Eötvös Loránd Tudományegyetem
Természettudományi Kar

Körosztási polinomok

Szakdolgozat

Készítette: Csomós Beatrix

Matematika BSc, matematikai elemző szakirány

Témavezető: Ágoston István

Egyetemi docens

Algebra és Számelmélet Tanszék

Budapest

2014

Tartalomjegyzék

Köszönetnyilvánítás

Hálás köszönetemet szeretném kifejezni témavezetőmnek, Ágoston Istvánnak, aki hasznos tanácsaival, észrevételeivel nagyban hozzájárult szakdolgozatom elkészüléséhez. Továbbá köszönettel tartozom az eddigi matematika tanáraimnak is, akik megmutatták ennek a tudománynak a szépségeit, segítettek az egyetemi évek alatt. Köszönetet szeretnék továbbá mondani a családomnak, akik támogatása és olykor fejmosása nélkül nem sikerült volna eljutnom idáig. A kollégáimnak is hálás köszönet jár a rengeteg türelemért, illetve bíztatásért. Köszönet jár még évfolyamtársaimnak, akikkel egymást támogatva jutottunk el a szakdolgozat megírásáig. Végül és nem utolsó sorban szeretnék köszönetet mondani vőlegényemnek, Reinhardt Norbertnek, hogy minden örömömben és nehézségemben osztozott velem, támogatott és hitt bennem. Köszönöm mindenkinek!

1. fejezet

Bevezetés

Tanulmányaim során sokan kérdezték meg, miért éppen matematika? Ilyen helyzetben kissé büszkén kezdek mesélni a szépségeiről, amit magaménak tudhatok, hátha őket is magával ragadja ez a fantasztikus tudomány. A legtöbb esetben ez nem így történik, inkább megcsóválják a fejüket, és hol tisztelettel nézve rám, hol bolondnak tartva tovább folytatják megszokott életüket. Írásommal szeretném megmutatni, hogy valóban komolyan gondoltam minden mondatomat, valóban szeretem és látom a szépséget benne. Remélem pár matematikával nem foglalkozó embernek tudom bebizonyítani, hogy érdemes matematikát olvasni, tanulmányozni.

Szakdolgozatom célja, az algebra egyik számomra érdekes témájának, a körosztási polinomoknak a bemutatása. A dolgozat első fejezetében ismertetem az általános definícióját, előállítását illetve tulajdonságait. Mivel az egyetemi tanulmányok során ezeket algebrából mindenki megismeri, így inkább pár érdekességet szeretnék megmutatni ebben a részben. A következő fejezetben a körosztási polinomok irreducibilitását fogom vizsgálni, míg végül az utolsóban néhány példán, tételen keresztül szeretném megmutatni főként a számelmélettel való kapcsolatát, de szót ejtünk a sokszögek szerkeszthetőségéről is.

2. fejezet

Körosztási polinomokról általánosan

Ebben a részben megismerkedünk a körosztási polinomok általános definíciójával, néhány tulajdonságával. Megmutatjuk a körosztási polinomok közti összefüggések segítségével hogyan tudjuk egyszerűbben megadni őket.

2.1. Alapismeretek

Először is szükségünk van egy másik fontos definícióra, hogy értelmezni tudjuk az általános definíciót a körosztási polinomokra.

2.1.1. Definíció: Az *n-edik komplex egységgyökök* azok a z komplex számok, melyekre igaz, hogy $z^n = 1$, ahol $n = 1, 2, 3 \ldots$ pozitív egész szám. Egy n-edik egységgyököt *primitív n-edik egységgyöknek* nevezzük, ha semelyik $k < n$, $k = 1, 2, \ldots, n-1$ pozitív egész szám esetén nem k-adik egységgyök.

Könnyű belátni, hogy egy n-edik egységgyök pontosan akkor primitív, ha a hatványai az összes n-edik egységgyököt kiadják. Még a rend definícióját is megadjuk, mielőtt rátérünk a körosztási polinomokra.

2.1.2. Definíció: Egy $z \in \mathbb{C}$ rendje, $o(z)$ az a legkisebb pozitív n, melyre $z^n = 1$. (Ha ilyen nincs, akkor $o(z) = \infty$. Ez azt is jelenti, hogy $z \in \mathbb{C}$ pontosan akkor primitív n-edik egységgyök, ha $o(z) = n$.

Ezután már könnyen definiálni tudjuk az n-edik körosztási polinomot.

2.1.3. Definíció: Ha $n \geq 1$ akkor, Φ_n jelölje az *n-edik körosztási polinomot*, vagyis azt a normált polinomot, melynek gyökei pontosan a primitív n-edik egységgyökök (mindegyik egyszeres). Képletben:

$$\Phi_n(x) = (x - \xi_1) \cdots (x - \xi_{\varphi(n)}),$$

ahol $\xi_1, \ldots, \xi_{\varphi(n)}$ az összes primitív n-edik egységgyök, vagyis az összes olyan komplex szám, melynek rendje n.

A definícióból könnyen látható, hogy Φ_n foka $\varphi(n)$, ahol $\varphi(n)$ az ismert Euler-féle φ függvény. Azt, hogy a primitív n-edik egységgyökök száma miért $\varphi(n)$, azt a következő tételből láthatjuk.

2.1.4. Tétel: A primitív n-edik egységgyökök pontosan az

$$\eta = \cos(2k\pi/n) + i \sin(2k\pi/n)$$

alakú számok, ahol k és n relatív prímek és $0 < k \leq n$. Így a primitív n-edik egységgyökök száma $\varphi(n)$.

2.2. Kiszámítása a gyakorlatban

Most nézzük meg a kiszámítását gyakorlatban:

Kis n számok esetén még közvetlenül kiszámolhatjuk definícióból a körosztási polinomokat. Az első 2 polinom nyílván:

$$\Phi_1(x) = x - 1 \text{ és } \Phi_2(x) = x - (-1) = x + 1$$

Viszont nagyobb n-ekre már a $\sin(2\pi/n)$ és a $\cos(2\pi/n)$ értékét is csak nehezen, közelítőleg tudjuk megadni, az összeszorzás pedig végleg megnehezíti a dolgot. Ennek könnyítése érdekében megmutatjuk, hogy ezek a polinomok rekurzívan is megadhatóak. Ehhez először szükségünk van néhány összefüggés, következmény ismertetésére.

2.2.1. Lemma: Ha $n \geq 1$, akkor $\prod_{d|n} \Phi_d(x) = x^n - 1$.

Bizonyítás: Legyen $\eta = \cos(2\pi/n) + i\sin(2\pi/n)$. Könnyen látható, hogy η primitív n-edik egységgyök, ezért ennek hatványai az n-edik egységgyököket adják meg. Ezek éppen az $x^n - 1$ gyökei, és mivel n különböző számról van szó, így egyszerűen fel tudjuk írni $x^n - 1$ gyöktényezős alakját.

$$x^n - 1 = (x - \eta)(x - \eta^2) \cdots (x - \eta^n)$$

A gyöktényezőket csoportosítjuk a megfelelő egységgyökök rendje szerint. Jelölje f_d a d rendű egységgyökökhöz tartozó gyöktényezők szorzatát. Így megkapjuk a következő egyenletet:

$$x^n - 1 = \prod_d f_d(x).$$

Ebből következik, hogy elég azt belátni, hogy az itt szereplő d számok pontosan n osztói, és hogy ezekre $f_d = \Phi_d$. Ha egy d szám szerepel, vagyis ha $d = o(\eta^m)$ teljesül valamelyik m-re, akkor $(\eta^m)^n = (\eta^n)^m = 1^m = 1$ miatt n jó kitevője η^m-nek, és így $d|n$. Ebből következik, hogy ezek a d számok tényleg csak n osztói lehetnek.

Tegyük fel, hogy $d|n$. Ekkor Φ_d gyöktényezős felbontásában az összes d rendű koplex szám szerepel, f_d felbontásában pedig az összes olyan d-ed rendű komplex számok szerepelnek, amelyek egyben n-edik egységgyökök is (mindegyik egyszeres). De ezek ugyanazok a számok, hiszen ha egy ξ számra $d = o(\xi)|n$, akkor $\xi = 1$, ezért ξ egy n-edik egységgyök. Ezzel beláttuk, hogy az $f_d = \Phi_d$. $\square$

(Forrás: Kiss Emil: Bevezetés az algebrába)

Most lássuk, ennek egy következményét.

2.2.2. Következmény: Ha $n \geq 1$, akkor a $\Phi_n(x)$ körosztási polinom egész együtthatós.

Bizonyítás: Ezt a következményt indirekt bizonyítjuk. Tegyük fel, hogy ez az állítás nem igaz, és vegyünk egy n legkisebb pozitív egészet, melyre $\Phi_n(x)$ nem egész együtthatós. A (2.2.1) lemma miatt

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

Az n minimalitása miatt a nevezőben csak egész együtthatós polinomok vannak, amik normáltak is. Ezért a nevező maga is egész együtthatós és normált is. Minden olyan polinommal lehet maradékosan osztani, melynek főegyütthatója invertálható. Ezért a számláló maradékosan eloszthető a nevezővel $\mathbb{Z}[x]$-ben. A maradékos osztás egyértelműsége miatt a hányados és a maradék ugyanaz, mintha az osztást $\mathbb{C}$ felett végeznénk el. De $\mathbb{C}$ felett pontosan tudjuk, hogy a hányados a $\Phi_n(x)$, a maradék pedig nulla. Tehát $\mathbb{Z}$ felett is $\Phi_n(x)$ a hányados, vagyis $\Phi_n(x)$ egész együtthatós, ami ellentmond a feltevésünknek, tehát az állítás igaz. □

(Forrás: Kiss Emil: Bevezetés az algebrába)

Ezek ismeretében könnyen meghatározhatjuk az első pár körosztási polinomot:

$\Phi_1(x)$-et és $\Phi_2(x)$-et már láttuk az előbb, most számoljuk ki a következő 10 körosztási polinomot a felső lemma segítségével.

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

$$\Phi_4(x) = \frac{x^3 - 1}{\Phi_1(x)\Phi_2(x)} = \frac{x^4 - 1}{x^2 - 1} = x^2 + 1$$

$$\Phi_5(x) = \frac{x^5 - 1}{\Phi_1(x)} = \frac{x^5 - 1}{x - 1} = x^4 + x^3 + x^2 + x + 1$$

$$\Phi_6(x) = \frac{x^6-1}{\Phi_1(x)\Phi_3(x)\Phi_2(x)} = \frac{x^6-1}{(x^3-1)(x+1)} = \frac{x^3+1}{x+1} = x^2-x+1$$

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

$$\Phi_8(x) = \frac{x^8-1}{\Phi_1(x)\Phi_2(x)\Phi_4(x)} = \frac{x^8-1}{(x^4-1)} = x^4+1$$

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

$$\Phi_{10}(x) = \frac{x^{10}-1}{\Phi_1(x)\Phi_2(x)\Phi_5(x)} = \frac{x^{10}-1}{(x^5-1)\Phi_2(x)} = \frac{x^5+1}{\Phi_2(x)} = x^4-x^3+x^2-x+1$$

$$\Phi_{11}(x) = \frac{x^{11}-1}{\Phi_1(x)} = x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1$$

$$\Phi_{12}(x) = \frac{x^{12}-1}{\Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_4(x)\Phi_6(x)} = \frac{x^{12}-1}{(x^6-1)\Phi_4(x)} = \frac{x^6+1}{x^2+1} = x^4-x^2+1$$

Egy idő után ezek a számolások is bonyolultá válnak, de a további redukciós képletekkel, amikkel megismerkedünk, sokat könnyíthetünk a helyzetünkön.

2.2.3. Tétel: Minden p prímre, $\Phi_p(x) = x^{p-1} + \cdots + 1$.

Ezt nem bizonyítjuk, hiszen ez egyszerű számolással adódik a a (2.2.1) lemmából. Most nézzünk két bonyolultabb képletet, de ezek bizonyításához szükségünk van előbb a Möbius-függvény definíciójára.

2.2.4. Definíció: Möbius-függvényt jelölje $\mu(n)$, amit az alábbiak szerint definiálunk.

$$\mu(n) = \begin{cases} 1 & \text{ha } n = 1 \\ (-1)^k & \text{ha } n = p_1 p_2 \dots p_k, \text{ ahol } p_i\text{-k különböző prímek} \\ 0 & \text{különben} \end{cases}$$

2.2.5. Lemma: Ha $\mu(n)$ jelöli a Möbius-függvényt, akkor

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

Ezt nem bizonyítjuk, de a bizonyítás megtalálható a R.Thangadurai: On the coefficients of cyclotomic polynomials című írásban.

2.2.6. Tétel: Ha n páratlan, akkor $\Phi_{2n}(x) = \Phi_n(-x)$

Bizonyítás:

$$\begin{aligned} \Phi_{2n}(x) &= \prod_{d|(2n)} (x^d - 1)^{\mu(\frac{2n}{d})} \\ &= \prod_{2|d, d|2n} (x^d - 1)^{\mu(\frac{2n}{d})} \prod_{d|n} (x^d - 1)^{\mu(\frac{2n}{d})} \\ &= \prod_{d|n} [(x^d - 1)^{\mu(\frac{2n}{d})} (x^{2d} - 1)^{\mu(\frac{n}{d})}] \\ &= \prod_{d|n} [(x^d - 1)^{\mu(\frac{2n}{d})} (x^d - 1)^{\mu(\frac{n}{d})} (x^d + 1)^{\mu(\frac{n}{d})}] \\ &= \prod_{d|n} (x^d + 1)^{\mu(\frac{n}{d})}, \text{mivel } \mu(2k) = -\mu(k) \text{ páratlan k esetén} \\ &= \prod_{d|n} (-x^d - 1)^{\mu(\frac{n}{d})} = \Phi_n(-x), \text{mivel } \mu\left(\frac{n}{d}\right) \text{ csak páros sok } d\text{-re nem 0.} \end{aligned}$$

□

2.2.7. Tétel: Legyen $m|n$ pozitív egészek úgy, hogy n minden prím osztója osztja m-et is. Ekkor $\Phi_n(x) = \Phi_m(x^{\frac{n}{m}})$.

Bizonyítás: Tudjuk, hogy $\mu(k) = 0$ minden k egészre, melyek nem négyzetmentesek, ekkor

$$\begin{aligned}\Phi_n(x) &= \prod_{d|n}(x^{\frac{n}{d}} - 1)^{\mu(d)} = \prod_{d|n, d|m}(x^{\frac{n}{d}} - 1)^{\mu(d)} \\ &= \prod_{d|m}((x^{\frac{n}{m}})^{\frac{m}{d}} - 1)^{\mu(d)} = \Phi_m(x^{\frac{n}{m}}).\end{aligned}$$

□

Most lássunk egy-egy példát ezek használatáról:

1. **példa:** $\Phi_{14}(x)$-et számoljuk ki a fenti tétel segítségével.
$\Phi_{14}(x) = \Phi_7(-x) = x^6 - x^5 + x^4 - x^3 + x^2 - x + 1$

2. **példa:** $\Phi_{36}(x)$-et számoljuk ki a fenti módszer segítségével. $36 = 2^2 \cdot 3^2$, a fenti tétel miatt nekünk a két prímosztó szorzatát kell nézni, ami 6. Így ebből következik, hogy $\Phi_{36} = \Phi_6(x^6) = x^{12} - x^6 + 1$

A (2.2.6) és a (2.2.7) tételekből következik, hogy igazából nekünk elegendő kiszámolni az összes páratlan, négyeztmentes indexű körosztási polinomot, melyekből könnyen adódik az összes többi. Nézzük meg az elő 100 körosztási polinom közül, melyek azok, amiket feltétlenül meg kell adnunk.

A piros számok jelölik azokat az indexeket amik párosak, őket a fenti tételből ki tudjuk számítani. A kék számok jelölök a prím indexűeket, kivétel a (2-t). A zöld számok jelölik a nem négyzetmentes indexűeket.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

A felsorolásból jól látható, hogy csak a a feketén hagyott indexűeket kell kiszámítanunk, a (2.2.1) lemmma alapján, a többit a tételek segítségével gyorsan, egyszerűen megadhatjuk.

Ezek közül az első négyet meg is mutatjuk, de már ezeknek a kiszámítása is hosszú, bonyolult.

$$\Phi_{15}(x) = \frac{x^{15}-1}{\Phi_1(x)\Phi_3(x)\Phi_5(x)} = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$$

$$\Phi_{21}(x) = \frac{x^{21}-1}{\Phi_1(x)\Phi_3(x)\Phi_7(x)} = x^{12} - x^{11} + x^9 - x^8 + x^6 - x^4 + x^3 - x + 1$$

$$\begin{aligned}\Phi_{33}(x) = \frac{x^{33}-1}{\Phi_1(x)\Phi_3(x)\Phi_{11}(x)} &= x^{20} - x^{19} + x^{17} - x^{16} + 14 - x^{13} + x^{11} - \\ &\quad -x^{10} + x^9 - x^7 + x^6 - x^4 + x^3 - x + 1\end{aligned}$$

$$\begin{aligned}\Phi_{35}(x) = \frac{x^{35}-1}{\Phi_1(x)\Phi_5(x)\Phi_7(x)} &= x^{24} - x^{23} + x^{19} - x^{18} + x^{17} - x^{16} + x^{14} - \\ &\quad -x^{13} + x^{12} - x^{11} + x^{10} - x^8 + x^7 - \\ &\quad -x^6 + x^5 - x + 1\end{aligned}$$

2.3. Körosztási polinomok együtthatói

Könnyen gondolhatnánk az előzőek alapján, hogy az együtthatók csak a $\{0, 1, -1\}$ halmazból kerülnek ki, de ez nem igaz, hiszen a $\Phi_{105}(x)$-ben a 41-ed és 7-edfokú tag együtthatója -2. Ez a legkisebb fokú ellenpélda.

$$\begin{aligned}\Phi_{105}(x) &= x^{48} - x^{47} + x^{46} - x^{43} - 2x^{41} - x^{40} - x^{39} + x^{36} + \\ &\quad +x^{35} + x^{34} + x^{33} + x^{32} + x^{31} - x^{28} - x^{26} - x^{24} - \\ &\quad -x^{22} - x^{20} + x^{17} + x^{16} + x^{15} + x^{14} + x^{13} + x^{12} - \\ &\quad -x^9 - x^8 - 2x^7 - x^6 - x^5 + x^2 + x + 1\end{aligned}$$

Suzuki J. tételével pedig belátjuk, hogy ez nem kivétel, hiszen bármelyik egész szám lehet együttható.

2.3.1. Tétel: Bármelyik egész szám lehet a körosztási polinom együtthatója.

Bizonyítás: Ennek a bizonyításához felhasználjuk az alábbi lemmát.

2.3.2. Lemma: Bármely $t \geq 3$ pozitív egész számhoz léteznek olyan $p_1 < p_2 < \cdots < p_t$ prímek, melyekre teljesül, hogy $p_1 + p_2 > p_t$.

Bizonyítás: Rögzítsük $t \geq 3$-at. Indirekt módon tegyük fel, hogy tetszőleges $p_1 < p_2 < \cdots < p_t$-re teljesül a következő egyenlőtlenség, $p_1 + p_2 \leq p_t$. Ebben az esetben $2p_1 < p_t$ illetve 2^{k-1} és 2^k között kevesebb mint t prím van. Ez azt jelenti, hogy $\pi(2^k) < kt$, ahol a $\pi(s)$ az 1 és s közé eső prímek számát jelöli. Csebisev tétele miatt tudjuk, hogy $\pi(x) > \frac{cx}{\ln x}$, ahol c pozitív konstans. Ezért

$$\frac{c \cdot 2^k}{\ln 2^k} < kt \text{ azaz } c \cdot 2^k < k^2 \cdot t \cdot \ln 2 \text{ azaz } \frac{2^k}{k^2} < \frac{1}{c} \cdot t \cdot \ln 2.$$

Elég nagy k esetén ez az egyenlőtlenség sérül, hiszen

$$\frac{2^k}{k^2} \to \infty, \text{ ha } k \to \infty.$$

Ezzel a lemmát beláttuk. □

Legyen most $t \geq 3$ egy páratlan egész szám. Válasszuk úgy a prímeket, hogy $p_1 < p_2 < \cdots < p_t$, amire $p_1 + p_2 > p_t$. Legyen $p = p_t$, és vegyük a $\Phi_n(x)$ polinomot modulo x^{p+1}. Legyen t páratlan, ekkor az alábbi egyenletet kapjuk a (2.2.5) tétel miatt:

$$\Phi_{p_1 \cdots p_t}(x) = \frac{(x^{p_1} - 1) \cdots (x^{p_t} - 1)}{x - 1} \cdot \frac{\prod (x^{p_i p_j p_k} - 1)}{\prod (x^{p_i p_j} - 1)} \cdots$$

De $x^{p_i p_j} \equiv 0 \pmod{x^{p+1}}$, $x^{p_i p_j p_k} \equiv 0 \pmod{x^{p+1}}$ és így tovább. Ezért

$$\Phi_{p_1 \cdots p_t}(x) \equiv \pm \frac{(1 - x^{p_1}) \cdots (1 - x^{p_t})}{1 - x} \pmod{x^{p+1}}.$$

Itt a plusz előjelűt kell választanunk, mivel meggondolható, hogy $\Phi_{p_1 \dots p_t}(0) = 1$. A

$$p_i + p_j \geq p_1 + p_2 > p_t = p$$

egyenlőtlenség azt jelenti, hogy

$$(1 - x^{p_1}) \cdots (1 - x^{p_t}) \equiv (1 - x^{p_1} - \cdots - x^{p_t}) \pmod{x^{p+1}}.$$

Azt is tudjuk, hogy $(1 - x)^{-1} \equiv (1 + x + \cdots + x^p) \pmod{x^{p+1}}$. Ezért

$$\Phi_{p_1 \dots p_t}(x) \equiv (1 - x^{p_1} - \cdots - x^{p_t})(1 + x + \cdots + x^p) \pmod{x^{p+1}}.$$

Az $x^{p_i}, x^{p_i+1}, \dots, x^{p_i+p}$ tagok közül, a $x^p = x^{p_t}$ előfordul minden i-re, míg az x^{p-1}, x^{p-2} tagok megtalálhatóak minden $i \neq t$-re. Ezért az együtthatója x^p-nek $\Phi_{p_1 \dots p_t}$-ben $(-t + 1)$, x^{p-2}-é pedig $-(t - 1) + 1 = -t + 2$.

Ha most t végigfut az 1-nél nagyobb páratlan számokon, akkor $-t + 1$ és $-t + 2$ a (-1)-nél kisebb negatív egészeken. Azt, hogy 1-nél nagyobb pozitív együtthatókat is megkapjuk, az alábbi módon bizonyítjuk. Tekintsük a $\Phi_{2p_1 \cdots p_t}(x)$-t $t > 3$ páratlan t-re és $3 \leq p_1 \leq p_2 \cdots < p_t$-re, melyekre $p_1 + p_2 > p_t$. Mivel $p_1 \cdots p_t$ páratlan ezért a $\Phi_{2p_1 \cdots p_t}(x) = \Phi_{p_1 \cdots p_t}(-x)$. Mivel p_t páratlan, ezért $\Phi_{2p_1 \cdots p_t}(x)$-ben a$p_t$-edfokú tag együtthatója most $t - 1$ a $(p_t - 2)$-edfokú tagé pedig $t - 2$ lesz. Ezzel a tételt beláttuk. □

(Forrás: V.V Prasolov: Polynomials)

3. fejezet

Körosztási polinomok irreducibilitása

Az, hogy $\Phi_n(x)$ minden pozitív egészre irreducibilis $\mathbb{Q}[x]$-ben (illetve $\mathbb{Z}[x]$-ben), alapvető eredénynek számít a számelméletben. Ebben a fejezetben szeretnénk megismerkedni néhány klasszikus bizonyítással (természetesen a teljesség igénye nélkül). Az első bizonyítást Gauss adta arra, hogy ha p egy prím akkor a $\Phi_p(x)$ körosztási polinom irreducibilis. Kroncker ugyanezt az állítást egyszerűbben bizonyította, majd egy ennél sokkal általánosabb bizonyítást Schönemann és Eisenstein is megmutatott. Azt, hogy az állítást nem csak p prímekre igaz, hanem minden pozitív egészre, többen is megadták. Ezek közül egyet meg is mutatunk.

3.1. Φ_n irreducibilitása p prím esetén

3.1.1. Tétel: Adott p prím. Ekkor a $\Phi_p(x)$ körosztási polinom irreducibilis.

A Kronecker-féle bizonyítást nézzük meg először, de ehhez azonban szükségünk van egy lemmára:

3.1.2. Lemma: Legyen $f(x)$ egy tetszőleges egész együtthatós polinom, ξ pedig p-edik primitív egységgyök. Ekkor $f(\xi)\cdots f(\xi^{p-1})$ és $f(1)$ egészek és

$$f(\xi)\cdots\ f(\xi^{p-1}) \equiv f(1)^{p-1} \pmod{p}.$$

Bizonyítás: Annak a bizonyításánál, hogy $f(\xi)\cdots f(\xi^{p-1})$ egész, figyelembe kell venni, hogy ez egy szimmetrikus polinom $\xi,\ldots,\xi^{p-1}$ számokban, és így a szimmetrikus polinomok alaptétele miatt felírható a $\xi,\ldots\xi^{p-1}$ elemi szimmetrikus kifejezéseik egész együtthatós polinomjaik. De ezek az elemi szimmetrikus kifejezések épp a $\Phi_p = 1+\cdots+x^{p-1}$ együtthatói. Így $f(\xi)\cdots f(\xi^{p-1})$ valóban egészek. Most már csak azt kell bizonyítani, hogy a kongruencia teljesül. Legyen

$$g(x) = f(x)\cdots f(x^{p-1}) = \sum_n A_n x^n$$

és tekintsük a

$$\sum_{i=0}^{p-1} g(\xi^i)$$

kifejezést. A $g(x)$ polinom első felírásából

$$f(1)^{p-1} + (p-1)f(\xi)\cdots f(\xi^{p-1})$$

adódik, míg a második kifejezésből

$$\sum_{p|n} A_n p$$

adódik. Így

$$f(1)^{p-1} + (p-1)f(\xi)\cdots f(\xi^{p-1}) \equiv 0 \pmod{p}.$$

Ezzel így a lemmát beláttuk. □

Most már rátérhetünk a tétel bizonyítására.

Bizonyítás: Tegyük fel, hogy $\Phi_p(x)$ nem irreducibilis és írjuk fel az alábbi módon: $\Phi_p(x) = f(x)g(x)$, ahol egyik sem konstans polinom. A Gauss-lemma alapján feltehető az, hogy $f(x)$ és $g(x)$ polinomok egész együtthatósak. Ekkor $p = \Phi_p(1) = f(1)g(1)$. Ebből következik, hogy az egyik tényezőnek ± 1-nek

kell lennie. Tegyük fel, hogy $f(x) = \pm 1$. Egyrészt $f(\xi^k) = 0$, $k \neq 0$-ra (mod p) (mivel ezek gyökei a $\Phi_p(x)$-nek), így $f(\xi) \dots f(\xi^{p-1}) = 0$, másrészt viszont $f(1)^{p-1} \equiv 1$ (mod p), ami ellentmond a fenti kongruenciának. □

Egy másik és talán egyszerűbb bizonyítás Schönemanntól származik. Ez pedig így hangzik.

Bizonyítás: A következő kritériumunk van az irreducibilitásra: Adott $f(x)$ egy k-ad fokú egész együtthatós polinom. Tegyük fel, hogy p egy prím, a pedig egy egész szám. Ekkor legyen $f(x) = (x-a)^k + pg(x)$, $g(x)$ egész együtthatós polinom illetve p nem osztja $g(a)$-t. Ekkor az $f(x)$ irreducibilis. A binomiális tétel miatt, $x^p - 1 \equiv (x-1)^p$ (mod p), így

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} \equiv (x-1)^{p-1} \text{ (mod } p),$$

továbbá $\Phi_p(x) = x^{p-1} + \dots + 1$ így $\Phi_p(1) = p$. Így $\Phi_p(x)$ kielégíti a fenti kritériumot. □

Eisenstein is bizonyította a fenti tételt, az alábbi módon.

Bizonyítás: Itt is megfogalmazunk egy általános irreducibilitási kritériumot. (Ezt ismerjük manapság Schönemann-Eisenstein kritériumnak.) Adott $f(x) = c_k x^k + \dots + c_0$ egész együtthatós polinom. Tegyük fel, hogy p prím, p nem osztója c_k-nak, de osztja a $c_{k-1}, \dots, c_0$ együtthatókat, p^2 nem osztja c_0-t. Ekkor $f(x)$ irreducibilis. $\Phi_p(x)$ akkor és csak akkor irreducibilis, ha $\Phi_p(x+1)$ irreducibilis. De a binomiális tétel miatt:

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

ahol p osztója az $\binom{p}{i}$ együtthatóknak. Ez pedig kielégíti a fenti kritériumot. □

(Források a bizonyításokhoz: Steven H. Weintraub: Several proofs of the irreducibility of the cyclotomic polynomials)

Schönemann kritériuma és bizonyítása kissé feledésbe merült az elmúlt években, Eisensteiné viszont a mai napig jól ismert és tanított. A két bizonyítás a látszat ellenére ekvivalens egymással.

3.2. Az általános eset

Most térjünk át az "általános" körosztási polinomok irreducibilitására.

3.2.1. Tétel: Legyen n egy tetszőleges pozitív egész szám. Ekkor a $\Phi_n(x)$ körosztási polinom irreducibilis $\mathbb{Z}$ és $\mathbb{Q}$ felett.

Mielőtt ezt a tételt bizonyítjuk, szükségünk van egy másik tételre, amely így hangzik.

3.2.2. Tétel: Egy egész együtthatós polinom akkor és csak akkor irreducibilis $\mathbb{Z}$ felett ha

(1) vagy egy $\mathbb{Z}$-beli prímszám,

(2) vagy egy primitív polinom, amelyik $\mathbb{Q}$ felett irreducibilis.

Bizonyítás: A $\mathbb{Z}$-beli irreducibilis számokról tudjuk, hogy mint konstans polinomok szintén irreducibilisek. Tételezzük fel, hogy f nem konstans primitív polinom, amely $\mathbb{Q}$ felett is felbonthatatlan. Ha $f = gh$ egy felbontás, ahol g és $h \in \mathbb{Z}[x]$, akkor $\mathbb{Q}$ feletti felbonhatatlansága miatt vagy g vagy h egység $\mathbb{Q}$-ban, vagyis konstans. Mivel g és h egész együtthatós, így egész szám is. Mivel f primitív, ez az egész szám csak egység lehet, és így az $f = gh$ felbontás $\mathbb{Z}[x]$-ben is triviális. Tehát f irreducibilis $\mathbb{Z}$ felett. Megfordítva, tételezzük fel, hogy f irreducibilis $\mathbb{Z}[x]$-ben. Ekkor f felírható nk alakban, ahol n egész szám és k primitív polinom. Mivel f felbonthatatlan, ez a felbontás triviális. Így vagy n egység, vagy k egység. Ha f konstans, akkor felbonthatatlannak kell lennie $\mathbb{Z}$-ben, hiszen $\mathbb{Z}$-beli felbontások egyben $\mathbb{Z}[x]$-beli nemtriviális felbontások is. Ha f nem konstans primitív polinom, akkor azt kell bizonyítanunk, hogy nem csak $\mathbb{Z}$, hanem $\mathbb{Q}$ felett is irreducibilis. Tegyük fel, hogy f előáll nála alacsonyabb fokú racionális együtthatós g és h polinomok szorzataként. Ekkor f felírható g_0h_0 alakban is, ahol ezek egész együtthatós polinomok, és g_0 foka megyegyezik a g fokával, h_0 foka pedig h

fokával. Ebből következik, hogy egyik sem konstans, és így ez nemtriviális felbontás $\mathbb{Z}$-ben is, ami ellentmond f irreducibilitásának $\mathbb{Z}$ felett. $\square$

(Forrás: Kiss Emil: Bevezetés az algebrába)

Most rátérhetünk a (3.2.1) tétel bizonyítására.

Bizonyítás: A (3.2.2) tétel miatt a Φ_n körosztási polinom ugyanakkor felbonthatatlan $\mathbb{Z}$ és $\mathbb{Q}$ felett, hiszen primitív, és nem konstans. Bontsuk fel $\mathbb{Z}$ felett irreducibilisek szorzatára: $\Phi_n(x) = f_1(x) \dots f_s(x)$. Az f_i tényezők főegyüttható csak ± 1 lehet, tehát egyik sem konstans. Így mindegyik f_i irreducibilis $\mathbb{Q}[x]$ felett is. Azt kell bizonyítanunk, hogy ebben a felbontásban csak egy tényező szerepel. Ebben a következő lemma lesz a segítségünkre.

3.2.3. Lemma: Legyen p prím mely nem osztója n-nek. Ha egy ε számra $f_1(\varepsilon) = 0$, akkor $f_1(\varepsilon^p) = 0$.

A lemmából már következni fog a tétel is a következők miatt. Mivel f_1 legalább elsőfokú, van egy $\varepsilon \in \mathbb{C}$ gyöke, ami Φ_n-nek is gyöke, tehát egy primitív n-edik egységgyök. Ebből következik, hogy az összes n-edik primitív egységgyök hatványa ε-nak a (2.1.4) tétel miatt (méghozzá n-hez relatív prím kitevőjű hatványa). Legyen ε^m egy ilyen szám, ahol m és n realítv prímek. Az m febontható prímek szorzatára a következő módon: $m = p_1 \dots p_k$ ahol egyik tényező sem osztója n-nek. A lemma miatt ε^{p_1} gyöke f_1-nek. Ha alkalmazzuk a lemmát ε^{p_1}-re és p_2 prímszámra, azt kapjuk, hogy $\varepsilon^{p_1 p_2}$ is gyöke f_1-nek. Ha a lemmát még $k-2$-szer alkalmazzuk, akkor nyílvánvaló, hogy $\varepsilon^{p_1 \dots p_k} = \varepsilon^m$ is gyöke f_1-nek. Ebből azt kapjuk, hogy f_1-nek gyöke az összes primitív n-edik egységgyök, és így Φ_n összes gyöktényezője szerepel f_1-ben, így f_1 az egyetlen tényezője Φ_n-nek.

Így már csak a lemmát kell belátni, hogy a tétel valóban igaz legyen.

Bizonyítás: Tegyük fel, hogy $f_1(\varepsilon) = 0$, de $f_1(\varepsilon^p) \neq 0$. Mivel $p \nmid n$, az ε^p is primitív n-edik egységgyök, így gyöke Φ_n-nek. Emiatt ε^p gyöke valamelyik f_j polinomnak, ahol $j \neq 1$. Tegyük fel, hogy $j = 2$, amiből következik, hogy $f_2(\varepsilon^p) = 0$. Vizsgáljuk az $f_1(x)$ és az $f_2(x^p)$ polinomok kitüntetett közös

osztóját. Ugyanazt a racionális együtthatós f polinomot kapjuk, ha $\mathbb{Q}$ és $\mathbb{Z}$ felett számítjuk ki. Az f polinom nem konstans, mivel a két polinomnak ε a közös gyöke. Ezért $f|f_1$ és f_1 felbonthatatlanságából következik, hogy f az f_1 polinomnak nem nulla racionális konstansszorosa. Mivel $f(x)|f_2(x^p)$, ezért $f_1(x)$ osztója az $f_2(x^p)$ polinomnak $\mathbb{Q}[x]$-ben, de akkor osztója $\mathbb{Z}[x]$-ben is, hiszen ± 1 az f_1 főegyütthatója, és amikor a $g(x) = \frac{f_2(x^p)}{f_1(x)}$ osztást elvégezzük, végig $\mathbb{Z}[x]$-ben maradunk. Tekintsük a fent szereplő polinomok együtthatóit modulo p, és jelölje felülvonás az így kapott polinomokat. Ekkor azt kapjuk, hogy $\overline{f_1}(x)\overline{g}(x) = \overline{f_2}(x^p)$. A $\mathbb{Z}_p[x]$-ben tagonként lehet p-edik hatványra emelni, illetve tudjuk, hogy $\overline{f_2}(x^p) = \overline{f_2}(x)^p$. Ebből következik, hogy $\mathbb{Z}_p$-ben $\overline{f_1}|\overline{f_2}^p$ teljesül. Mivel f_1 főegyütthatója ± 1 , az $\overline{f_1}$ polinom sem konstans. Ez a polinom $\mathbb{Z}_p$ felett nem biztos, hogy irreducibilis, de biztos, hogy van egy felbonthahatlan k osztója $\mathbb{Z}_p$ felett. Ekkor $k|\overline{f_1}|\overline{f_2}^p$, amiből azt kapjuk, hogy $k|\overline{f_2}$, hiszen prímtulajdonságúak az irreducibilis polinomok $\mathbb{Z}_p[x]$-ben. Ezekből következik, hogy létezik egy olyan $k \in \mathbb{Z}_p[x]$ nem konstans polinom, ami $\overline{f_1}$-nak és $\overline{f_2}$-nak is osztója. Ezért $k^2|\overline{f_1 f_2}$. Azt tudjuk, hogy $f_1 f_2|\Phi_n$ és $\Phi_n|x^n - 1$. Ezért következik, hogy $k^2|\overline{x^n - 1}$. Viszont $p \nmid n$ esetén az $x^n - 1$ polinomnak nincs többszörös tényezője mod p. Ez viszont ellentmondás. $\square$

A lemma bebizonyításával a tételünket is beláttuk. $\square$

(Forrás: Kiss Emil: Bevezetés az algebrába)

4. fejezet

Körosztási polinomok alkalmazása

4.1. Prímszámok

Ebben a részben néhány számelmélettel kapcsolatos tételt, illetve pár feladatot mutatunk arra, mi mindenre használható a körosztási polinom.

Legelőször a speciális alakú prímszámok létezését vizsgáljuk a körosztási polinomok segítégével.

Először is azt fogjuk bebizonyítani, hogy van végtelen sok $4k+1$ alakú prímszám.

4.1.1. Tétel: Végtelen sok $4k+1$ alakú prímszám van.

Bizonyítás:

Ehhez előbb egy másik lemmát kell bizonyítanunk.

4.1.2. Lemma: Ha n egész, akkor n^2+1-nek nincs $4k-1$ alakú pozitív osztója.

Bizonyítás: Tegyük fel, hogy ez nem igaz, és legyen b a legkisebb $4k-1$ alakú pozitív osztója n^2+1-nek, valamely n egészre. Ekkor legyen $n = qb+r$, ahol

$0 \leq r < b$. Ilyenkor r^2+1 és $(r-b)^2+1$ mindkettő osztható b-vel. Legyen s az r és $r-b$ számok közül az, amelyik páros. Ekkor s^2+1 osztható b-vel, és $|s| \leq b$. Mivel itt $|s| = b$ nem lehet, ezért $s^2+1 \leq (b-1)^2+1 < b^2$. Legyen $t = (s^2+1)/b$, ekkor $t < b$ és t is osztja s^2+1-et, tehát b minimalitása miatt t nem lehet $4k-1$ alakú. Mivel t páratlan, ezért t csak $4k+1$ alakú lehet. Ezekből következik, hogy $t \cdot b$ 4-gyel osztva (-1) maradékot ad, viszont ez ellentmondás, hiszen $t \cdot b = s^2+1$ és s páros. Ezzel a lemmát beláttuk. □

Most térjünk vissza a tétel bizonyítására. A fentiekből jól látható, hogy ha n páros, akkor n^2+1 minden prímosztója $4k+1$ alakú. Tehát, ha $N \geq 2$, akkor $(N!)^2+1$ minden prímosztója $4k+1$ alakú, és mivel nagyobb N-nél ezzel beláttuk, hogy végtelen sok $4k+1$ alakú prímszám van. □

(Forrás: Új matematikai mozaik: Laczkovich Miklós írása)

A fentiekből észrevehető, hogy $x^2+1 = \Phi_4(x)$, tehát, ha a egy egész szám, akkor $\Phi_4(a)$ minden prím osztója vagy 2 vagy a fenti tétel miatt $4k+1$ alakú. A következőkben ennek az általánosítását fogjuk megmutatni, melyet Bauer Mihály bizonyított.

4.1.3. Tétel: Ha a egész szám, akkor $\Phi_n(a)$ minden prímosztója vagy osztója n-nek, vagy $nk+1$ alakú.

Bizonyítás: Legyen p egy prímosztója a $\Phi_n(a)$-nak. Az (2.2.1) lemma miatt $\Phi_n(a)|a^n-1$, ezért $p|a^n-1$, és ebből következik, hogy p nem osztója a-nak. Legyen d a legkisebb pozitív egész, amelyre a^d-1 osztható p-vel. Valójában $p|a^d-1$ alapján tudjuk, hogy $p|a^{d+1}-a, p|a^{d+2}-a^2 \ldots p|a^{d+i}-a^i$ minden i-re. Ebből következik, hogy a^m-1 akkor és csak akkor osztahtó p-vel, ha, ha m osztható d-vel. A kis Fermat-tétel miatt $p|a^{p-1}-1$ is igaz, tehát $d|n$ és $d|p-1$.

Vizsgáljuk először azt az esetet, amikor $d = n$. Akkor igaz, hogy $n|p-1$, amiből kapjuk, hogy $p = nk+1$, tehát a tétel egyik részét bizonyítottuk.

Nézzük, mi a helyzet azzal az esettel, ha $d < n$. Mivel $d|n$ és $d < n$, ezért a (2.2.1) lemmát alkalmazva n-re és d-re, megkapjuk azon Φ_m körosztási

polinomok szorzatát az

$$\frac{x^n-1}{x^d-1}$$

alakban, melyekre $m|n$, de $m \nmid d$. Ezek között ott van a $\Phi_n(x)$ polinom is, így $p|\Phi_n(a)$-ból következik, hogy

$$p\Big|\frac{x^n-1}{x^d-1}.$$

Viszont

$$\frac{a^n-1}{a^d-1} = 1+a^d+a^{2d}+\cdots+a^{n-d} = (a^d-1)+(a^{2d}-1)+\cdots+(a^{n-d}-1)+\frac{n}{d}$$

Mivel itt mindegyik $a^{id}-1$ alakú tag osztható p-vel, így ebből következik, hogy $p|\frac{n}{d}$-t is. Ezzel a tételt beláttuk. □

(Forrás: Új matematikai mozaik: Laczkovich Miklós írása)

Ezt a tételt egy példán keresztül szeretném szemléltetni.

3. példa: Tegyük fel, hogy faktorizálni szeretnénk a $k = 1000000001$ számot. Erről könnyen észrevehető, hogy ez a szám osztható 11-gyel, de az osztás elvégzése után kapott 90909091 szám további faktorizációja nem látszik annyira könnyűnek. Könnyebb a megoldása a feladatnak, ha arról az oldalról közelítjük meg, hogy $k = 10^9 + 1$ és előbb az $x^9 + 1$ polinomot faktorizáljuk.

$$x^9+1 = (x^3+1)(x^6-x^3+1) = (x+1)(x^2-x+1)(x^6-x^3+1),$$

amiből megkapjuk, hogy $k = 11\cdot91\cdot999001$. Ez még nem a teljes faktorizáció, de így visszavezettük egy 6 jegyű szám faktorizációjára. Ezt kiszámolni még mindig nagyon hosszadalmas, de ha észrevesszük, hogy $(x^6 - x^3 + 1) = \Phi_9(-x) = \Phi_{18}(x)$, akkor a fenti tételt alkalmazva látjuk, hogy k szám minden prímosztója vagy osztója 18-at vagy $18k + 1$ alakúak. Csak a $18k + 1$ alakú eset jöhetnek szóba, hiszen sem 2,és 3 nem osztója a k számnak. Így sokkal kevesebb prímszámot kell átvizsgálnunk. Tehát $k = 1000000001 = 11 \cdot 91 \cdot 999001 = 11 \cdot (7 \cdot 13) \cdot (19 \cdot 52579)$. A 19 illetve a 52579 valóban $18k + 1$ alakúak.

A Dirichlet nevezetes tétele azt mondja ki, hogy a számtani sorozatokban (triviális esetektől eltekintve) végtelen sok prím szerepel. Ennek egy speciális esete volt a $4k+1$ alakú prímekről szóló (4.1.1) tétel. Most általánosan azt mutatjuk meg, hogy tetszőleges m-re végtelen sok $mk+1$ alakú prím van. Mielőtt kimondjuk a tételt, szükségünk van a rend definíciójára.

4.1.4. Definíció: Legyen $(a,m)=1$. A k pozitív egészet az a rendjének nevezzük modulo m, ha $a^k \equiv 1 \pmod{m}$, de bármely $0 < i < k$ esetén $a^i \not\equiv 1 \pmod{m}$. Az a szám modulo m vett rendjét $o_m(a)$ jelöli.

4.1.5. Tétel: Bármely rögzített $m > 0$ esetén az $mk+1$, $k = 0,1,2,\ldots$ számok között végtelen sok prím található.

Bizonyítás: Ehhez előbb egy lemmát kell bizonyítani.

4.1.6. Lemma: Legyen c egy egész szám és q prímszám. Ekkor

$$o_q(c) = m \Longleftrightarrow q|\Phi_m(c) \text{ és } q \nmid m \tag{4.1}$$

Bizonyítás: Először az $\Rightarrow$ irányt bizonyítjuk:

Tegyük fel, hogy $o_q(c) = m$. Ekkor $m|q-1$ és így $q \nmid m$ is teljesül. Helyettesítsük a (2.2.1) lemma képletébe x helyére c-t. Akkor az alábbit kapjuk:

$$c^m - 1 = \prod_{d|m} \Phi_d(c) \tag{4.2}$$

Mivel $o_q(c) = m$, ezért $c^m \equiv 1 \pmod{q}$, és így a (4.1) bal oldala osztható q-val. Mivel q prím ezért jobb oldalon is valamelyik $\Phi_d(c)$ tényező is osztható q-val. Ekkor a $\Phi_d(c)|c^d - 1$ miatt $c^d \equiv 1 \pmod{q}$ valamelyik $d|m$-re. Mivel $o_q(c) = m$ ezért csak $d = m$ lehetséges, vagyis valóban $q|\Phi_m(c)$.

Nézzük most a $\Leftarrow$ irányt:

Ennél a $q|\Phi_m(c)$ és $q \nmid m$ feltételekből indulunk ki. Ekkor $\Phi_m(c)|c^m - 1$ miatt $c^m \equiv 1 \pmod{q}$. Tegyük fel indirekt, hogy $o_q(c) = t < m$. Ekkor $t|m$

és $c^t \equiv 1 \pmod{q}$. A (4.2) összefüggést m helyett t-re alkalmazva azt kapjuk, hogy van olyan $d|t$, amelyre $q|\Phi_d(c)$. Ez azt jelenti, hogy a (4.2) jobb oldalán legalább két tényező osztható q-val.

Tekintsük az $x^m - 1 = \prod_{d|m} \Phi_d$ egyenlőséget $\mathbb{Z}_q$ (modulo q test) felett. Ha ebben a helyzetben tekintjük az előző bekezdés utolsó mondatát, akkor azt kapjuk, hogy c mint $\mathbb{Z}_p$-beli elem, a $\prod_{d|m} \Phi_d$ szorzat legalább két tényezőjének gyöke. Mivel ez egy szorzat, melynek eredménye $x^m - 1$, ezért c kétszeres gyöke a $f(x) = x^m - 1 \in \mathbb{Z}_q[x]$ polinomnak. Ekkor az következő összefüggés miatt (mely azt mondja ki, hogy ha T egy tetszőleges kommutatív test, $f \in T[x]$, akkor $\alpha \in T$ elemet f polinom többszörös gyökének nevezzük, ha $(x-\alpha)^2|f$, ami pontosan akkor teljesül, ha $f(\alpha) = f'(\alpha) = 0$) $f'(c) = mc^{m-1} = 0$ $\mathbb{Z}_p$-ben.

Mivel $q \nmid m$ és $q \nmid c$, azaz a $\mathbb{Z}_q$ testben $m \neq 0$ és $c \neq 0$, ezért mc^{m-1} sem lehet 0, ami ellentmond az előzőnek. Ezzel a lemmát bebizonyítottuk. □

Tegyük fel indirekt módon, hogy csak véges sok $mk + 1$ alakú prím van(esetleg egy sincs), és legyenek ezek $p_1, p_2 \ldots, p_r$. Legyen $c = vmp_1 \ldots p_r$, ahol v tetszőleges pozitív egész. Elég nagy v esetén $\Phi_m(c) > 1$ teljesül.

Legyen ekkor q a $\Phi_m(c)$ egy tetszőleges prímosztója. Ekkor $\Phi_m(c)|c^m - 1$ miatt a $(q, c) = 1$, és emiatt a $q \nmid m$ is teljesül. Ezért a fenti lemma miatt $o_q(c) = m$. Ezekből következik, hogy $m|q-1$, azaz $q = mk + 1$ alakú. Már csak az kell, hogy végtelen sok is van belőle, de ez a $(q, c) = 1$ miatt $q \neq p_i$ így ez elletmond annak a feltevésnek, hogy $p_1, \ldots, p_r$ az összes $mk+1$ alakú prím. Ezzel a tételt beláttuk. □

(Forrás: Freud Róbert, Gyarmati Edit: Számelmélet)

Most lássunk néhány tételt, ami a körosztási polinomok és a prímszámok kapcsolatát mutatja be.

4.1.7. Tétel: Legyen n pozitív egész, a pedig egy egész szám. Ekkor $\Phi_n(a)$ minden p prímosztójára teljesül, hogy $p \equiv 1 \pmod{n}$ vagy $p|n$.

Bizonyítás: Legyen p prímosztója $\Phi_n(a)$-nek. Tudjuk, hogy $p \nmid a$, mert

$p|\Phi_n(a)|a^n-1$. Legyen $k=o_p(a)$, mivel $p|a^n-1$, ekkor $a^n\equiv 1 \pmod p$, így $k|n$. Ha $k=n$, ebből az következik, hogy $n|p-1$ tehát $p\equiv 1 \pmod n$, mivel Euler-tétel miatt $a^{p-1}\equiv 1 \pmod n$. Most nézzük azt az esetet mikor $k<n$. Mivel

$$0\equiv a^k-1\equiv \prod_{d|k}\Phi_d(a)(\bmod p)$$

akkor létezik d, mely osztja k-t és melyre $p|\Phi_d(a)$. De $d|k|n$ és $d<n$, így a feltétel szerint az a szám kétszeres gyöke az x^n-1 polinomnak modulo p, mivel $x^n-1=\prod_{d|n}\Phi_d(x)$, és itt $p|\Phi_d(a)$ és $p|\Phi_n(a)$. Az x^n-1 polinomnak a deriváltját véve ez csak akkor nem relatív prím az x^n-1 polinomhoz - ez a többszörös gyök létezésének a feltétele -, ha a derivált polinom 0, azaz $p|n$. Ezzel a tételt beláttuk. □

4.1.8. Tétel: Legyen p prím szám, és a egész. Akkor $1+a+\cdots+a^{p-1}$ összes q prímosztójára teljesül, hogy $q\equiv 1 \pmod p$ vagy $q=p$.

Bizonyítás: Legyen q egy prímosztója $1+a+\cdots+a^{p-1}$-nek. Mivel

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

ezért $1+a+\cdots+a^{p-1}=\Phi_p(a)$. A 4.1.7 tételből következik, hogy $q\equiv 1 \pmod p$ vagy $q|p$, tehát $q=p$. □

Ezekre a tételekre lássunk most egy példát:

4. példa:(IMO Shortlist,2006)

Találjuk meg az összes egész megoldását az alábbi egyenletnek.

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

Megoldás:

A felső egyenlet ekvivalens a $1+x+\cdots+x^6=(y-1)(1+y\cdots+y^4)$ egyenlettel. A 4.1.8 tétel miatt tudjuk, hogy minden q prímosztója

$1 + \cdots + x^{p-1}$-nak vagy $p = q$-val vagy $q \equiv 1 \pmod{p}$. Ez azt jelenti, hogy minden p prímosztója $1 + \cdots + x^6$-nak vagy $p = 7$-tel vagy $p \equiv 1 \pmod{7}$. Ezért $(y-1) \equiv 0 \pmod{7}$ vagy $(y-1) \equiv 1 \pmod{7}$. Ebből következik, hogy $y \equiv 1$ vagy $y \equiv 2 \pmod{7}$. Ha $y \equiv 1 \pmod{7}$, akkor az $1 + y + \cdots + y^4 \equiv 5 \not\equiv 0, 1 \pmod{7}$ ami ellentmondás. Ha pedig $y \equiv 2 \pmod{7}$, akkor az $1 + y + \cdots + y^4 \equiv 31 \equiv 3 \not\equiv 0, 1 \pmod{7}$, akkor ez is ellentmondáshoz vezet. Így a példa megoldására azt kapjuk, hogy ennek az egyenletnek nincs egész megoldása.

(Forrás: Yimin Ge: Elementary Properties of Cyclotomic Polynomials)

4.2. $\Phi_n(2)$ alakú prímek

Ha már a prímszámoknál járunk, érdemes megemlíteni a $\Phi_n(2)$ alakú prímszámokat.

Ha $n = 2^m$, akkor a $\Phi_{2^m}(2) = 2^{2^{m-1}} + 1 = F_{m-1}$-t, azaz a Fermat-számokat, ha pedig p prím, akkor a $\Phi_p(2) = 2^p - 1 = M_p$-t, a Mersenne-számokat adják meg. A Fermat és a Mersenne-prímek két ritka alosztályába tartozik a $\Phi_n(2)$ alakú prímek között. De az még nyitott kérdés, hogy $\Phi_n(2)$ faktorizációját hogyan lehet megoldani $O(n)$ művelettel modulo $\Phi_n(2)$, mikor n nem prím vagy 2 hatványa. Feltehetőleg az első $\Phi_n(2)$ alakú prímszámokat Yves Gallot számította ki. Az ő által megjelentetett cikkben ([6]) megadja azon $1 \leq n \leq 6500$ számokat, melyre $\Phi_n(2)$ valóban prímet ad.

Lássuk ezeket a számokat:

2,	3,	4,	5,	6,	7,	8,	9,	10,	12,
13,	14,	15,	16,	17,	19,	22,	24,	26,	27,
30,	31,	32,	33,	34,	38,	40,	42,	46,	49,
56,	61,	62,	65,	69,	77,	78,	80,	85,	86,
89,	90,	93,	98,	107,	120,	122,	126,	127,	129,
133,	145,	150,	158,	165,	170,	174,	184,	192,	195,
202,	208,	234,	254,	261,	280,	296,	312,	322,	334,
345,	366,	374,	382,	398,	410,	414,	425,	447,	471,
507,	521,	550,	567,	579,	590,	600,	607,	626	690,
694,	712,	745,	795,	816,	897,	909,	954,	990,	1106,
1192,	1224,	1230,	1279,	1384,	1386,	1402,	1464,	1512,	1554,
1562,	1600,	1670,	1683,	1727,	1781,	1834,	1904,	1990,	1992,
2008,	2037,	2203,	2281,	2298,	2353,	2406,	2456,	2499,	2536,
2838,	3006,	3074,	3217,	3415,	3418,	3481,	3766,	3817,	3927,
4167	,4253,	4423,	4480,	5053,	5064,	5217,	5234,	5238,	5250,
5325,	5382,	5403,	5421,	6120.					

(Forrás: Yves Gallot: Cyclotomic polynomials and prime numbers)

4.3. Völgytétel

Ebben a részben a $d(n)$ függvény egy érdekes viselkedését fogjuk megnézni. Bármely C egész számra tudunk találni végtelen sok hármas szomszédot, melyekre teljesül, hogy a pozitív osztóiknak a száma legalább C-vel eltér, azaz a grafikonjában tetszőlegesen mély „völgyet" és „hegyet" tartalmazhat. Freud Róbert és Gyarmati Edit: Számelmélet című könyvében [4] ennek a tételnek a bizonyításához a Dirichlet-tételt használják fel, mi pedig látni fogunk egy olyan bizonyítást, ami a körosztási polinomokat használja.

4.3.1. Tétel: Ha $d(n)$ jelöli az n egész szám pozitív osztóinak a számát, akkor minden $C > 0$-ra létezik olyan n, hogy $d(n-1) > d(n) + C$, és $d(n+1) > d(n) + C$.

Bizonyítás: Legyen $m = 15^k$, ahol k pozitív egész szám. Ekkor vizsgáljuk a $p(x) = x^m - 1$ és a $q(x) = x^m + 1$ polinomokat. Ezekre igaz, hogy

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

és

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

mivel m páratlan.

Ezért a $p(x)$ és $q(x)$ polinomokat is $d(m) = d(3^k \cdot 5^k) = (k+1)^2$ darab különböző irreducibilis egész együtthatós polinom szorzatára bontottuk. Tekintsük a $p(x)$ ilyen szorzatalakjában a tényezőkből képezhető részszorzatokat. Ezekből $2^{(k+1)^2}$ darab van, és a tényezők irreducibilitása miatt mind különböző polinomok. Emiatt bármely kettő értéke legfeljebb véges sok helyen egyezhet meg, vagyis létezik olyan A konstans, hogy $t > A$-ra a $p(x)$ tényezőiből képezhető részszorzatok helyettesítési értéke t-ben mind különböző. Hasonlóképpen létezik ilyen B konstans a $q(x)$ tényezőiből képezett részszorzatokhoz is.

Így látható, hogy minden $t > S = max(A, B)$ egészre a $p(t)$ és $q(t)$ egészeknek legalább ennyi különböző (nem feltétlenül pozitív) osztója van, mint a fenti szorzatalakjukban a tényezőkből képezhető részszorzatok száma. Ez a szám $2^{d(m)} = 2^{(k+1)^2}$. Így $d(p(t)), d(q(t)) \geq 2^{(k+1)^2-1}$, mivel pontosan ugyanannyi negatív osztója van, mint pozitív.

Végtelen sok prímszám van, ezért választható úgy egy $r > S$ pozitív prím, amire teljesül az előbbiek szerint a $d(r^m-1), d(r^m+1) \geq 2^{k^2+2k}$. Ezzel szemben $d(r^m) = m+1 = 15^k+1$. Itt $2^{k^2+2k} > 2^{k^2}$, míg $15^k+1 < 16^k = 2^{4k}$, vagyis $k > 4$-re tudjuk, hogy $d(r^m \pm 1) - d(r^m) > 2^{k^2} - 2^{4k} = 2^{4k}(2^{k^2-4k} - 1)$ $> 2^{4k} > C$ elég nagy k-t választva. Ekkor az $n = r^m$ választással az n rendelkezik a fenti tulajdonságokkal. Ezzel a tételt beláttuk. □

(Forrás: Ágoston Tamás írása)

4.4. Számelméleten kívüli alkalmazása

Végezetül egy pár mondatot írok arról, hogy hogyan függenek össze a körosztási polinomok a szabályos sokszögek szerkeszthetőségével.

Nézzük meg az első pár n-et, mely esetben a szabályos n-sokszög megszerkeszthető körzővel és vonalzóval.

$$3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20, 24, \ldots$$

Ebből a felsorolásból nem is látszik, mi alapján döntjük el, hogy meg tudjuk-e szerkeszteni vagy sem. A következőkben láthatjuk, hogy ezt egész egyszerűen le lehet ellenőrizni. Szabályos n-szög pontosan akkor szerkeszthető, ha meg tudjuk szerkeszteni azt a szöget, amely alatt látszik a sokszög egyik oldala. Ez a szög a $2\pi/n$ szög, így az a kérdés, hogy tudunk-e szerkeszteni $\cos(2\pi/n)$ hosszú szakaszt, vagyis, a komplex számsík
$\varepsilon = \cos(2\pi/n) + i\sin(2\pi/n)$ pontja megszerkeszthető-e, amennyiben adott a 0 és az 1 pont. Erről az ε pontról tudjuk, hogy egy primitív n-edik egységgyök, tehát gyöke Φ_n-nek. Azt is láttuk már a 3. fejezetben, hogy Φ_n kör-

osztási polinom irreducibilis. Gauss bebizonyította, hogy ha egy irreducibilis polinomnak ($\mathbb{Q}[x]$-belinek) van szerkeszthető gyöke, akkor a foka 2-hatvány. Mivel a 2.1.4 tételből tudjuk, hogy Φ_n foka $\varphi(n)$, ez azt jelenti, hogy ha szerkeszthető szabályos n-szög, akkor $\varphi(n)$-nek 2-hatványnak kell lennie. Tudjuk, hogy ha $n = \prod_{p|n} p^{\alpha_p}$, akkor a $\varphi(n) = \prod_{p|n} p^{\alpha_{p-1}}(p-1)$. Szóval ez akkor 2-hatvány, ha $p|n, p > 2$ esetén $\alpha_p = 1$ és $p-1$ 2-hatvány. A 2-hatvány+1 alakú prímeket, ahogy az előbb láttuk, Fermat-prímeknek nevezzük, tehát egy szabályos n-szög, akkor szerkeszthető, ha $n = 2^{\alpha} \cdot p_1 \cdot \cdots \cdot p_r$, ahol $\alpha, r \geq 0$ egészek, és $p_1, \ldots p_r$ különböző Fermat-prímek. (Ennek a tételnek a megfordítása is igaz, de ennek bizonyításásra nem térünk ki.) Ez az összefüggés magyarázza a „körosztási polinom" elnevezést is.

5. fejezet

Összefoglalás

Szakdolgozatomban egy kis ízelítőt adtam arra, hogy mi mindenre használható a körosztási polinom.

Az első fejezetben megismerkedünk az alap fogalmakkal. A lehetetlennek tűnű kiszámításból, lemmákon és tételeken keresztül eljutottunk ahhoz a módszerhez, amely megkönnyítette a helyzetünket. A fejezet végén beláttuk azt az érdekességet, hogy bármelyik egész szám lehet $\Phi_n(x)$ együtthatója.

A második fejezetben a körosztási polinomok irreducibilitásáról láttunk pár bizonyítást először p prím esetén, majd a fejezet végén minden n-re is beláttuk.

Az utolsó fejezetben láthattuk néhány alkalmazását a számelméletben. Megnéztük, hogy prímfaktorizációnál mennyire megkönnyíti a helyzetünket a körosztási polinomok használata, ismerete. Beláttuk, hogy végtelen sok $mk+1$ alakú prím van, ha $m \geq 0$. Néhány tételt és egy példát is láttunk a prímek és a $\Phi_n(x)$ kapcsolatára. Pár szót ejtettünk a $\Phi_n(2)$ alakú prímekről, illetve a Völgytétellel is megismerkedünk. A szabályos sokszögek szerkesztésénél is megnéztük a szerepét, mely által a fejezet legvégén még az is kiderült, hogy honnan ered a név azaz a, KÖROSZTÁSI POLINOM.

Irodalomjegyzék

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

[2] Vivtor V. Prasolov: Polynomials, Springer, 2001

[3] Új matematikai mozaik: Laczkovich Miklós: A Körosztási polinomokról, Typotex Kiadó, 2002

[4] Freud Róbert, Gyarmati Edit: Számelmélet, Nemzeti Tankönyvkiadó, 2006

[5] Yimin Ge: Elementary Properties of Cyclotomic Polynomials, $http://www.yimin-ge.com/doc/cyclotomic\_polynomials.pdf$

[6] Yves Gallot: Cyclotomic polynomials and prime numbers, $http://yves.gallot.pagesperso-orange.fr/papers/cyclotomic.pdf$

[7] R.Thangadurai: On the coefficients of cyclotomic polynomials, $http://www.bprim.org/cyclotomicfieldbook/th.pdf$

[8] Steven H. Weintraub: Several proofs of the irreducibility of the cyclotomic polynomials, $http://www.lehigh.edu/\ shw2/c-poly/several\_proofs.pdf$

[9] Ágoston Tamás írása

NYILATKOZAT

Név: Csomós Beatrix
ELTE Természettudományi Kar, szak: Matematika BSc
Neptun azonosító: P0179N
Szakdolgozat címe: Körosztási polinomok

A **szakdolgozat** szerzőjeként fegyelmi felelősségem tudatában kijelentem, hogy a dolgozatom önálló munkám eredménye, saját szellemi termékem, abban a hivatkozások és idézések standard szabályait következetesen alkalmaztam, mások által írt részeket a megfelelő idézés nélkül nem használtam fel.

Budapest, 2014. május 28.

_____
a hallgató aláírása