid c$ és p prím, ezért nincs 1-től különböző osztója ami c-t is osztaná, tehát p és c relatív prímek. A c felbontásában szerepel n, ezért $p \nmid n$ is igaz. A lemmát alkalmazva $o_p(c) = n$. Mivel c rendje n és a $\mathbb{Z}_p^\times$ csoport rendje $p-1$, ezért $n \mid p-1$. Írjuk fel $p-1 = nk$ alakban. Az egyenletet rendezve kapjuk, hogy $p = nk + 1$. $(p, c) = 1$, azaz $p \neq p_i$, vagyis találtunk egy $p_1, ..., p_s$ prímektől különböző új prímet.

4.2. Völgytétel

A következő tételben $d(n)$ jelzi az $n \in \mathbb{N}$ szám pozitív osztóinak a számát.

4.2.1. Tétel. ***(Völgytétel)*** *Tetszőleges K pozitív egész számhoz végtelen sok olyan n egész található, amelyre*

$$d(n-1) - d(n) > K$$

és

$$d(n+1) - d(n) > K$$

is teljesül.

A tétel tehát azt mondja ki, hogy a $d(n)$ függvény gráfjában akármilyen nagy völgyek is előfordulnak.

Bizonyítás. Legyen $m = 15^k$, $f(x) = x^m - 1$ és $g(x) = x^m + 1$. Ekkor

$$f(x) = \prod_{d|m} \Phi_d(x)$$

$$g(x) = \frac{x^{2m}-1}{x^m-1} = \prod_{\substack{d|2m \\ d\nmid m}} \Phi_d(x) = \prod_{d|m} \Phi_{2d}(x),$$

mert m páratlan. Az $f(x)$ és $g(x)$ polinomokat a $d \mid m$ feltétel miatt d(m) darab tényezőre bontottuk. Itt $d(15^k) = d(3^k 5^k) = (k+1)^2$, azaz a $15^k = 3^k 5^k$ számnak $(k+1)^2$ osztója van, mert a 3 hatványai közül választhatok k+1 darabot:$3^0, 3^1, 3^2, 3^3, ..., 3^k$ és az 5 hatványai közül is k+1 darabot tudok kiválasztani:$5^0, 5^1, 5^2, 5^3, ..., 5^k$, ezeknek bármilyen kombinációját vehetem az osztója lesz az m számnak, tehát $(k+1)^2$ osztója van m-nek. Nézzük az $f(x)$ szorzatalakjában lévő tényezőkből képezhető részszorzatokat. Mindegyik tényezőről el kell döntenünk, hogy benne legyen a részszorzatban vagy sem. Minden tényezőre nézve két lehetőségünk van és $(k+1)^2$ tényező van, vagyis $2^{(k+1)^2}$ ilyen részszorzat van. A részszorzatokról tudjuk, hogy mindegyik különböző, mert minden tényező irreducibilis. Mivel bármely két részszorzat különbözik, így akárhogyan is választunk ki két részszorzatot maximum véges sok helyen vehetik fel ugyanazt az értéket. Létezik hát egy L_1 konstans küszöbszám, melyre $y > L_1$ esetén az $f(x)$ tényezőiből előállított a t helyen vett helyettesítési értéke minden esetben különböző. Ugyanezt a gondolatmenetet felhasználva a $g(x)$ polinom tényezőiből konstruált részsorozatokhoz is létezik ilyen L_2 konstans küszöbszám.

Válasszuk $L = max(L_1, L_2)$ és $\forall L < y \in \mathbb{Z}^+$ az $f(y)$ és $g(y)$ egész számoknak legalább annyi különböző osztója van, mint a polinomok szorzatalakjában a tényezőkből előállítható részszorzatok száma, hiszen ha egy függvény részszorzata a másiknak akkor biztosan osztója is és a tényezők egész együtthatósak, ezért $f(y)$ és $g(y)$ osztóinak száma legalább $2^{(k+1)^2}$. A negatív és pozitív osztókat egyaránt számoltuk, továbbá ha egy pozitív szám osztója akkor az ellentettje is az, azaz $d(f(y)), d(g(y)) \geq 2^{(k+1)^2-1}$.

Azt akarjuk belátni, hogy $d(y \pm 1)$ és $d(y)$ különbsége bármilyen nagy lehet. Tudjuk, hogy végtelen sok prím van, ezért tudunk választani olyan pozitív prímszámot mely nagyobb L-nél. Jelöljük ezt a számot p-vel. Az f és g polinomoknak p helyen vett helyettesítési értékeire alkalmazva a $d(n)$ függvényt az előbbiek szerint: $d(p^m - 1), d(p^m + 1) \geq 2^{k^2+2k}$.

Viszont $d(p^m) = m+1 = 15^k+1$. Ha egy $d(p^m \pm 1) - d(p^m)$-nél kisebb értékről megmutatjuk, hogy bármilyen nagy lehet, akkor a kezdeti értékre is igaz lesz. A $d(p^m \pm 1)$-et alulról becsülve, a $d(p^m)$-et felülről becsülve a különbségünk biztosan kisebb lesz. Vagyis, $d(p^m-1), d(p^m+1) \geq 2^{k^2+2k} > 2^{k^2}$ és $d(r^m) = m+1 = 15^k+1 < 16^k = 2^{4k}$. A becslést felhasználva kapjuk, hogy $d(p^m \pm 1) - d(p^m) \geq 2^{k^2+2k} - 15^k + 1 \geq 2^{k^2} - 2^{4k} = 2^{4k}(2^{k^2-4k} - 1)$. A $k > 4$ esetekre látjuk, hogy $2^{k^2-4k} - 1$ érték nagyobb mint 1, ezért ha a szorzatból elhagyjuk ezt a tagot, a kifejezés tovább csökken, feltéve, hogy $k > 4$. Minden K szám esetén található olyan k melyre $2^{4k} > K$. Az $n = p^m$ választásra teljesülnek a tételben szereplő feltételek.

4.3. Bunyakovszky sejtés

4.3.1. Sejtés. ***(Bunyakovszky)*** *Tegyük fel, hogy f egy egész együtthatós egyváltozós polinom, melynek a foka pozitív. Ha*

- *f főegyütthatója pozitív;*
- *f irreducibilis az $\mathbb{Z}[x]$ felett;*
- *$n \in \mathbb{Z}^+$-ra az $f(n)$ számok relatív prímek*

feltételek is teljesülnek, akkor az $f(x)$ polinom értéke prím végtelen sok pozitív egészre.

Láttuk, hogy a körosztási polinomokra teljesül az első két feltétel. A harmadik feltételről is tudjuk, hogy teljesül, mert csak akkor nem lennének relatív prímek, ha találnánk olyan 1-től különböző számot, mely osztja f összes együtthatóját. Ez nem lehetséges, mert a konstans tag mindig 1, illetve -1, ha $n = 1$.

Tehát a sejtés szerint a körosztási polinom értéke végtelen sok n-re prím. A következőkben nézzük meg ezt konkrét n értékekre. Vegyük a körosztási polinomokat és vizsgáljuk meg, hogy az n-edik körosztási polinom milyen legkisebb értékekre lesz prím. Ahogy növeljük n értékét vajon hogyan és milyen mértékben változik ez a szám? Az első 100 körosztási polinomra határoztam meg ezeket a minimális értékeket, ezen értékek egy sorozatot alkotnak. Az alábbi kódot a *Maple* nevű programban

futtattam le, melynek eredményeit az alábbi táblázatban összegzem. A táblázatot úgy töltöttem fel, hogy az oszlopszámát az n szám tízes helyi értéken lévő szám adja, valamint a sorszám pedig az egyes helyi értéken szereplő érték. *f:= proc(n) local k; for k from 2 do if isprime(numtheory:-cyclotomic(n, k)) then return k fi od end proc:*
seq(f(n), n = 1 .. 100); [16]

3	5	3	2	14	30	2	3	21	11
2	2	2	2	2	11	2	3	61	4
2	2	10	2	15	24	3	11	41	2
2	2	2	2	25	7	30	16	7	6
2	2	22	14	11	7	2	59	2	44
2	2	2	3	2	2	9	7	2	4
2	2	2	61	5	5	46	2	8	12
2	6	4	2	5	7	85	2	5	2
2	2	6	10	2	19	2	22	2	63
2	4	2	2	6	3	3	2	2	20

5. Wedderburn tétel

Ebben a fejezetben a ferdetestekkel fogunk foglalkozni. A csoportelmélet és a körosztási polinomok segítségével szeretnénk bebizonyítani, hogyha egy ferdetest véges akkor kommutatív is.

5.0.1. Tétel. ***(Wedderburn)*** *Minden véges ferdetest kommutatív.*

Bizonyítás. Vegyünk egy D véges ferdetestet. Jelöljük Z-vel D centrumát. Ekkor Z kommutatív test, így $|Z| = q = p^k$ valamilyen p prímre. Mivel Z részteste D-nek, ezért D vektortér Z felett, így $|D| = q$, ahol $n = dim_{\mathbb{Z}} D$. Legyen D^* a D ferdetest multiplikatív csoportja. Számoljuk meg D^* elemeit úgy, hogy összeadjuk a D^*-beli konjugáltosztályok elemszámát. Itt a Z^*-beli elemek fognak megfelelni az egyelemű konjugáltosztályoknak. Ugyanakkor azt is tudjuk, hogy tetszőleges $\alpha \in D^*$ elemre α konjugáltosztályának, $[\alpha]$-nak az elemszáma megegyezik α centralizátorának az elemszámával D^*-ben:

$$\big|[\alpha]\big| = \big|D^* : C_{D^*}(\alpha)\big|,$$

ahol $C_{D^*}(\alpha) = x \in D^* \big| x\alpha = \alpha x$. Könnyen látható, hogy $C_{D^*}(\alpha)$ is ferdetest (a 0-val kiegészítve), és így $\big|C_{D^*}(\alpha)\big| = q^d - 1$, ahol $d \mid n$. Így D^* elemszámára az alábbi összefüggést kapjuk (ezt nevezzük osztályegyenletnek):

$$\big|D^*\big| = q^n - 1 = q - 1 + \sum_d \frac{q^n - 1}{q^d - 1}$$

és itt a szummázás olyan d-kre történik, melyek osztói n-nek, de nem egyenlők vele. Az $x^n - 1 = \prod_{d|n} \Phi_d(x)$ összefüggésből látható, hogy $\Phi_n(x) \mid x^n - 1$, sőt $\Phi_n(x) \mid \frac{x^n-1}{x^d-1}$

minden $d \mid n$, $d \neq n$ esetén. Mivel ez az oszthatóság $\mathbb{Z}[x]$-ben is teljesül, ha x helyébe q-t helyettesítik, akkor $\mathbb{Z}$-beli oszthatóságot kapunk. Így: $\Phi_n(q) \mid q^n - 1$ és $\Phi_n(q) \mid \frac{q^n-1}{q^d-1}$ minden $d \mid n$, $d \neq n$ esetén. Ebből viszont az osztályegyenlet alapján azt kapjuk, hogy $\Phi_n(q) \mid q - 1$. Most megmutatjuk, hogy ez csak $n = 1$ esetén

lehetséges. $n > 1$ esetén ugyanis $\Phi_n(x)$ gyöktényezői között szerepel egy $(x - \varepsilon_0)$, ahol ε_0 az egységkörön van, és nem egyenlő 1-gyel. Ekkor:

$$\big|\Phi_n(q)\big| = \prod \big|(q - \varepsilon_i)\big| \geq \big|q - \varepsilon_0\big| > q - 1,$$

hiszen $\big|q - \varepsilon_i\big| \geq 1 \forall i$-re és $\big|q - \varepsilon_0\big| > (q-1)\varepsilon$ ugyanis messzebb van q-tól, mint az 1.

Hivatkozások

[1] Victor V. Prasolov: Polynomials

[2] Pantelis A. Damianou: On prime values of cyclotomic polynomials
https://arxiv.org/pdf/1101.1152.pdf

[3] http://oeis.org/A085398

[4] https://brilliant.org/wiki/cyclotomic-polynomials/

[5] R. Thangadurai: On the Coefficients of Cyclotomic Polynomials
https://www.bprim.org/sites/default/files/th.pdf

[6] http://en.wikipedia.org/wiki/bunyakovsky_conjecture

[7] http://faculty.bard.edu/~belk/math318/CyclotomicPolynomials.pdf

[8] Lawrence Sun: Cyclotomic polynomials ín Olympiad Number Theory

[9] Freud, Gyarmati: Számelmélet

[10] Kiss Emil: Bevezetés az algebrába Typotex Kiadó, 2007

[11] Gary Brookfield: The coefficients of cyclotomic polynomials
https://pdfs.semanticscholar.org/f354/8fbdeb5405066759e39d3eb9c978b571aebf.pdf

[12] Brett Porter: Cyclotomic polynomials

[13] Jameson: The cyclotomic polynomials

[14] Keith Kearnes, Kiss Emil, Szendrei Ágnes: Gauss egészek és Dirichlet tétele

[15] Ágoston Tamás írása

[16] Robert Israel programja