A KÖROSZTÁSI POLINOM

És ha minden császár kiadja pátensét és ukázát, hogy kétszer kettő ezentúl öt legyen, ha minden pápa kiadja bulláját, hogy kétszer kettőt ötnek higgyék, és ha minden pénzkirály ötnek fogja is számítani a kétszer kettőt, az azért mégis örökké négy marad.

Jókai Mór: *Fekete gyémántok*

1. Számolás komplex egységgyökökkel

Ha csak szorozni kell, akkor a komplex egységgyökökkel trigonometrikus alakban nagyon könnyű számolni. Ha összeadni is akarunk, akkor viszont trigonometrikus összegek keletkeznek, amiket pontosan nem mindig tudunk kiszámítani.

1.1. Feladat. Legyen $\varepsilon = \cos 10^\circ + i \sin 10^\circ$. Igaz-e, hogy $\varepsilon^{13} + \varepsilon = \varepsilon^7$?

A feladat megoldásához a $\cos 130^\circ + \cos 10^\circ = \cos 70^\circ$ és $\sin 130^\circ + \sin 10^\circ = \sin 70^\circ$ egyenlőségeket kell ellenőrizni. Ez kalkulátorral csak közelítőleg tehető meg, ami az $\varepsilon^{13} + \varepsilon = \varepsilon^7$ összefüggést esetleg cáfolhatja, de nem bizonyíthatja. Némi ötletességgel, és a trigonometrikus azonosságok alkalmazásával kihozható persze, hogy ezek az egyenlőségek igazak. De ez reménytelen akkor, ha egy bonyolultabb ε-ra vonatkozó egyenlőséget kell igazolni vagy cáfolni. Egy olyan módszert szeretnénk kidolgozni, hogy tetszőleges $f \in \mathbb{Q}[x]$ polinomra mechanikusan eldönthessük, hogy $f(\varepsilon)$ nulla-e, vagy sem. Látni fogjuk, hogy a kapott eszközöket egészen váratlan célokra, például számelméleti vagy geometriai tételek bizonyítására is fel tudjuk majd használni.

Ha olyan racionális együtthatós polinomot keresünk, amelynek $\varepsilon = \cos 10^\circ + i \sin 10^\circ$ gyöke, akkor a legkézenfekvőbb az $x^{36} - 1$-et tekinteni (hiszen ε nyilván harminchatodik egységgyök). Persze ε gyöke az $x^{36} - 1$ többszöröseinek is. De nemcsak ezeknek gyöke! Az $x^{36} - 1$ szorzattá alakítható, mint $(x^{18} - 1)(x^{18} + 1)$, és így ε valamelyik tényezőnek gyöke lesz. Könnyű látni, hogy ez a második tényező: az elsőnek ε nem lehet gyöke, mert akkor tizennyolcadik egységgyök lenne, márpedig ε *primitív* harminchatodik egységgyök.

Szorzattá bontható az $x^{18} + 1$ polinom is:

$$x^{18} + 1 = \left(x^6\right)^3 + 1 = (x^6 + 1)(x^{12} - x^6 + 1)\,.$$

Melyik tényezőnek lesz gyöke az ε? Ha $\varepsilon^6 = -1$ lenne, akkor négyzetre emelve $\varepsilon^{12} = 1$, ami ismét ellentmond annak, hogy ε primitív harminchatodik egységgyök. Tehát ε a második tényezőnek lesz gyöke. Ebből már következik, hogy a fenti feladat állítása igaz, hiszen $\varepsilon^{13} + \varepsilon - \varepsilon^7 = \varepsilon(\varepsilon^{12} - \varepsilon^6 + 1) = 0$.

Tehát a $g(x) = x^{12} - x^6 + 1$ polinom többszöröseinek gyöke az ε. Gyöke-e más racionális együtthatós polinomnak is? Ha g-t még tovább tudjuk bontani szorzatra, akkor igen. De nem ez a helyzet.

1.2. Feladat. Igazoljuk, hogy $x^{12} - x^6 + 1$ felbonthatatlan $\mathbb{Q}$ felett.

Ennek a (nehéz) feladatnak a felhasználásával meg tudjuk adni a fent keresett eljárást. Belátjuk ugyanis, hogy egy racionális együtthatós polinomnak akkor és csak akkor gyöke $\varepsilon = \cos 10^\circ + i \sin 10^\circ$, ha a $g(x) = x^{12} - x^6 + 1$-gyel osztható. Ezt az oszthatóságot pedig könnyen el tudjuk dönteni a maradékos osztás segítségével. Állításunkat két lépésben bizonyítjuk.

1.3. Állítás. *Tekintsük az összes olyan racionális együtthatós polinomot, melynek ε gyöke. Ha m ezek között egy lehető legalacsonyabb fokszámú polinom, akkor a többiek éppen az m többszörösei.*

Bizonyítás. Mivel $m(\varepsilon) = 0$, az ε gyöke m minden többszörösének. Megfordítva, tegyük fel, hogy $f(\varepsilon) = 0$, ahol $f \in \mathbb{Q}[x]$. Osszuk el maradékosan f-et m-mel: $f = mq + r$, ahol $q, r \in \mathbb{Q}[x]$, és $r = 0$ (ebben az esetben készen vagyunk), vagy r foka kisebb, mint m foka. Az ε számot behelyettesítve $f(\varepsilon) = m(\varepsilon)q(\varepsilon) + r(\varepsilon)$ adódik, és mivel $f(\varepsilon) = m(\varepsilon) = 0$, ezért $r(\varepsilon) = 0$. Ez ellentmond annak, hogy m-et minimális fokúnak választottuk. $\square$

1.4. Állítás. *Ha $f \in \mathbb{Q}[x]$, akkor $f(\varepsilon) = 0 \Longleftrightarrow g \mid f$.*

Bizonyítás. Az állítást az imént láttuk be g helyett m-re. Speciálisan $g(\varepsilon) = 0$ miatt $m \mid g$. De g irreducibilis, és ezért m vagy konstans, vagy g-nek asszociáltja. Konstans nem lehet, hiszen ε gyöke. Ezért $m \sim g$, és így a többszöröseik halmaza is ugyanaz. $\square$

1.5. Kérdés. Gondoljuk végig az elemrendre vonatkozó $b^k = 1 \Longleftrightarrow o(b) \mid k$ állítás bizonyítását, és keressük meg az analógiákat az iménti gondolatmenettel.

Az elhangzott bizonyításokat végiggondolva láthatjuk, hogy csak nagyon keveset használtunk ki ε és g speciális tulajdonságaiból. Legyen ε helyett α tetszőleges komplex szám. Az α *minimálpolinomjának* nevezzük azt a legalacsonyabb fokú, racionális együtthatós, normált polinomot, melynek α gyöke.

1.6. Kérdés. Jogunk van-e **a** minimálpolinomról beszélni? Mennyire egyértelmű ez? Miért követeljük meg, hogy a minimálpolinom normált legyen?

Természetesen előfordulhat az, hogy egy komplex szám nem gyöke egyetlen racionális együtthatós nem nulla polinomnak sem. Ezeket *transzcendens* számoknak nevezzük. Transzcendens szám például a π (ezt nagyon nehéz bebizonyítani), ez az oka annak, hogy a körnégyszögesítés nem oldható meg körzővel és vonalzóval. Azok a számok, amelyek gyökei egy alkalmas racionális együtthatós, nem nulla polinomnak, az *algebrai* számok. Ezeknek van minimálpolinomja.

A fenti bizonyítások az általános esetben a következőt adják.

1.7. Tétel. *Legyen α tetszőleges algebrai komplex szám, és m a minimálpolinomja.*

(1) *Azok a racionális együtthatós polinomok, melyeknek α gyöke, éppen m többszörösei.*

(2) *Ha g normált, irreducibilis $\mathbb{Q}$ felett, és gyöke az α, akkor g az α minimálpolinomja.*

1.8. Gyakorlat. Általánosítsuk a minimálpolinom fogalmát és a 1.7. Tételt a racionális számok teste helyett $\mathbb{C}$ tetszőleges résztestére.

1.9. Gyakorlat. Igazoljuk, hogy ha egy komplex számnak van minimálpolinomja, akkor az irreducibilis ($\mathbb{Q}$ felett).

1.10. Gyakorlat. Keressük meg az alábbi egységgyökök minimálpolinomjait: 1, -1, i, $-i$, $\cos 22.5^\circ + i \sin 22.5^\circ$.

1.11. Gyakorlat. Legyen $\varepsilon = \cos 22.5^\circ + i \sin 22.5^\circ$. Igaz-e, hogy $\varepsilon^{10} + 4 = 3\varepsilon$?

2. A körosztási polinom kiszámítása

Hogyan találhatjuk meg a komplex egységgyökök minimálpolinomjait? Vizsgáljuk meg az $\varepsilon = \cos 10^\circ + i \sin 10^\circ$ esetben kapott $g(x) = x^{12} - x^6 + 1$ polinomot. Mik ennek a gyökei? Emlékezzünk: az ε számról, amikor beláttuk, hogy gyöke g-nek, csak azt használtuk ki, hogy primitív harminchatodik egységgyök. Ezért g-nek mindegyik primitív harminchatodik egységgyök gyöke lesz. Mivel azonban az Euler-függvény képlete szerint $\varphi(36) = 12$ primitív harminchatodik egységgyök van, és g tizenkettedfokú polinom, ezért g gyökei pontosan a primitív harminchatodik egységgyökök.

2.1. Gyakorlat. Igazoljuk a már bizonyított
$$x^{12} - x^6 + 1 = \frac{x^{36} - 1}{(x^{18} - 1)(x^6 + 1)} = \frac{(x^{36} - 1)(x^6 - 1)}{(x^{18} - 1)(x^{12} - 1)}$$
képlet felhasználásával, de a primitív egységgyökök számára való hivatkozás nélkül, hogy $x^{12} - x^6 + 1$ gyökei pontosan a primitív harminchatodik egységgyökök.

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

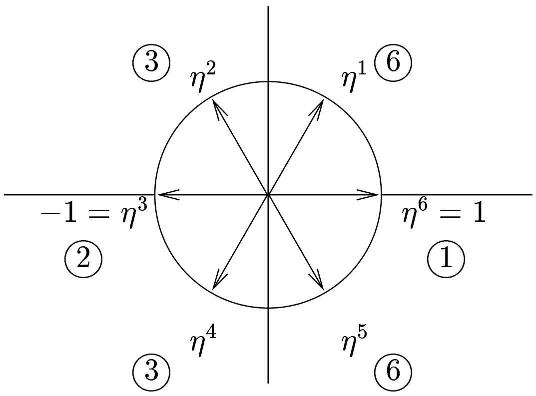
Természetesen Φ_n egyértelműen meghatározott: $\Phi_n(x) = (x - \xi_1) \ldots (x - \xi_{\varphi(n)})$, ahol $\xi_1, \ldots, \xi_{\varphi(n)}$ az összes primitív n-edik egységgyök, vagyis az összes n-edrendű komplex szám. Látjuk azt is, hogy Φ_n foka $\varphi(n)$. A definíciót kis n számok esetén közvetlenül felhasználhatjuk a körosztási polinomok kiszámítására. Nyilván $\Phi_1(x) = x - 1$ és $\Phi_2(x) = x - (-1) = x + 1$. A negyedik egységgyökök (1, -1, i és $-i$) közül az i és a $-i$ negyedrendű, azaz primitív, és ezért $\Phi_4(x) = (x - i)(x + i) = x^2 + 1$.

2.3. Gyakorlat. Mutassuk meg a megfelelő egységgyökök algebrai alakjának kiszámításával, hogy $\Phi_3(x) = x^2 + x + 1$, $\Phi_6(x) = x^2 - x + 1$, és $\Phi_{12}(x) = x^4 - x^2 + 1$.

Láthatjuk, hogy ez a közvetlen módszer általában nem működik: nagyobb n-ekre már a $\sin(2\pi/n)$ és $\cos(2\pi/n)$ értékét is csak közelítőleg tudjuk kiszámolni, a beszorzás pedig végképp elbonyolítja a dolgot. Pedig az eredmény szép: az összes eddig tárgyalt esetben egész együtthatós polinom jött ki, és látni fogjuk, hogy meglepő módon ez általában is így van. Az általános eljárás hasonlítani fog ahhoz, amit az előző fejezetben alkalmaztunk, amikor beláttuk, hogy $\Phi_{36}(x) = x^{12} - x^6 + 1$.

Hogyan határozhatnánk meg például a Φ_3 polinomot? Ennek gyökei harmadik egységgyökök. A három harmadik egységgyök az $x^3 - 1$ polinom három gyöke. Ezek közül az 1 nem jó, mert az nem primitív harmadik egységgyök, de a másik kettő igen. Ezért ez a másik két szám az $(x^3 - 1)/(x - 1) = x^2 + x + 1$ polinomnak lesz gyöke. Azaz $\Phi_3(x) = x^2 + x + 1$.

Ha a hatodik körosztási polinomot akarjuk kiszámítani, akkor a hatodik egységgyököket kell áttekintenünk. Legyen $\eta = \cos 60^\circ + i \sin 60^\circ$. Ez primitív hatodik egységgyök, ezért a hatodik egységgyökök ennek a hatványai. A hatvány rendjére vonatkozó képletből látjuk, hogy $o(\eta) = o(\eta^5) = 6$ (ezek a hatodik primitív egységgyökök), $o(\eta^2) = o(\eta^4) = 3$ (tehát η^2 és η^4 pont a két primitív harmadik egységgyök), $o(\eta^3) = 2$ (valójában $\eta^3 = -1$), végül $o(\eta^6) = 1$ (és $\eta^6 = 1$). Az ábrán feltüntettük a hatodik egységgyököket, és bekarikázva a rendjüket is.



Mivel $x^6 - 1$ gyökei pont a hatodik egységgyökök, azt kapjuk, hogy

$$x^6 - 1 = (x - \eta)(x - \eta^2)(x - \eta^3)(x - \eta^4)(x - \eta^5)(x - \eta^6)\,.$$

Csoportosítsuk a gyöktényezőket az egységgyökök rendjei szerint.

$$\begin{aligned} x^6 - 1 &= \big[(x - \eta)(x - \eta^5)\big]\ \big[(x - \eta^2)(x - \eta^4)\big]\ (x - \eta^3)\ (x - \eta^6) = \\ &= \qquad \Phi_6(x) \qquad \cdot \qquad \Phi_3(x) \qquad \cdot\ \Phi_2(x)\ \cdot \Phi_1(x)\,. \end{aligned}$$

Innen

$$\Phi_6(x) = \frac{x^6 - 1}{\Phi_1(x)\Phi_2(x)\Phi_3(x)}\,.$$

Mivel a Φ_1, Φ_2 és Φ_3 polinomokat már kiszámoltuk, osztással megkapjuk a keresett Φ_6-ot is. A számolást lerövidíti, ha felhasználjuk a korábban már bebizonyított $\Phi_1(x)\Phi_3(x) = x^3 - 1$ összefüggést:

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

2.4. Gyakorlat. Kövessük végig ezt a gondolatmenetet $n = 6$ helyett $n = 12$-re, és határozzuk meg a Φ_{12} polinomot ezzel a módszerrel is.

Az elhangzott gondolatmenetet most már könnyű általánosítani.

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

Bizonyítás. Legyen $\eta = \cos(2\pi/n) + i\sin(2\pi/n)$. Ekkor η primitív n-edik egységgyök, és ezért hatványai az n-edik egységgyököket adják meg. Ezek éppen az $x^n - 1$ gyökei, és mivel n különböző számról van szó, az $x^n - 1$ gyöktényezős alakja

$$x^n - 1 = (x - \eta)(x - \eta^2)\ldots(x - \eta^n)\,.$$

Ismét a megfelelő egységgyökök rendjei szerint csoportosítjuk a gyöktényezőket. Jelölje f_d a d rendű egységgyökökhöz tartozó gyöktényezők szorzatát. Így

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

Elég belátni, hogy a fellépő d számok pontosan n osztói, és hogy ezekre $f_d = \Phi_d$.

Mivel $\eta^n = 1$, ezért minden m-re $(\eta^m)^n = 1$, és így $d = o(\eta^m) \mid n$, vagyis a fellépő d számok tényleg csak n osztói lehetnek. Tegyük fel, hogy $d \mid n$. Ekkor Φ_d-ben az *összes* d rendű komplex szám szerepel, f_d-ben pedig az olyan d rendű komplex számok szerepelnek, amik egyben n-edik egységgyökök is. De ha egy ξ számra $d = o(\xi) \mid n$, akkor $\xi^n = 1$, ezért ξ mindenképpen n-edik egységgyök. Tehát $f_d = \Phi_d$. $\square$

2.6. Gyakorlat. Igazoljuk, hogy tetszőleges $n \geq 1$ egészre $\sum_{d|n} \varphi(d) = n$.

2.7. Következmény. *Ha $n \geq 1$, akkor a Φ_n körosztási polinom egész együtthatós.*

Bizonyítás. Legyen n a legkisebb olyan pozitív egész, melyre Φ_n nem egész együtthatós. Az előbbi lemma miatt

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

Az n minimalitása miatt a nevezőben csupa egész együtthatós polinom van, amik normáltak is. Ezért a nevező maga is normált, és egész együtthatós. Tudjuk, hogy minden olyan polinommal lehet maradékosan osztani, melynek a főegyütthatója invertálható. Ezért a számláló maradékosan elosztható a nevezővel $\mathbb{Z}[x]$-ben. A maradékos osztás ($\mathbb{C}$ feletti) egyértelműsége miatt a hányados és a maradék ugyanaz, mint ha az osztást $\mathbb{C}$ felett végeznénk. De $\mathbb{C}$ felett tudjuk, hogy a hányados Φ_n és a maradék nulla. Tehát $\mathbb{Z}$ felett is Φ_n a hányados, vagyis Φ_n mégis egész együtthatós. Ez az ellentmondás bizonyítja az állítást. □

Ebben a bizonyításban a teljes indukciónak egy formáját használtuk, feltettük, hogy az állítás minden n-nél kisebb értékre igaz, és beláttuk ebből, hogy n-re is igaz. Noha a fenti fogalmazásból is látszik, hadd hangsúlyozzuk még egyszer, hogy ilyenkor az indukciónak nincs „kezdő esete". Például az $n = 1$-et nem kell külön megnézni: a fenti gondolatmenetnek ekkor is működnie kell. Ha $n = 1$, akkor az, hogy minden n-nél kisebb értékre tudjuk az állítást, *üres feltétel.* A fenti képlet most így néz ki:

$$\Phi_1(x) = \frac{x^1 - 1}{\prod\limits_{\substack{d \mid 1 \\ d \neq 1}} \Phi_d(x)}\,.$$

A nevező *üres szorzat*, értéke tehát 1, és így a $\Phi_1(x) = x - 1$ összefüggést kapjuk, ami persze bizonyítja, hogy Φ_1 egész együtthatós.

A tanulság az, hogy miképpen egy programozónak figyelnie kell arra, hogy a programja akkor is jól működjön, ha mondjuk egy ciklus nullaszor fut le, *minden bizonyításban figyeljünk oda az „extrém" esetekre is, például arra, amikor egy halmaz, összeg, vagy szorzat üres, mert a bizonyításnak ilyenkor is működnie kell.*

Mint a Φ_6 példáján láttuk, az iménti bizonyítás egyben módot ad arra, hogy a körosztási polinomokat rekurzívan kiszámítsuk.

2.8. Gyakorlat. Számítsuk ki az n-edik körosztási polinomot az összes $n \leq 20$ egészre.

2.9. Gyakorlat. Számítsuk ki a prímhatvány-indexű körosztási polinomokat.

2.10. Feladat. Bizonyítsuk be, hogy $\Phi_n(x) = \prod_{d \mid n} (x^{n/d} - 1)^{\mu(d)}$, ahol μ az úgynevezett *Möbius-függvény:* ha az m pozitív egész szám s darab különböző prím szorzata, akkor $\mu(m) = (-1)^s$, egyébként pedig $\mu(m) = 0$. (Definiáltuk $\mu(1)$-et is?)

2.11. Feladat. Határozzuk meg a körosztási polinomok felhasználásával rendre a 12-edik, 18-adik illetve 24-edik primitív egységgyökök összegét és szorzatát. Általánosítsuk a feladatot!

2.12. Feladat. Határozzuk meg a Φ_n polinom együtthatóinak összegét.

2.13. Feladat. Legyenek $m \mid n$ pozitív egészek úgy, hogy n minden prímosztója osztja m-et is. Igazoljuk, hogy $\Phi_n(x) = \Phi_m(x^{n/m})$.

2.14. Gyakorlat. Számítsuk ki az előző feladat alapján a $\Phi_n(x)$ polinomokat, ha $n = 36, 72, 144, 100$.

2.15. Feladat. Állapítsuk meg, hogy ha ε egy n-edik primitív egységgyök, akkor mennyi lehet $-\varepsilon$ rendje.

2.16. Gyakorlat. Mutassuk meg, hogy ha $n > 1$ páratlan, akkor $\Phi_{2n}(x) = \Phi_n(-x)$.

2.17. Feladat. Határozzuk meg a $\Phi_n(-1)$ értékeket.

2.18. Feladat. Mutassuk meg, hogy két relatív prím rendű komplex szám szorzatának rendje a rendjeik szorzata. Általánosítható-e az állítás tetszőleges csoportra?

2.19. Feladat. Legyenek m és n relatív prím egészek. Mutassuk meg, hogy minden mn-edik primitív egységgyök egyértelműen előáll egy m-edik és egy n-edik primitív egységgyök szorzataként. Vezessük le ebből, hogy az Euler-függvény multiplikatív.

2.20. Feladat. A 2.16. Gyakorlat általánosításaként mutassuk meg, hogy ha m és n relatív prímek, akkor

$$\Phi_{mn}(x) = \prod_{o(\eta)=m} \Phi_n(\eta x)\,,$$

kivéve az $m = 2$, $n = 1$ esetben, amikor a két oldal egymás ellentettje.

Ezek a feladatok lehetővé teszik a Φ_n körosztási polinom kiszámítását sok esetben. Eleve elég páratlan négyzetmentes n számokkal foglalkozni a 2.13. Feladat és a 2.16. Gyakorlat miatt. Prímszámokra persze a 2.9. Feladat megadja az eredményt. A `MAPLE` program segítségével tetszőleges n esetén kiszámítható Φ_n (sőt, az eredményt a matematikai dokumentumok szedésére mindenki által használt, Donald Knuth által tervezett TEX nyelv formátumában is megkaphatjuk). Például a

```
with(numtheory):
for n from 3 by 2 to 105 do
  if issqrfree(n) and not isprime(n) then
    print(n, cyclotomic(n,x))
  fi
od;
```

parancssorozat kiírja páratlan, négyzetmentes, nem prím számokra a körosztási polinomokat 105-ig. Az eredmény a következő:

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

$$\Phi_{21} = x^{12} - x^{11} + x^9 - x^8 + x^6 - x^4 + x^3 - x + 1$$

$$\Phi_{33} = x^{20} - x^{19} + x^{17} - x^{16} + x^{14} - x^{13} + x^{11} - x^{10} + x^9 - x^7 + x^6 - x^4 + x^3 - x + 1$$

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

$$\Phi_{39} = x^{24} - x^{23} + x^{21} - x^{20} + x^{18} - x^{17} + x^{15} - x^{14} + x^{12} - x^{10} + \\ + x^9 - x^7 + x^6 - x^4 + x^3 - x + 1$$

$$\Phi_{51} = x^{32} - x^{31} + x^{29} - x^{28} + x^{26} - x^{25} + x^{23} - x^{22} + x^{20} - x^{19} + x^{17} - x^{16} + x^{15} - \\ - x^{13} + x^{12} - x^{10} + x^9 - x^7 + x^6 - x^4 + x^3 - x + 1$$

$$\Phi_{55} = x^{40} - x^{39} + x^{35} - x^{34} + x^{30} - x^{28} + x^{25} - x^{23} + x^{20} - x^{17} + \\ + x^{15} - x^{12} + x^{10} - x^6 + x^5 - x + 1$$

$$\Phi_{57} = x^{36} - x^{35} + x^{33} - x^{32} + x^{30} - x^{29} + x^{27} - x^{26} + x^{24} - x^{23} + x^{21} - x^{20} + x^{18} - \\ - x^{16} + x^{15} - x^{13} + x^{12} - x^{10} + x^9 - x^7 + x^6 - x^4 + x^3 - x + 1$$

$$\Phi_{65} = x^{48} - x^{47} + x^{43} - x^{42} + x^{38} - x^{37} + x^{35} - x^{34} + x^{33} - x^{32} + x^{30} - x^{29} + x^{28} - \\ - x^{27} + x^{25} - x^{24} + x^{23} - x^{21} + x^{20} - x^{19} + x^{18} - x^{16} + x^{15} - x^{14} + x^{13} - \\ - x^{11} + x^{10} - x^6 + x^5 - x + 1$$

$$\Phi_{69} = x^{44} - x^{43} + x^{41} - x^{40} + x^{38} - x^{37} + x^{35} - x^{34} + x^{32} - x^{31} + x^{29} - x^{28} + x^{26} - \\ - x^{25} + x^{23} - x^{22} + x^{21} - x^{19} + x^{18} - x^{16} + x^{15} - x^{13} + x^{12} - x^{10} + x^9 - \\ - x^7 + x^6 - x^4 + x^3 - x + 1$$

$$\Phi_{77} = x^{60} - x^{59} + x^{53} - x^{52} + x^{49} - x^{48} + x^{46} - x^{45} + x^{42} - x^{41} + x^{39} - x^{37} + x^{35} - \\ - x^{34} + x^{32} - x^{30} + x^{28} - x^{26} + x^{25} - x^{23} + x^{21} - x^{19} + x^{18} - x^{15} + x^{14} - \\ - x^{12} + x^{11} - x^8 + x^7 - x + 1$$

$$\Phi_{85} = x^{64} - x^{63} + x^{59} - x^{58} + x^{54} - x^{53} + x^{49} - x^{48} + x^{47} - x^{46} + x^{44} - x^{43} + x^{42} - \\ - x^{41} + x^{39} - x^{38} + x^{37} - x^{36} + x^{34} - x^{33} + x^{32} - x^{31} + x^{30} - x^{28} + x^{27} - \\ - x^{26} + x^{25} - x^{23} + x^{22} - x^{21} + x^{20} - x^{18} + x^{17} - x^{16} + x^{15} - x^{11} + \\ + x^{10} - x^6 + x^5 - x + 1$$

$$\Phi_{87} = x^{56} - x^{55} + x^{53} - x^{52} + x^{50} - x^{49} + x^{47} - x^{46} + x^{44} - x^{43} + x^{41} - x^{40} + x^{38} - \\ - x^{37} + x^{35} - x^{34} + x^{32} - x^{31} + x^{29} - x^{28} + x^{27} - x^{25} + x^{24} - x^{22} + x^{21} - \\ - x^{19} + x^{18} - x^{16} + x^{15} - x^{13} + x^{12} - x^{10} + x^9 - x^7 + x^6 - x^4 + x^3 - x + 1$$

$$\Phi_{91} = x^{72} - x^{71} + x^{65} - x^{64} + x^{59} - x^{57} + x^{52} - x^{50} + x^{46} - x^{43} + x^{39} - x^{36} + x^{33} - \\ - x^{29} + x^{26} - x^{22} + x^{20} - x^{15} + x^{13} - x^8 + x^7 - x + 1$$

$$\Phi_{93} = x^{60} - x^{59} + x^{57} - x^{56} + x^{54} - x^{53} + x^{51} - x^{50} + x^{48} - x^{47} + x^{45} - x^{44} + x^{42} - \\ - x^{41} + x^{39} - x^{38} + x^{36} - x^{35} + x^{33} - x^{32} + x^{30} - x^{28} + x^{27} - x^{25} + x^{24} - \\ - x^{22} + x^{21} - x^{19} + x^{18} - x^{16} + x^{15} - x^{13} + x^{12} - x^{10} + x^9 - x^7 + x^6 - \\ - x^4 + x^3 - x + 1$$

$$\begin{aligned}\Phi_{95} = {} & x^{72} - x^{71} + x^{67} - x^{66} + x^{62} - x^{61} + x^{57} - x^{56} + x^{53} - x^{51} + x^{48} - x^{46} + x^{43} - \\ & - x^{41} + x^{38} - x^{36} + x^{34} - x^{31} + x^{29} - x^{26} + x^{24} - x^{21} + x^{19} - x^{16} + x^{15} - \\ & - x^{11} + x^{10} - x^{6} + x^{5} - x + 1 \\ \Phi_{105} = {} & x^{48} + x^{47} + x^{46} - x^{43} - x^{42} - 2\,x^{41} - x^{40} - x^{39} + x^{36} + x^{35} + x^{34} + x^{33} + \\ & + x^{32} + x^{31} - x^{28} - x^{26} - x^{24} - x^{22} - x^{20} + x^{17} + x^{16} + x^{15} + x^{14} + x^{13} + \\ & + x^{12} - x^{9} - x^{8} - 2\,x^{7} - x^{6} - x^{5} + x^{2} + x + 1\end{aligned}$$

Ebből már láthatjuk, hogy $n = 105$ a legkisebb olyan szám, melyre a Φ_n polinomnak van olyan együtthatója, ami nem a $0, 1, -1$ számok valamelyike. Ezt számítógép nélkül is megmutathatjuk, mert nem nehéz kiszámolni, hogy ha n két különböző prím szorzata, akkor Φ_n együtthatói csak a $0, 1, -1$ számok lehetnek.

2.21. Gyakorlat. Határozzuk meg a `MAPLE` program segítségével azt a legkisebb n értéket, melyre a Φ_n polinomnak van kettőnél, illetve háromnál nagyobb abszolút értékű együtthatója.

3. A körosztási polinom $\mathbb{Z}_p$ felett

Be fogjuk bizonyítani, hogy az n-edik körosztási polinom irreducibilis $\mathbb{Q}$ felett, és ezért tényleg a primitív n-edik egységgyökök minimálpolinomja. Fel fogjuk használni a körosztási polinomokat a Dirichlet-tétel egy speciális esetének bizonyítására is. Mindkét bizonyítás mélyén az a gondolat bújik meg, hogy a körosztási polinomokkal mod p számolunk egy alkalmas p prímszámra.

Idézzük fel, mit is jelent az, hogy „mod m számolunk” valamely $m \geq 1$ egészre. Arról van ilyenkor szó, hogy a számoknak csak az m-mel vett osztási maradéka érdekel bennünket, azaz például m helyett már nullát írunk, $m+1$ helyett 1-et, és így tovább. Ha két számot össze kell adni, akkor az eredményt azonnal redukáljuk mod m, és ezt tesszük a szorzásnál is. Ez sokszor nagyon leegyszerűsíti a számolásokat, mert a „fölösleges” (azaz m-mel osztható) tagokat le se kell írnunk, más esetekben pedig az az előny, hogy csak véges sok lehetséges maradékkal kell foglalkoznunk.

Kissé pontosabban, jelölje felülvonás a mod m maradékképzést, azaz legyen $\overline{a}$ az a szám m-mel való osztási maradéka. Ekkor $\overline{a} \in \{0, 1, \ldots, m-1\}$, ezt a halmazt $\mathbb{Z}_m$ jelöli. Ha $u, v \in \mathbb{Z}_m$, akkor u és v összegét úgy számítjuk ki, hogy az $u + v$ egész számot mod m redukáljuk, vagyis az eredmény $\overline{u+v}$ lesz. Ezt a műveletet $+_m$ jelöli. Hasonlóan $u \cdot_m v = \overline{u \cdot v}$. Ha a szövegkörnyezetből világos, hogy a számolás mod m történik, akkor az $_m$ indexet el fogjuk hagyni. Tanultuk, hogy ezekre a műveletekre a $\mathbb{Z}_m$ gyűrű, ami test is, ha m prímszám.

3.1. Gyakorlat. Bizonyítsuk be, hogy a mod m maradékképzés művelettartó leképezés, azaz tetszőleges a, b egész számokra $\overline{a+b} = \overline{a} +_m \overline{b}$ és $\overline{a \cdot b} = \overline{a} \cdot_m \overline{b}$.

A felülvonás jelölést kiterjeszthetjük polinomokra is a következőképpen. Legyen $f \in \mathbb{Z}[x]$, és vegyük f együtthatóit mod m (azaz „húzzuk őket felül"). Ekkor egy $\overline{f} \in \mathbb{Z}_m[x]$ polinomot kapunk. Ez még mindig műveletartó leképezés lesz.

3.2. Gyakorlat. Legyen $f, g \in \mathbb{Z}[x]$. Igazoljuk, hogy $\overline{f+g} = \overline{f} +_m \overline{g}$ és $\overline{f \cdot g} = \overline{f} \cdot_m \overline{g}$.

Az első észrevételünk, ami nagyon megkönnyíti a számolást mod p, a következő.

3.3. Lemma. *Ha p prímszám, akkor $\mathbb{Z}_p[x]$-ben összeget és különbséget tagonként lehet p-edik (sőt, p^k-adik) hatványra emelni.*

3.4. Kérdés. Igaz marad-e a binomiális tétel tetszőleges kommutatív gyűrű felett? Nem okoz-e zavart, hogy a binomiális együtthatók nem gyűrűelemek, hanem számok?

Bizonyítás. A p^k-adik hatványra emelés k darab p-edik hatványra emelés egymásutánja, így elég ez utóbbival foglalkozni. Legyen $f, g \in \mathbb{Z}_p[x]$. A binomiális tétel szerint

$$(f+g)^p = f^p + \binom{p}{1} f^{p-1} g + \binom{p}{2} f^{p-2} g^2 + \cdots + \binom{p}{p-1} f g^{p-1} + g^p .$$

Az itt szereplő binomiális együtthatók azonban mind oszthatók p-vel, hiszen a

$$\binom{p}{j} = \frac{p!}{j!\,(p-j)!}$$

tört számlálója p-vel osztható, de $1 \leq j \leq p-1$ esetén a nevezőben szereplő faktoriálisok tényezői p-nél kisebbek, azaz p-vel nem oszthatók, és ezért a p prímtulajdonsága miatt a nevező sem osztható p-vel. Ha azonban $\mathbb{Z}_p[x]$ egy elemét p-szer összeadjuk önmagával, akkor nullát kapunk, és ezért a fenti összegben csak $f^p + g^p$ marad meg.

A most bizonyított állítást alkalmazva

$$(f-g)^p = (f+(-g))^p = f^p + (-g)^p = f^p - g^p ,$$

ha ugyanis p páratlan, akkor $(-1)^p = -1$, ha meg $p = 2$, akkor $\mathbb{Z}_p[x]$-ben tetszőleges g elemre $g = -g$ (hiszen $g + g = 0$). Azaz $\mathbb{Z}_2$ felett nem kell törődni az előjelekkel. $\square$

3.5. Gyakorlat. Vezessük le a kis-Fermat tételt az előző lemmából.

3.6. Következmény. *Legyen p prímszám. Ha $f \in \mathbb{Z}_p[x]$, akkor $f(x^p) = f(x)^p$.*

Bizonyítás. Ha $f(x) = a_0 + a_1 x + \cdots + a_n x^n$, akkor $f(x)^p = a_0^p + a_1^p x^p + \cdots + a_n^p (x^p)^n$. A kis-Fermat tétel miatt azonban minden $a_j^p = a_j$, és ezért készen vagyunk. $\square$

Ha a körosztási polinomokat mod p szeretnénk vizsgálni, akkor itt is az őket megadó $\prod_{d|n} \Phi_d(x) = x^n - 1$ rekurzióból érdemes kiindulni. Némi óvatosságra inthet azonban, hogy míg az $x^n - 1$ polinomnak $\mathbb{C}$-ben n különböző gyöke van, addig $\mathbb{Z}_p$ felett, az előbbi következmény miatt, $x^p - 1 = (x-1)^p$. Sőt általában, ha $p \mid n$, akkor

$$x^n - 1 = (x^p)^{n/p} - 1 = \left(x^{n/p} - 1\right)^p .$$

Vagyis az $x^n - 1$ polinomnak van többszörös tényezője. Fogjuk látni, hogy ez problémákat okoz, és ezért először is vizsgáljuk meg, hogy $p \nmid n$ esetén is lehetséges-e ez.

3.7. Lemma. *Ha p prímszám, akkor az $x^n - 1 \in \mathbb{Z}_p[x]$ polinomnak akkor és csak akkor van többszörös tényezője ($\mathbb{Z}_p$ felett), ha $p \mid n$.*

A bizonyításban a formális deriválás módszerét fogjuk használni.

3.8. Kérdés. Amikor egy általános T test felett egy polinom formális deriváltját tekintjük, nem okoz-e gondot az, hogy az $(x^n)' = nx^{n-1}$ képletben a kitevőbeli n egy egész szám, a polinom együtthatója viszont T-beli elem kell, hogy legyen?

Bizonyítás. A $p \mid n$ esetet már láttuk. Tegyük most fel, hogy $p \nmid n$, és $k(x)^2 \mid x^n - 1$ egy nem konstans $k \in \mathbb{Z}_p[x]$ polinomra. Ez azt jelenti, hogy van olyan $h \in \mathbb{Z}_p[x]$, melyre $k(x)^2 h(x) = x^n - 1$. Deriváljuk ezt az egyenlőséget. A szorzat deriválási szabályát ($(fg)' = f'g + fg'$) kétszer alkalmazva kapjuk, hogy

$$(k^2h)' = (k^2)'h + k^2h' = (k'k + kk')h + k^2h' = k(2k'h + kh')\,.$$

Azaz $k(x) \mid (x^n - 1)' = nx^{n-1}$. Mivel $p \nmid n$, az n együttható értéke mod p sem nulla, és így a $\mathbb{Z}_p[x]$-beli alaptétel miatt $k(x) = cx^{\ell}$, ahol $1 \le \ell \le n-1$ és $0 \ne c \in \mathbb{Z}_p$. Azaz $x \mid k(x)$, ami ellentmond annak, hogy $k(x)^2 \mid x^n - 1$, hiszen $x \nmid x^n - 1$. □

Megjegyezzük, hogy az n-edik körosztási polinom mod p vizsgálata során általában feltehetjük, hogy $p \nmid n$, a következő állítás miatt.

3.9. Feladat. Legyen p prímszám, és $n = p^k m$, ahol már $p \nmid m$. Mutassuk meg, hogy modulo p a Φ_n egyenlő a $\Phi_m^{\varphi(p^k)}$ polinommal.

Most kiszámítjuk, hogy $p \nmid n$ esetén mik a mod p tekintett körosztási polinom gyökei a $\mathbb{Z}_p$ testben. Idézzük fel a számelméleti elemrend fogalmát: ha $(c, m) = 1$, akkor $o_m(c)$ azt mondja meg, hogy c hatványai milyen hosszú periódus szerint ismétlődnek mod m (speciálisan $c^k \equiv 1 \ (m) \Longleftrightarrow o_m(c) \mid k$). Az Euler-Fermat tétel miatt így $o_m(c) \mid \varphi(m)$. Ha $m = p$ prím, akkor tehát $o_p(c)$ a $\overline{c}$ elem rendje a $\mathbb{Z}_p$ test multiplikatív csoportjában.

A Φ_n körosztási polinom komplex gyökei a $\mathbb{C}$ multiplikatív csoportjának n rendű elemei. Ugyanez igaz $\mathbb{Z}_p$ felett is, ha $p \nmid n$.

3.10. Tétel. *Legyen p prímszám. Ha $p \nmid n$, akkor a mod p vett $\overline{\Phi_n}$ körosztási polinom gyökei a $\mathbb{Z}_p$ testben pontosan $\mathbb{Z}_p$ multiplikatív csoportjának n rendű elemei.*

Bizonyítás. Tegyük fel, hogy $\varepsilon \in \mathbb{Z}_p$ gyöke $\overline{\Phi_n}$-nak, és legyen ℓ az ε rendje $\mathbb{Z}_p$ multiplikatív csoportjában. Mivel $\Phi_n(x) \mid x^n - 1$, ezért $\varepsilon^n - 1 = 0$, azaz $\ell \mid n$. Tegyük fel indirekte, hogy $\ell < n$. Ekkor ε gyöke már az $x^{\ell} - 1 \in \mathbb{Z}_p[x]$-nek is. De $x^{\ell} - 1 = \prod_{d \mid \ell} \Phi_d(x)$, vagyis van olyan $m \mid \ell$, hogy $\overline{\Phi_m}(\varepsilon) = 0$. Tehát az $x - \varepsilon$ gyöktényező kiemelhető a $\overline{\Phi_n}$ és a $\overline{\Phi_m}$ polinomokból. Persze $m \mid n$ és $m \ne n$, azaz ekkor ε legalább kétszeres gyöke $\overline{\Phi_m(x)}\,\overline{\Phi_n(x)} \mid x^n - 1$-nek. Az $x^n - 1$ polinomnak azonban nincs többszörös gyöke $\mathbb{Z}_p$-ben a 3.7. Lemma miatt. Ez az ellentmondás bizonyítja, hogy ε rendje tényleg n.

Legyen most ε egy n-edrendű eleme $\mathbb{Z}_p$-nek. Ekkor ε gyöke $x^n - 1 = \prod_{d|n} \overline{\Phi_d}(x)$-nek, tehát valamelyik $\overline{\Phi_d}$-nak is. Ha $d \neq n$ lenne, akkor $\Phi_d(x) \mid x^d - 1$ miatt $\varepsilon^d = 1$ teljesülne, ami ellentmond annak, hogy ε rendje n. □

A fenti gondolatmenet $\mathbb{C}$ felett is elmondható. Felépíthettük volna tehát az anyagot úgy is, hogy a körosztási polinomokat rekurzívan definiáljuk, és a most bizonyított állítást használjuk annak megmutatására, hogy a kapott polinomok gyökei éppen a primitív n-edik egységgyökök.

3.11. Gyakorlat. Számítsuk ki a $\Phi_p(x+1)$ polinomot, ahol p prímszám, és vizsgáljuk meg, alkalmazható-e rá a Schönemann-Eisenstein kritérium. Mi a helyzet a prímhatvány-indexű körosztási polinomokkal?

3.12. Feladat. Mutassuk meg, hogy a Φ_n polinom egy alkalmas eltoltjára akkor és csak akkor teljesül a Schönemann-Eisenstein kritérium, ha n prímhatvány, vagy egy páratlan prímhatvány kétszerese.

Aki ismeri a test karakterisztikájával kapcsolatos elemi tényeket (ez tanárszakon másodéves anyag), az általánosíthatja az eddig elmondottakat tetszőleges T testre. A $\prod_{d|n} \Phi_d(x) = x^n - 1$ rekurzióval tetszőleges T test felett definiálhatjuk a körosztási polinomokat.

3.13. Gyakorlat. Mutassuk meg, hogy ha a T test karakterisztikája nulla, akkor a T feletti körosztási polinomok megegyeznek a $\mathbb{Q}$ feletti (szokásos) körosztási polinomokkal, ha pedig T karakterisztikája a p prím, akkor a T feletti körosztási polinomok úgy kaphatók, hogy a szokásos körosztási polinomokat mod p vesszük.

3.14. Gyakorlat. Legyen T test, és tegyük fel, hogy T karakterisztikája nulla, vagy n-et nem osztó prímszám. Mutassuk meg, hogy Φ_n gyökei T-ben pontosan a T multiplikatív csoportjának n-edrendű elemei.

3.15. Feladat. Legyen $f \in \mathbb{Z}_p[x]$ irreducibilis polinom. Igazoljuk, hogy f-nek nem lehet többszörös gyöke egyetlenegy $\mathbb{Z}_p$-t (résztestként) tartalmazó testben sem.

4. Két számelméleti alkalmazás

Az első alkalmazás egy igen nevezetes tétel igen egyszerű bizonyítása. Legyen p prímszám. A g számot primitív gyöknek nevezzük mod p, ha a mod p vett rendje $p-1$, vagyis ha g hatványaiként a $\mathbb{Z}_p$ minden nem nulla eleme előáll.

4.1. Tétel. *Minden p prímszámra létezik primitív gyök mod p.*

Bizonyítás. A kis-Fermat tétel szerint $\mathbb{Z}_p$ összes eleme gyöke az $x^p - x$ polinomnak. Mivel e polinom foka p, és $\mathbb{Z}_p$-nek is p eleme van, ezért $x^p - x$ gyöktényezők szorzatára bomlik $\mathbb{Z}_p$ felett. De $\Phi_{p-1}(x) \mid x^{p-1} - 1 \mid x^p - x$, ezért $\overline{\Phi_{p-1}}$ is gyöktényezők szorzatára bomlik $\mathbb{Z}_p$ felett. Tehát van egy g gyöke $\mathbb{Z}_p$-ben. A 3.10. Tétel miatt g rendje $p-1$. □

Megjegyezzük, hogy az $x^p - x$ polinom $\mathbb{Z}_p$ feletti gyöktényezős felbontásából a Wilson-tételre is kapható bizonyítás, ha az x-szel való leosztás után a konstans tagot tekintjük. A fenti bizonyítást elemi csoportelméleti ismeretek birtokában könnyen általánosíthatjuk tetszőleges véges testre.

4.2. Gyakorlat. Igazoljuk, hogy minden véges test multiplikatív csoportja ciklikus.

A másik alkalmazás során Dirichlet tételének egy speciális esetét igazoljuk elemi úton. Dirichlet tétele azt mondja ki, hogy ha $a \neq 0$ és b relatív prím egész számok, akkor az $ak+b$ $(k = 1, 2, \dots)$ számtani sorozatban végtelen sok prímszám van. A tétel általános bizonyítása nagyon nehéz, és a bizonyításhoz csoportelméleti, valamint analízisbeli eszközök is kellenek. Ugyanakkor a $b = 1$ speciális eset a körosztási polinomok felhasználásával bebizonyítható egy nagyon szellemes, elemi gondolatmenettel.

A Dirichlet-tétel speciális eseteinek elemi bizonyításai általában indirektek: feltesszük, hogy csak véges sok adott alakú prím van, és felírunk egy olyan kifejezést, ami ezekhez relatív prím, és mégis van egy adott alakú prímosztója. Például a $4k+1$ esetben a lényeg az az észrevétel, hogy a c^2+1 kifejezés minden páratlan prímosztója $4k+1$ alakú, ez teszi lehetővé, hogy „új” $4k+1$ alakú prímet találjunk.

Tegyük most fel, hogy a p páratlan prím osztja a c^4+1 kifejezést. Ekkor $p \nmid c$, és a $c^4 \equiv -1$ (p) kongruencia azt mutatja, hogy (az értelmes) $o_p(c) \nmid 4$ (hiszen $p \neq 2$ miatt $-1 \not\equiv 1$ (p)). Ugyanakkor négyzetre emelve $c^8 \equiv 1$ (p) adódik. Azaz $o_p(c) \mid 8$. Ezért $o_p(c)$ csak 8 lehet, és így $8 = o_p(c) \mid \varphi(p) = p-1$. Vagyis p tényleg $8k+1$ alakú.

4.3. Gyakorlat. Bizonyítsuk be, hogy $c^4 - c^2 + 1$ minden prímosztója $12k+1$ alakú, vagy 12-nek osztója. Vezessük le ebből a Dirichlet-tétel $12k+1$ esetét.

Hogyan lehet ezeket a gondolatmeneteket általánosítani? Vegyük észre, hogy x^2+1 épp a $\Phi_4(x)$ körosztási polinom, ebből jött ki a $4k+1$ eset. Hasonlóan a $8k+1$ eset a $\Phi_8(x) = x^4+1$, a $12k+1$ eset pedig a $\Phi_{12}(x) = x^4 - x^2 + 1$ vizsgálatából jön ki.

4.4. Lemma. *Tegyük fel, hogy a p prím osztja a $\Phi_n(c)$ kifejezést valamilyen c egész számra, de $p \nmid n$. Ekkor a p prím $nk+1$ alakú (azaz $n \mid p-1$).*

Bizonyítás. Mivel $p \mid \Phi_n(c)$, a $\overline{c} \in \mathbb{Z}_p$ gyöke $\overline{\Phi_n} \in \mathbb{Z}_p[x]$-nek. A 3.10. Tétel és $p \nmid n$ miatt tehát $o_p(c) = n$. Ekkor $n = o_p(c) \mid \varphi(p) = p-1$. □

A Dirichlet-tétel $nk+1$ speciális esetét most már könnyen igazolhatjuk a szokásos technikával. Tegyük fel, hogy csak véges sok (esetleg nulla darab) $nk+1$ alakú prím van, ezek legyenek $p_1, \dots, p_s$. Tekintsük a $N = \Phi_n(ntp_1 \dots p_s)$ számot, ahol $t \in \mathbb{Z}$. Persze $N \mid (ntp_1 \dots p_s)^n - 1$, és ezért ha p prímosztója N-nek, akkor $p \nmid n$, és p különbözik a $p_1, \dots, p_s$ mindegyikétől. Az előző lemma miatt a p prím $nk+1$ alakú, azaz „új”, ami ellentmond a $p_1, \dots, p_s$ választásának.

4.5. Kérdés. Készen vagyunk a bizonyítással? Mi a t szám szerepe?

A bizonyítással akkor vagyunk készen, ha az N számnak van prímosztója, azaz $N \neq \pm 1$. Ez valamelyik t-re biztosan bekövetkezik, hiszen egy nem konstans polinom a ± 1 értéket csak véges sok helyen veheti fel (a polinomok azonossági tétele miatt).

4.6. Gyakorlat. Igazoljuk, hogy valójában már $k > 2$ esetén $|\Phi_n(k)| > 1$.

A fenti bizonyítást, bármennyire szép is, nem szabad túlértékelni. Az analitikus módszer sokkal erősebb, mert az $ak + b$ alakú prímszámok számáról is felvilágosítást ad (miként azt láttuk a számtani sorozatok prímszámtételénél).

Megjegyezzük még, hogy Bauer Mihálynak sikerült elemi bizonyítást találnia a Dirichlet-tétel $nk - 1$ speciális esetére. A bizonyítás (melynek vázlata megtalálható Erdős-Surányi: *Válogatott fejezetek a számelméletből* című könyvében) a körosztási polinomok helyett egy másik, de hasonló rekurzióval definiálható polinomsorozatot használ. Található elemi megoldás a $8k+3$ és $8k+5$ sorozatokra is (lásd Szalay Mihály tagozatos gimnáziumi számelmélet tankönyvében a 69. feladatot). Ugyanebben a könyvben a Dirichlet-tétel teljes (analitikus) bizonyítása is megtalálható.

4.7. Gyakorlat. Tegyük fel, hogy be tudjuk látni, hogy tetszőleges $(a, b) = 1$ ($a \geq 2$, b tetszőleges egész) esetén az $ak+b$ ($k = 1, 2, \dots$) számtani sorozatban *van* prímszám. Mutassuk meg, hogy akkor mindegyik ilyen sorozatban végtelen sok prím van.

4.8. Feladat. Mutassuk meg, hogy ha $a, n > 1$ egészek, akkor $n \mid \varphi(a^n - 1)$. Ezt és a φ képletét felhasználva lássuk be a Dirichlet-tételt a $pk + 1$ esetre, ha p prím.

4.9. Feladat. Mely p prímekre és $p \mid n$ egészekre fordulhat elő, hogy $p^2 \mid \Phi_n(c)$ valamilyen c egészre?

4.10. Feladat. Legyenek $m \neq n$ pozitív egészek. Mikor létezik olyan c egész szám, melyre a $\Phi_m(c)$ és a $\Phi_n(c)$ **számok** nem relatív prímek? Mennyi lehet ekkor e két szám legnagyobb közös osztója?

5. A körosztási polinom irreducibilitása

Az alábbi tételnek híres következménye, hogy egy szabályos n-szög akkor és csak akkor szerkeszthető körzővel és vonalzóval, ha $\varphi(n)$ kettő-hatvány.

5.1. Tétel. *Ha $n \geq 1$, akkor az n-edik körosztási polinom irreducibilis $\mathbb{Z}$ és $\mathbb{Q}$ felett.*

A tétel bizonyításához legyen $\Phi_n(x) = f_1(x) \dots f_s(x)$ az n-edik körosztási polinom $\mathbb{Z}[x]$-beli felbontása felbonthatatlanok szorzatára. Mivel Φ_n normált, az f_i polinomok főegyütthatója csak ± 1 lehet. Ezért az f_i polinomok primitívek, és így az ismert tétel szerint irreducibilisek $\mathbb{Q}$ felett is (speciálisan tehát mindegyik legalább elsőfokú). Azt kell megmutatnunk, hogy ebben a felbontásban csak egy polinom szerepel.

5.2. Lemma. *Legyen $p \nmid n$ prím. Ha egy ε számra $f_1(\varepsilon) = 0$, akkor $f_1(\varepsilon^p) = 0$.*

Ha ezt a lemmát belátjuk, akkor a tétel bizonyításával is készen vagyunk. Valóban, mivel f_1 legalább elsőfokú, van egy $\varepsilon \in \mathbb{C}$ gyöke, ami persze Φ_n-nek is gyöke, azaz primitív n-edik egységgyök. Tehát az összes n-edik primitív egységgyök hatványa ε-nak, méghozzá n-hez relatív prím kitevőjű hatványa. Tekintsük az ε^m számot, ahol $(m, n) = 1$. Az m szám felbontható prímek szorzatára: $m = p_1 \ldots p_\ell$, ahol persze $p_j \nmid n$. A lemma miatt ε^{p_1} gyöke f_1-nek. Most alkalmazzuk a lemmát az ε^{p_1} számra és a p_2 prímszámra. Azt kapjuk, hogy $(\varepsilon^{p_1})^{p_2} = \varepsilon^{p_1 p_2}$ is gyöke f_1-nek. A lemmát még $\ell - 2$-szer alkalmazva kapjuk, hogy $\varepsilon^{p_1 \cdots p_\ell} = \varepsilon^m$ is gyöke f_1-nek. Azaz f_1-nek gyöke az összes n-edik primitív egységgyök, és így Φ_n összes gyöktényezője már f_1-ben szerepel. Tehát f_1 a Φ_n felbontásának egyetlen tényezője. Ezzel beláttuk, hogy a tétel tényleg következik a lemmából, és így elég a lemmát bebizonyítani.

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, azaz gyöke Φ_n-nek. Ezért ε^p gyöke valamelyik f_j polinomnak is (ahol $j \neq 1$). Az indexek átszámozásával feltehetjük, hogy $j = 2$. Tehát $f_2(\varepsilon^p) = 0$.

Mivel f_1 irreducibilis $\mathbb{Q}$ felett, az f_1 az ε szám minimálpolinomja (lásd 1.7. Tétel). De ε gyöke az $f_2(x^p)$ polinomnak is, és ezért az 1.7. Tétel miatt $f_1(x) \mid f_2(x^p)$. Ez az oszthatóság $\mathbb{Q}$ felett érvényes, vagyis van olyan $g \in \mathbb{Q}[x]$, melyre $f_1(x)g(x) = f_2(x^p)$. Azonban f_1 főegyütthatója ± 1, ezért amikor a $g(x) = f_2(x^p)/f_1(x)$ osztást elvégezzük, akkor végig $\mathbb{Z}[x]$-ben maradunk. Ezért valójában $g \in \mathbb{Z}[x]$.

Vegyük a szereplő polinomok együtthatóit mod p, és jelölje felülvonás az így kapott polinomokat. Ekkor $\overline{f_1}(x)\overline{g}(x) = \overline{f_2}(x^p)$. A 3.6. Következmény miatt $\overline{f_2}(x^p) = \overline{f_2}(x)^p$. Tehát $\overline{f_1} \mid \overline{f_2}^p$, ahol az oszthatóság $\mathbb{Z}_p[x]$-ben értendő. Mivel f_1 főegyütthatója ± 1, az $\overline{f_1}$ polinom sem konstans. Ez a polinom $\mathbb{Z}_p$ felett nem biztos, hogy irreducibilis, de mindenképpen van egy $\mathbb{Z}_p$ felett irreducibilis k osztója. Ekkor $k \mid \overline{f_1} \mid \overline{f_2}^p$, és mivel az irreducibilis polinomok $\mathbb{Z}_p[x]$-ben prímtulajdonságúak, $k \mid \overline{f_2}$.

Találtunk tehát egy olyan $k \in \mathbb{Z}_p[x]$ nem konstans polinomot, ami $\overline{f_1}$-nak is és $\overline{f_2}$-nak is osztója. Ezért $k^2 \mid \overline{f_1 f_2}$. Viszont $f_1 f_2 \mid \Phi_n$, és $\Phi_n(x) \mid x^n - 1$. Ezért végülis $k^2 \mid \overline{x^n - 1}$. Ez azonban ellentmond a 3.7. Lemmának, ami szerint $p \nmid n$ esetén $x^n - 1$-nek nincs többszörös tényezője mod p. Ezzel a tétel bizonyítását befejeztük. $\square$

5.3. Gyakorlat. Bontsuk az $x^{12} - 1$ polinomot irreducibilisek szorzatára $\mathbb{Z}$, $\mathbb{Z}_2$, $\mathbb{Z}_3$ és $\mathbb{Z}_5$ felett.

A következő feladat megoldásához célszerű ismerni a testbővítések és a véges testek alapvető tulajdonságait. Ezekről tanárszakon általában másodéven esik szó.

5.4. Feladat. Legyen p prímszám, és $p \nmid n$ pozitív egész. Mutassuk meg, hogy Φ_n mod p felbomlik $o_n(p)$ fokú, $\mathbb{Z}_p$ felett irreducibilis polinomok szorzatára.

MEGOLDÁSOK, EREDMÉNYEK

Számolás komplex egységgyökökkel

1.2. A feladat állítása következik a 5.1. Tételből.

1.5. A két esetben két hasonló tulajdonságú halmazt tekintettünk: a „jó" kitevők halmazát (azon kitevőket, amelyekre g-t emelve 1-et kapunk), illetve a „jó" polinomok halmazát (azon polinomokat, melyeknek ε gyöke). Ezek a halmazok mindkét esetben zártak az összeadásra, és az elemek többszörözésére (azaz *ideálok*). Mindkét esetben a halmaz „legkisebb" elemét kerestük meg. Az első esetben a „kicsiség" mértéke a szám abszolút értéke, a másodikban a polinom foka. Mindkét esetben a maradékos osztás biztosította, hogy a halmaz többi eleme a „legkisebb" elem többszöröse. (Haladóbbaknak: mindkét esetben azon múlt a dolog, hogy minden euklideszi gyűrű főideálgyűrű.)

1.6. Tegyük fel, hogy m_1 és m_2 is minimálpolinomja α-nak, azaz mindkettő legalacsonyabb fokú olyan normált polinom, amelynek α gyöke. Ekkor persze a fokuk megegyezik, az $m_1 - m_2$ polinomból tehát kiesik a főegyüttható. Ennek a különbségnek α még mindig gyöke, és ez a fokszám minimalitása miatt csak úgy lehet, hogy $m_1 - m_2 = 0$, vagyis $m_1 = m_2$. Ha nem tennénk fel, hogy a minimálpolinom normált, akkor megfelelően módosított gondolatmenettel azt kapnánk, hogy m_1 és m_2 egymás konstansszorosai, azaz asszociáltak. Ekkor tehát a minimálpolinom csak asszociáltság erejéig lenne egyértelmű. Az, hogy a minimálpolinom asszociáltság erejéig egyértelmű, a 1.7. Tétel első állításából is nyilván következik.

1.8. Mindössze annyi az eltérés, hogy $\mathbb{Q}$ feletti polinomok helyett T felettiekről kell beszélni, és az irreducibilitást is T felett kell feltenni. Ily módon az összes eddigi állítás érvényben marad, ugyanazzal a bizonyítással. Valójában a minimálpolinomnak értelme, és hasonló tulajdonságai vannak, ha egy tetszőleges test feletti egységelemes algebra elemeit tekintjük.

1.9. Tegyük fel, hogy az $\alpha \in \mathbb{C}$ szám m minimálpolinomja előáll két alacsonyabb fokú polinom szorzataként: $m = fg$, ahol $f, g \in \mathbb{Q}[x]$. Ekkor $0 = m(\alpha) = f(\alpha)g(\alpha)$. Mivel $\mathbb{C}$ nullosztómentes, $f(\alpha)$ és $g(\alpha)$ egyike nulla, ami lehetetlen, hiszen m a legalacsonyabb fokú racionális együtthatós, nem nulla polinom, amelynek α gyöke. Az állítás általában is igaz, ha egy nullosztómentes algebra elemeit tekintjük.

1.10. A válaszok rendre $x-1$, $x+1$, x^2+1 ($\pm i$ esetén), x^4+1. Azt kell csak ellenőrizni, hogy a megadott számok gyökei ezeknek a polinomoknak (ez nyilvánvaló), és hogy ezek a polinomok irreducibilisek $\mathbb{Q}$ felett (ami nyilvánvaló a legfeljebb másodfokúak esetén, az x^4+1 polinomra pedig a legegyszerűbb úgy megmutatni, hogy észrevesszük: $(x+1)^4+1$-re teljesül a Schönemann-Eisenstein kritérium).

1.11. Nem. A fentiek szerint azt kell csak ellenőrizni, hogy x^4+1 nem osztója az $x^{10}-3x+4$ polinomnak.

A körosztási polinom kiszámítása

2.1. Azt kell megmutatni, hogy g gyökei a harminchatodrendű számok, és minden gyöktényező egyszer fordul elő. Tegyük fel, hogy η gyöke g-nek, és legyen $m = o(\eta)$. A legutolsó törtből indulunk ki. A számlálóban az $x^{36}-1$ gyökei azok az η számok, melyekre $m \mid 36$. Az x^6-1 szorzó miatt azok az η számok, ahol $m \mid 6$, még egyszer szerepelnek. Ugyanakkor a nevezőben szereplő $x^{18}-1$ és $x^{12}-1$ eltünteti azokat a gyöktényezőket, ahol $m \mid 18$ és $m \mid 12$. A 18 és a 36 közös osztóihoz, azaz a 6 osztóihoz tartozó gyöktényezőket kétszer tüntettük el, de azok a számlálóban is kétszer szerepeltek. Azon m számokhoz tartozó egységgyökök maradtak tehát meg, ahol $m \mid 36$, de $m \nmid 18$ és $m \nmid 12$. Ekkor m csak 36 lehet.

2.3. A harmadik primitív egységgyökök $-1/2 \pm i\sqrt{3}/2$, a hatodikak $1/2 \pm i\sqrt{3}/2$, a tizenkettedikek $\pm\sqrt{3}/2 \pm i/2$. Innen az állítás beszorzással adódik.

2.4. Ha $o(\eta) = 12$, akkor hatványai között négy tizenkettedrendű, két hatodrendű, két negyedrendű, két harmadrendű, egy másodrendű és egy elsőrendű szám van. Az adódik, hogy $\Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_4(x)\Phi_6(x)\Phi_{12}(x) = x^{12}-1$. Az osztás elvégzésekor érdemes a nevezőben minél több tényezőt összevonni, mert ezzel a számolást rövidíthetjük. A 6 osztóihoz tartozó körosztási polinomok szorzata x^6-1, ezért

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

2.6. Tekintsük a $\prod_{d|n}\Phi_d(x) = x^n-1$ képletben a fokszámokat.

2.8. Az eddig még nem említett eredmények a következők. Ha $n = p$ prím, akkor $\Phi_p(x) = 1+x+x^2+\cdots+x^{p-1}$ (lásd a következő feladatot). Ebben a feladatban hasonló képletet kapunk prímhatványokra is, speciálisan $\Phi_8(x) = x^4+1$, $\Phi_{16}(x) = x^8+1$, $\Phi_9(x) = x^6+x^3+1$. Ha n egy páratlan szám kétszerese, akkor is azonnal felírható az eredmény a 2.16. Gyakorlat alapján: $\Phi_{10}(x) = x^4-x^3+x^2-x+1$, $\Phi_{14}(x) = x^6-x^5+x^4-x^3+x^2-x+1$, végül $\Phi_{18}(x) = x^6-x^3+1$. A megmaradt esetek: $\Phi_{15}(x) = x^8-x^7+x^5-x^4+x^3-x+1$, $\Phi_{20}(x) = \Phi_{10}(x^2)$ (lásd a 2.13. Feladatot).

2.9. A rekurziós képlet alapján, ha p prím, akkor

$$\Phi_{p^k}(x) = \frac{x^{p^k}-1}{\Phi_1\Phi_p\dots\Phi_{p^{k-1}}} = \frac{x^{p^k}-1}{x^{p^{k-1}}-1},$$

hiszen a nevezőben szereplő indexek éppen p^{k-1} osztói. Az $y = x^{p^{k-1}}$ helyettesítéssel azonnal látszik, hogy mennyi ennek a törtnek az értéke:

$$\Phi_{p^k}(x) = \frac{y^p-1}{y-1} = 1+y+\dots+y^{p-1} = 1+x^{p^{k-1}}+x^{2p^{k-1}}+\dots+x^{(p-1)p^{k-1}}.$$

2.10. Mivel az 1 nulla darab prím szorzata (üres szorzat), ezért $\mu(1) = (-1)^0 = 1$. Vegyük észre, hogy a bizonyítandó képlet $n = 36$ speciális esete éppen a 2.1. Gyakorlatbeli utolsó tört. Ezért csak az a dolgunk, hogy az ottani gondolatmenetet általánosítsuk. Azt kell belátnunk, hogy a $\prod_{d|n}(x^{n/d}-1)^{\mu(d)}$ képletben $o(\eta) = n$ esetén $x-\eta$ az első hatványon szerepel, egyébként pedig a nulladikon. Legyen $o(\eta) = m$. Ekkor $x^{n/d}-1$-ben $x-\eta$ az első hatványon szerepel, ha $m \mid (n/d)$, egyébként pedig a nulladikon. Persze $m \mid (n/d) \Longleftrightarrow d \mid (n/m)$. Ezért a $\prod_{d|n}(x^{n/d}-1)^{\mu(d)}$ képletben $x-\eta$ kitevője $\sum_{d|(n/m)}\mu(d)$. Azt kell tehát belátnunk, hogy

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

Ez $k = 1$ esetén nyilvánvaló. Tegyük fel, hogy $k > 1$, és legyenek $p_1, \dots, p_s$ a k szám különböző prímosztói. A $\mu(d)$ értéke 0, kivéve ha d különböző prímek szorzata, azaz $p_1 \cdot \ldots \cdot p_s$ egy rész-szorzata. Ha páratlan sok prímet szorzunk össze, akkor $\mu(d) = -1$, ha páros sokat, akkor $\mu(d) = 1$. Vagyis a fenti összeg értéke akkor lesz nulla, ha a $\{p_1, \dots, p_s\}$ halmaznak ugyanannyi páratlan elemű részhalmaza van, mint páros elemű. Ez $s \geq 1$ (vagyis $k > 1$) esetén igaz, hiszen a páros elemszámú részhalmazok száma

$$\binom{s}{0}+\binom{s}{2}+\binom{s}{4}+\dots,$$

a páratlanoké

$$\binom{s}{1}+\binom{s}{3}+\binom{s}{5}+\dots,$$

viszont a binomiális tétel szerint

$$\binom{s}{0}-\binom{s}{1}+\binom{s}{2}-\binom{s}{3}+\binom{s}{4}-\binom{s}{5}+-\dots = (1-1)^s = 0.$$

2.11. Belátjuk, hogy az n-edik primitív egységgyökök összege $\mu(n)$, ahol μ az előző feladatban definiált Möbius-függvény, szorzatuk pedig mindig 1, kivéve az $n = 2$

esetet, amikor -1. Az utóbbi állítást érdemes megpróbálni bebizonyítani úgy is, hogy minden primitív n-edik egységgyököt párosítunk az inverzével (ami szintén primitív n-edik egységgyök). Mi mindkét állítást a gyökök és együtthatók összefüggésének felhasználásával igazoljuk. Ezek alapján ugyanis a primitív n-edik egységgyökök $S(n)$ összege a $\Phi_n(x)$ körosztási polinomban a „felülről második tag”, vagyis az $x^{\varphi(n)-1}$-es tag együtthatójának ellentettje, szorzatuk pedig a konstans tag $(-1)^{\varphi(n)}$-szerese.

A $\prod_{d|n} \Phi_d(x) = x^n - 1$ összefüggésben nézzük meg, mi az x^{n-1} együtthatója a két oldalon. A jobboldalon ez 0, kivéve az $n = 1$ esetet, amikor -1. A másik oldalon x^{n-1}-es tagot csak úgy kaphatunk, ha egy kivételével mindegyik polinomból a legmagasabb fokú tagot vesszük, a kivételesből pedig a második legmagasabb fokút (hiszen $n-1$ csak eggyel kevesebb, mint a szorzatpolinom foka). Mivel $\Phi_d(x)$-ben a második legmagasabb fokú tag együtthatója $-S(d)$, és az összes Φ_d polinom normált, a baloldalon az x^{n-1} együtthatója a $-S(d)$ számok összege lesz. A két oldalt egybevetve tehát beláttuk, hogy

$$\sum_{d|n} S(d) = \begin{cases} 1 & \text{ha } n = 1, \\ 0 & \text{ha } n \neq 1. \end{cases}$$

Ez ugyanaz az összefüggés, amit az előző feladatban igazoltunk S helyett μ-re. Ezért n szerinti indukcióval azonnal látjuk, hogy $S(n) = \mu(n)$. (Ha ugyanis ezt tudjuk már az n-nél kisebb összes d-re, speciálisan n valódi osztóira, akkor a most bizonyított összefüggésben a baloldali összeg egy tag kivételével azonos μ-re és S-re, a jobboldalon pedig ugyanaz a szám áll, és így a hiányzó egy-egy tag is egyenlő.)

A szorzatra vonatkozó összefüggést hasonlóan, de egyszerűbben vezethetjük le. A $\prod_{d|n} \Phi_d(x) = x^n - 1$ összefüggés konstans tagját nézve (azaz nullát helyettesítve) kapjuk, hogy $\prod_{d|n} \Phi_d(0) = -1$, és innen indukcióval azonnal látszik, hogy $\Phi_n(0)$ értéke mindig 1, kivéve $n = 1$-re, amikor -1. Nekünk $(-1)^{\varphi(n)}\Phi_n(0)$ kell, amit könnyen megkaphatunk, hiszen $\varphi(n)$ akkor és csak akkor páros, ha $n > 2$.

2.12. A $\Phi_n(1)$ értéket kell meghatároznunk. Most is rekurzívan számolunk, de a $\prod_{d|n} \Phi_d(x) = x^n - 1$ összefüggésbe közvetlenül 1-et helyettesíteni nem érdemes, hiszen a Φ_1 miatt nullát kapunk. Ezért előbb osszunk le $\Phi_1(x) = x - 1$-gyel. Az eredmény:

$$\prod_{\substack{d|n \\ d\neq 1}} \Phi_d(x) = \frac{x^n - 1}{x - 1} = 1 + x + x^2 + \cdots + x^{n-1}.$$

Felmerül a kérdés, hogy szabad-e az így kapott egyenlőségbe $x = 1$-et helyettesíteni, nem jelentené-e ez azt, hogy az imént $1 - 1 = 0$-val osztottunk? A válasz az, hogy szabad, ugyanis az $x-1$-gyel való osztáskor polinomok osztását végeztük el, nem pedig helyettesítési értékekét, azaz számokét. Az eredmény tehát azonosság, polinomok egyenlősége, azaz a két oldal együtthatóról együtthatóra megegyezik.

A kapott azonosságba 1-et helyettesítve könnyen látható indukcióval, hogy ha n hatványa p-nek, de nem 1, akkor $\Phi_n(1) = p$, ha pedig n nem prímhatvány, akkor $\Phi_n(1) = 1$. Természetesen $n = 1$-re közvetlenül látszik, hogy az eredmény nulla.

2.13. A feladatra két megoldást adunk. Az első nagyon rövid számolás, ami felhasználja a 2.10. Feladatban bizonyított összefüggést. A második bizonyítás hosszabb, de nagyon tanulságos, mert gyakoroljuk általa az elemrend fogalmát.

Az első bizonyításban tehát induljunk ki abból, hogy $\Phi_n(x) = \prod_{d|n}(x^{n/d} - 1)^{\mu(d)}$. Ebben a szorzatban eltekinthetünk azoktól a tényezőktől, amelyekre a $\mu(d)$ kitevő nulla, hiszen ezek értéke 1. Tehát csak azok a $d \mid n$ számok az érdekesek, amelyek csupa különböző prímek szorzatai. Mivel n minden prímosztója osztója m-nek is, az ilyen d számok m-nek is osztói. Ezért

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

(az utolsó lépésben m-re alkalmaztuk a 2.10. Feladatban bizonyított formulát).

A második, közvetlen bizonyításban megmutatjuk, hogy ugyanazok az $x - \eta$ gyöktényezők szerepelnek a képlet mindkét oldalán. Azaz belátjuk, hogy $o(\eta) = n$ akkor és csak akkor, ha $o(\eta^{n/m}) = m$. A hatvány rendjére vonatkozó képlet szerint $o(\eta^{n/m}) = o(\eta)/(o(\eta), n/m)$. Ha $o(\eta) = n$, akkor ez $n/(n, n/m) = n/(n/m) = m$. Megfordítva, tegyük fel, hogy $o(\eta)/(o(\eta), n/m) = m$. Azaz

$$o(\eta) = (o(\eta), n/m)m = (o(\eta)m, n) = (m, n/o(\eta))o(\eta)\,.$$

Itt kétszer használtuk a kitüntetett közös osztó kiemelési tulajdonságát. (A második esetben is szabad ezt megtenni, azaz $o(\eta) \mid n$, hiszen ez már az $o(\eta) = (o(\eta)m, n)$ összefüggésből következik.) Azt kaptuk tehát, hogy $(m, n/o(\eta)) = 1$. Ha az $n/o(\eta)$ számnak lenne egy p prímosztója, akkor persze $p \mid n$, és a feltételünk szerint n prímosztói mind osztják m-et, azaz $p \mid m$, ahonnan a $p \mid (m, n/o(\eta)) = 1$ ellentmondás adódik. Ezért az $n/o(\eta)$ egész számnak nincs prímosztója, vagyis $n/o(\eta) = 1$, ami a kívánt $o(\eta) = n$ állítást bizonyítja.

2.14. Az előző feladat alapján a körosztási polinomokat elég a négyzetmentes esetben ismerni. Ha ugyanis az n szám tetszőleges, és az m az n prímosztóinak a szorzata, akkor m négyzetmentes, és Φ_m ismeretében $\Phi_n(x) = \Phi_m(x^{n/m})$ is kiszámítható. Speciálisan $\Phi_{36}(x) = \Phi_6(x^6) = x^{12} - x^6 + 1$, $\Phi_{72}(x) = \Phi_6(x^{12}) = x^{24} - x^{12} + 1$, $\Phi_{144}(x) = \Phi_6(x^{24}) = x^{48} - x^{24} + 1$, $\Phi_{100}(x) = \Phi_{10}(x^{10}) = x^{40} - x^{30} + x^{20} - x^{10} + 1$ (itt felhasználtuk a 2.8. Gyakorlat eredményét).

2.15. Belátjuk a következőt: ha $n = o(\varepsilon)$ páratlan, akkor $o(-\varepsilon) = 2o(\varepsilon)$. Ha n páros, de néggyel nem osztható, akkor $o(-\varepsilon) = o(\varepsilon)/2$. Végül ha $4 \mid n$, akkor $o(-\varepsilon) = o(\varepsilon)$.

Vegyük először is észre, hogy ha n páros, akkor $\varepsilon^{n/2} = -1$. Valóban, ilyenkor $\varepsilon^{n/2}$ négyzete 1, azaz $\varepsilon^{n/2}$ csak ± 1 lehet, de 1 nem, mert ε rendje $n > n/2$. (Vessük össze ezt az észrevételt azzal a ténnyel, hogy páratlan p prímek esetén a -1 indexe minden primitív gyökre nézve $(p-1)/2)$.

Legyen $o(-\varepsilon)=k$. Ha n páros, akkor $(-\varepsilon)^n=1$, és így $k=o(-\varepsilon)\mid n$. A $(-\varepsilon)^k=1$ összefüggést négyzetre emelve $\varepsilon^{2k}=1$, azaz $n=o(\varepsilon)\mid 2k$, és így $(n/2)\mid k$ adódik. Tehát k vagy $n/2$, vagy n. Az előző bekezdésbeli észrevétel miatt $\varepsilon^{n/2}=-1$, azaz $(-\varepsilon)^{n/2}=-(-1)^{n/2}$. Ez pontosan akkor 1, ha $n/2$ páratlan szám. Ilyenkor tehát $k=n/2$. Ha viszont $n/2$ páros, akkor $k\nmid(n/2)$, és ezért $k=n$.

Végül tegyük fel, hogy n páratlan. Ebben az esetben is célhoz érhetünk a fentihez hasonló gondolatmenettel (gyakorlásképpen ezt érdemes megkeresni). Gondolkozhatunk azonban a következőképpen is. Legyen η egy $2n$-edik primitív egységgyök. A már bizonyított állítás szerint $o(-\eta)=(2n)/2=n$. De $\varphi(2n)=\varphi(n)$ miatt a $2n$-edik és az n-edik primitív egységgyökök száma ugyanannyi. Ezért $-\eta$ alakban (e számok nyilván páronként különbözők) megkapunk minden n-edik egységgyököt. Azaz ha $\varepsilon=-\eta$, akkor $o(-\varepsilon)=o(\eta)=2n$.

2.16. Az előző feladat megoldásában már beláttuk, hogy ha n páratlan, akkor a $2n$-edik primitív egységgyökök éppen az n-edik primitív egységgyökök ellentettjei. Ezért

$$\Phi_{2n}(x)=\prod_{o(\eta)=2n}(x-\eta)=\prod_{o(\varepsilon)=n}(x+\varepsilon)=(-1)^{\varphi(n)}\prod_{o(\varepsilon)=n}(-x-\varepsilon)=(-1)^{\varphi(n)}\Phi_n(-x)\,.$$

2.17. Eljárhatnánk a 2.12. Feladat megoldásában használt módon is, csak most $\Phi_2(x)=x+1$-gyel kell leosztani a rekurziót páros n esetén. Ennél egyszerűbb azonban, ha ennek a feladatnak az *eredményére* vezetjük vissza az állítást. Ha $n=4m$, akkor a 2.13. Feladat miatt $\Phi_n(x)=\Phi_{2m}(x^2)$, és így $\Phi_n(-1)=\Phi_{2m}(1)$, ami 2, ha m kettő-hatvány, különben 1. Ha n nem osztható néggyel, akkor a 2.16. Gyakorlat miatt páratlan $n>1$ esetén az eredmény $\Phi_{2n}(1)=1$, ha viszont $n=2k>2$, akkor $\Phi_n(-1)=\Phi_k(1)$. A fennmaradó „kis” eseteket kézzel kiszámolhatjuk. A végeredmény a következő: $\Phi_1(-1)=-2$, $\Phi_2(-1)=0$, $\Phi_n(-1)=2$, ha $n>2$ kettő-hatvány, $\Phi_n(-1)=p$, ha $n=2p^k>2$ (p prím), a többi esetben az eredmény 1.

2.18. Tegyük fel, hogy $o(\eta)=m$ és $o(\varepsilon)=n$, ahol $(m,n)=1$. Legyen $o(\eta\varepsilon)=k$, ekkor $(\eta\varepsilon)^k=1$. Ezt m-edik hatványra emelve $\eta^m=1$ miatt $\varepsilon^{km}=1$ adódik, tehát $n=o(\varepsilon)\mid km$. Mivel $(m,n)=1$, ezért ebből $n\mid k$ következik. Hasonlóan (de n-edik hatványra emeléssel) adódik, hogy $m\mid k$. Mivel $(m,n)=1$, ezért $mn\mid k$. Viszont nyilván $(\eta\varepsilon)^{mn}=1$, és így $k\mid mn$. Ezért $k=mn$.

Ez a bizonyítás szó szerint elmondható akkor is, ha η és ε egy csoport **felcserélhető** elemei, azaz $\varepsilon\eta=\eta\varepsilon$. Általában az állítás nem igaz, például ha vesszük a sík egybevágósági transzformációit az összetett transzformáció képzésére, mint műveletre nézve, akkor az origó körüli 120 fokos forgatás rendje 3, az x-tengelyre való tükrözés rendje 2. E két transzformáció bármilyen sorrendben vett kompozíciója tengelyes tükrözés, és ezért másodrendű.

2.19. Legyen θ egy mn-edik primitív egységgyök. Az $nx+my=1$ lineáris diofantikus egyenlet megoldható, mert m és n relatív prímek. Ekkor $\theta=\theta^{nx+my}=\theta^{nx}\theta^{my}$. A hatvány rendjének képlete szerint $o(\theta^{nx})=mn/(mn,nx)$. Nyilván $(mn,nx)=n(m,x)$, és az $nx+my=1$ összefüggés miatt $(m,x)=1$. Ezért $o(\theta^{nx})=m$. Hasonlóan $o(\theta^{my})=n$. Ezért θ tényleg előáll egy primitív m-edik és egy primitív n-edik egységgyök szorzataként.

Most belátjuk, hogy ez az előállítás egyértelmű. Tegyük fel, hogy $o(\eta)=o(\eta')=m$ és $o(\varepsilon)=o(\varepsilon')=n$. Ha $\eta\varepsilon=\eta'\varepsilon'$, akkor innen $\eta/\eta'=\varepsilon'/\varepsilon$. A baloldalon egy m-edik, a jobboldalon egy n-edik egységgyök van, azaz a baloldal rendje m-nek, a jobboldalé n-nek osztója. Mivel $(m,n)=1$, ez csak úgy lehet, hogy az egyenlőség mindkét oldalán 1 áll, azaz $\eta=\eta'$ és $\varepsilon=\varepsilon'$.

Az Euler-függvény multiplikativitásának bizonyításához tekintsük az összes $\eta\varepsilon$ szorzatot, ahol $o(\eta)=m$ és $o(\varepsilon)=n$. Az előző bekezdésben bizonyított állítás szerint az ilyen szorzatok száma $\varphi(m)\varphi(n)$. Az előző feladat szerint az így kapott $\eta\varepsilon$ szorzatok mind mn rendű számok, és az első bekezdés szerint minden mn rendű szám előáll egy ilyen szorzatként. Ezért ezek a szorzatok éppen az mn-edik primitív egységgyököket adják, és így számuk $\varphi(mn)$.

2.20. Az előző feladat szerint

$$\Phi_{mn}(x)=\prod_{o(\eta)=m,\ o(\varepsilon)=n}(x-\eta\varepsilon)=\left(\prod_{o(\eta)=m}\eta\right)^{\varphi(n)}\prod_{o(\eta)=m,\ o(\varepsilon)=n}(x/\eta-\varepsilon)\,.$$

A zárójelben álló szorzat a 2.11. Feladat miatt 1, kivéve az $m=2$ esetet, amikor -1, ez adja a minusz előjelet az $m=2$, $n=1$ esetben. Csoportosítsunk η szerint:

$$\prod_{o(\eta)=m,\ o(\varepsilon)=n}(x/\eta-\varepsilon)=\prod_{o(\eta)=m}\left(\prod_{o(\varepsilon)=n}(x/\eta-\varepsilon)\right)=\prod_{o(\eta)=m}\Phi_n(x/\eta)\,.$$

Tudjuk, hogy ha η befutja az m-edik primitív egységgyököket, akkor $1/\eta$ is, és ezért ha x/η helyett ηx-et írunk, azzal csak a tényezők sorrendjét változtatjuk.

2.21. Még a primitív

```
with(numtheory):
for n from 3 by 2 do
  if issqrfree(n) and not isprime(n) then
    s := coeffs(cyclotomic(n,x));
    for i in s do
      if i > 4 or i < -4 then
        print(n, sort(cyclotomic(n,x)));
        break
      fi
    od
  fi
od;
```

`MAPLE`-program is húsz másodperc alatt kiszámolja (egy 200 MHz-es Pentiumos gépen, `LINUX` operációs rendszer alatt), hogy a legkisebb n az $1785 = 3 \cdot 5 \cdot 7 \cdot 17$, melyre Φ_n-ben van legalább 5 abszolút értékű együttható. Az $n = 385 = 5 \cdot 7 \cdot 11$ a legkisebb olyan érték, melyre Φ_n-ben előfordul legalább 3 abszolút értékű együttható, és $n = 1365 = 3 \cdot 5 \cdot 7 \cdot 13$ esetén fordul elő először legalább 4 abszolút értékű együttható.

A körosztási polinom $\mathbb{Z}_p$ felett

3.1. A $+_m$ összeadás definíciója szerint $u +_m v$ az $u + v$ szám m-mel való osztási maradéka, vagyis $\overline{u+v}$, és ezért $u +_m v \equiv u + v\ (m)$. Először belátjuk, hogy $a, b \in \mathbb{Z}$ esetén $\overline{a+b} = \overline{a} +_m \overline{b}$. Mivel $\overline{a} \equiv a\ (m)$, $\overline{b} \equiv b\ (m)$, és $\overline{a} +_m \overline{b} \equiv \overline{a} + \overline{b}\ (m)$, ezért $\overline{a} +_m \overline{b} \equiv \overline{a} + \overline{b} \equiv a + b \equiv \overline{a+b}\ (m)$. Tehát a 0 és $m-1$ közötti $\overline{a} +_m \overline{b}$ és $\overline{a+b}$ számok kongruensek egymással modulo m, és így egyenlőek. Hasonlóan igazolható az $\overline{a \cdot b} = \overline{a} \cdot_m \overline{b}$ összefüggés is.

3.2. Legyen $f(x) = \sum_{i=0}^{n} a_i x^i$ és $g(x) = \sum_{j=0}^{m} b_j x^j$. Tudjuk, hogy fg-ben az x^k együtthatója

$$a_0 b_k + a_1 b_{k-1} + \cdots + a_k b_0\,,$$

(azzal a konvencióval, hogy $a_i = 0$ ha $i > n$ és $b_j = 0$ ha $j > m$). Ezért az x^k együtthatója $\overline{fg}$-ban

$$\overline{a_0 b_k + a_1 b_{k-1} + \cdots + a_k b_0}\,.$$

A definíció szerint $\overline{f}(x) = \sum_{i=0}^{n} \overline{a_i} x^i$ és $\overline{g}(x) = \sum_{j=0}^{m} \overline{b_j} x^j$. Ezért az $\overline{f} \cdot_m \overline{g}$ ($\mathbb{Z}_m[x]$-ben értelmezett) szorzatban az x^k együtthatója

$$\overline{a_0} \cdot_m \overline{b_k} +_m \overline{a_1} \cdot_m \overline{b_{k-1}} +_m \cdots +_m \overline{a_k} \cdot_m \overline{b_0}\,.$$

Az utolsó két kiemelt képlet pedig tényleg egyenlő, hiszen az előző gyakorlatban beláttuk, hogy a felülvonás egész számokra összeg- és szorzattartó. Az $\overline{f+g} = \overline{f} +_m \overline{g}$ képlet hasonló, de sokkal egyszerűbb számolással látható be.

3.4. A binomiális tétel bizonyításakor kifejtjük az $(r+s)^n$ hatványt, és az eredmény egy összeg lesz, amelynek tagjai r és s tényezőjű szorzatok. Ezt a kifejtést megtehetjük általános gyűrűben is. Ha a gyűrű kommutatív, akkor a kapott szorzatokat $r^j s^{n-j}$ alakban írhatjuk. Az a kombinatorikus leszámlálás, miszerint ilyen tagból $\binom{n}{j}$ darab van, szintén minden gyűrűben ugyanaz. Tehát a binomiális tétel tetszőleges kommutatív gyűrűben érvényes marad. A bizonyításból azt is látjuk, hogy az $\binom{n}{j} r^j s^{n-j}$ jelentése: adjuk össze $r^j s^{n-j}$-t $\binom{n}{j}$ példányban. Ez tehát értelmes dolog.

3.5. Ha kéttagú összeget szabad tagonként p-edik hatványra emelni, akkor több tagút is (akinek ez nem nyilvánvaló, az a tagok száma szerinti indukcióval bizonyíthatja).

Ezért $\mathbb{Z}_p$-ben

$$(1+1+\cdots+1)^p = 1^p + 1^p + \cdots + 1^p = 1+1+\cdots+1\,.$$

Mivel $\mathbb{Z}_p$ minden eleme $1+1+\cdots+1$ alakú, minden $u \in \mathbb{Z}_p$ esetén $u^p = u$ (itt a hatványozás persze mod p műveletet jelent). Ha $a \in \mathbb{Z}$, akkor felülvonással jelölve a mod p maradékképzést, a 3.1. Gyakorlat szerint $\overline{a^p} = \overline{a}^p$ (itt a baloldalon $\mathbb{Z}$-beli, a jobboldalon $\mathbb{Z}_p$-beli hatványozás szerepel). Már láttuk, hogy $\overline{a}^p = \overline{a}$. Ezért $\overline{a^p} = \overline{a}$, ami azzal ekvivalens, hogy $p \mid a^p - a$, vagyis $a^p \equiv a\ (p)$.

3.8. A válasz ugyanaz, mint az 3.4. Kérdés esetében. Ha n nemnegatív egész szám, és t eleme egy tetszőleges T testnek, akkor $nt = t+t+\cdots+t$, ahol az összegnek n tagja van. (Speciálisan $n=0$ esetén az üres összeget kapjuk, melynek értéke t nulleleme.) Például ha $T = \mathbb{Z}_p$, akkor az x^n deriváltja $\overline{n}x^{n-1}$-nel lesz egyenlő, ahol $\overline{n}$ az n szám p-vel való osztási maradéka, és itt $\overline{n}$ eleme $\mathbb{Z}_p$-nek.

3.9. Tegyük fel, hogy n a legkisebb ellenpélda az állításra. Végig mod p számolunk (de nem írjuk ki a felülvonásokat). Tekintsük a $\prod_{d|n} \Phi_d(x) = x^n - 1$ összefüggést. A d szám egyértelműen felírható $d = p^j m'$ alakban, ahol $0 \le j \le k$ és $m' \mid m$. Az indukciós feltevés szerint $d < m$ esetén teljesül $\mathbb{Z}_p$ felett, hogy $\Phi_d = \Phi_{m'}^{\varphi(p^j)}$. Gyűjtsük össze rögzített m' mellett ezeket a tényezőket. Az eredmény

$$\Phi_{m'}^{\varphi(p^0)+\varphi(p^1)+\cdots+\varphi(p^k)} = \Phi_{m'}^{p^k}$$

(a kitevőben a 2.6. Gyakorlatban bizonyított $\sum_{d|p^k} \varphi(d) = p^k$ összefüggést használtuk). A fentieket összeszorozva, és felhasználva, hogy $\prod_{m'|m} \Phi_{m'}(x) = x^m - 1$,

$$\prod_{d|n} \Phi_d(x) = \left(\prod_{m'|m} \Phi_{m'}(x) \right)^{p^k} = (x^m - 1)^{p^k} = x^{mp^k} - 1 = x^n - 1$$

adódik (hiszen mod p szabad tagonként p^k-adik hatványra emelni). De **csaltunk,** mert felhasználtuk a $\Phi_d = \Phi_{m'}^{\varphi(p^j)}$ összefüggést a $d = n$ esetben is, márpedig pont ezt kellene belátni. Ezt kikompenzálva, immár helyesen számolva az jön ki, hogy

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

Felhasználva, hogy $\prod_{d|n} \Phi_d(x) = x^n - 1$, azt kapjuk, hogy a baloldali tört értéke 1, vagyis $\Phi_n(x) = \Phi_m(x)^{\varphi(p^k)}$, amit bizonyítani kellett.

Valamivel talán egyszerűbb a számolás, ha a fenti módszerrel csak az $n = pm$ esetet intézzük el, majd alkalmazzuk a 2.13. Feladatot.

3.11. A 2.9. Gyakorlat képlete alapján

$$\Phi_{p^k}(x) = \frac{x^{p^k} - 1}{x^{p^{k-1}} - 1} = 1 + x^{p^{k-1}} + x^{2p^{k-1}} + \cdots + x^{(p-1)p^{k-1}}\,.$$

Ezért $\Phi_{p^k}(x+1)$ konstans tagja az $x=0$ helyen vett helyettesítési érték, vagyis p. Továbbá $\mathbb{Z}_p[x]$-ben számolva

$$\Phi_{p^k}(x+1) = \frac{(x+1)^{p^k}-1}{(x+1)^{p^{k-1}}-1} = \frac{x^{p^k}+1-1}{x^{p^{k-1}}+1-1} = x^{p^k-p^{k-1}}.$$

Ez $\mathbb{Z}$-ben azt jelenti, hogy $\Phi_{p^k}(x+1)$ minden együtthatója osztható p-vel, kivéve a főegyütthatót. A Schönemann-Eisenstein kritérium tehát teljesül, és így Φ_n irreducibilis $\mathbb{Q}$ felett, ha n prímhatvány.

3.12. A 3.11. és 2.16. Gyakorlatok alapján látjuk, hogy prímhatványra és páratlan prímhatvány kétszeresére a körosztási polinom egy eltoltja tényleg teljesíti a Schönemann-Eisenstein kritérium feltételét. Megfordítva, tegyük fel, hogy $\Phi_n(x+c)$ a p prímre teljesíti a kritériumot. Áttérve $\mathbb{Z}_p$-re azt kapjuk, hogy $\overline{\Phi_n}(x+\overline{c}) = x^{\varphi(n)}$, hiszen a főegyüttható kivételével minden együttható eltűnik mod p. Ebbe az azonosságba $y = x - \overline{c}$-t írva adódik, hogy $\overline{\Phi_n}(y) = (y-\overline{c})^{\varphi(n)}$.

Legyen $n = p^k m$, ahol már $p \nmid n$. A 3.9. Feladat szerint $\overline{\Phi_n}(y) = \overline{\Phi_m}(y)^{\varphi(p^k)}$, és így

$$\overline{\Phi_m}(y) = (y-\overline{c})^{\frac{\varphi(n)}{\varphi(p^k)}} = (y-\overline{c})^{\varphi(m)}.$$

De $\Phi_m(y) \mid y^m - 1$, és $p \nmid m$ (valamint a 3.7. Lemma) miatt tudjuk, hogy az $y^m - 1$ polinomnak nincs többszörös tényezője mod p. Ezért $\varphi(m) = 1$, azaz $m = 1$ vagy 2.

3.13. Ha T karakterisztikája nulla, azaz prímteste izomorf $\mathbb{Q}$-val, akkor a szokásos körosztási polinomokat kapjuk (hiszen $\mathbb{Q}$-ból soha nem kell kilépnünk, amikor kiszámítjuk őket). Ha viszont T karakterisztikája a p prím, akkor a prímtest a $\mathbb{Z}_p$-vel izomorf, és a mod p vett Φ_n polinomok nyilván kielégítik a rekurziós képletet.

3.14. A bizonyítás szó szerint ugyanaz, mint a $\mathbb{Z}_p$ esetén, csak a felhasznált 3.7. Lemmát is általánosítani kell T-re. Az általánosítás azt mondja ki, hogy a T test felett az $x^n - 1$ polinomnak akkor és csak akkor van többszörös tényezője, ha a T test karakterisztikája egy n-et osztó prímszám. Ennek a bizonyítása is ugyanaz (deriválással), mint $\mathbb{Z}_p$ esetén.

3.15. Ha f-nek lenne többszörös gyöke egy $\mathbb{Z}_p$-t tartalmazó testben, akkor f-nek és f' deriváltjának az (f, f') kitüntetett közös osztója nem konstans. Ez a kitüntetett közös osztó ugyanaz $\mathbb{Z}_p$-ben és abban a bővebb testben, hiszen az euklideszi algoritmus elvégzésekor $\mathbb{Z}_p$-ben maradunk. Mivel f irreducibilis $\mathbb{Z}_p$ felett, $(f, f') \mid f$, és (f, f') nem konstans, csak az lehet, hogy (f, f') asszociáltja f-nek, azaz $f \sim (f, f') \mid f'$. Az f viszont nem oszthatja a saját deriváltját, hiszen f' az f-nél alacsonyabb fokú, *kivéve ha a deriváltnak nincs foka,* azaz $f' = 0$. Az $(x^n)' = nx^{n-1}$ akkor lesz nulla $\mathbb{Z}_p$-ben, ha $p \mid n$ (lásd a 3.8. Kérdésre adott választ). Ezért $f' = 0$ azt jelenti, hogy az f polinomban csupa p-vel osztható kitevőjű tagok vannak, azaz $f(x) = g(x^p)$ alkalmas $g \in \mathbb{Z}_p[x]$-re. A 3.6. Következmény miatt ekkor $f(x) = g(x)^p$, ami ellentmond annak, hogy f irreducibilis $\mathbb{Z}_p$ fölött (akár konstans a g, akár nem).

Két számelméleti alkalmazás

4.2. A T multiplikatív csoportjára alkalmazzuk Lagrange tételét. Azt kapjuk, hogy minden elem rendje osztja a csoport rendjét, vagyis az $x^{|T|-1}-1$ polinomnak T minden nem nulla eleme gyöke. Innen a bizonyítás ugyanaz, mint $\mathbb{Z}_p$-re, csak a 3.14. Gyakorlat eredményét kell alkalmazni $n = |T| - 1$-re.

4.3. Tegyük fel, hogy $p \nmid 12$, és $p \mid c^4 - c^2 + 1$. Most is azt fogjuk belátni, hogy $o_p(c) = 12$, hiszen ebből $12 \mid \varphi(p) = p - 1$ következik. Kiindulunk a

$$\begin{aligned} c^{12} - 1 = {}& \Phi_1(c) \quad \Phi_2(c) \qquad \Phi_3(c) \qquad \Phi_4(c) \qquad \Phi_6(c) \qquad \Phi_{12}(c) \quad = \\ & (c-1)(c+1)(c^2+c+1)(c^2+1)(c^2-c+1)(c^4-c^2+1) \end{aligned}$$

felbontásból. A jobboldalt osztja a p, és ezért a baloldalt is, vagyis $c^{12} \equiv 1 \ (p)$, ahonnan $o_p(c) \mid 12$ következik (és az, hogy $o_p(c)$ értelmes). Meg kell még mutatni, hogy $o_p(c)$ nem valódi osztója a 12-nek, vagyis nem osztója sem a 6-nak, sem a 4-nek (hiszen ezek a 12 maximális osztói). Ha $c^4 \equiv 1 \ (p)$ lenne, akkor $0 \equiv c^4 - c^2 + 1 \equiv 2 - c^2 \ (p)$ teljesülne, de akkor $1 \equiv c^4 = (c^2)^2 \equiv 2^2 = 4 \ (p)$, azaz $p \mid 3$, amit kizártunk. Ha viszont $p \mid c^6 - 1$ állna fenn, akkor $p \mid (c^4 - c^2 + 1)(c^2 + 1) = c^6 + 1$ miatt $p \mid (c^6 + 1) - (c^6 - 1) = 2$, és ezt is kizártuk.

A bizonyítást befejeztük, de joggal zavarhat minket annak „ad-hoc" jellege: ezeket a trükkös számolásokat nem sok esélyünk van tetszőleges n-re általánosítani, és az is valahogy „véletlenszerűen" jött ki, hogy $p = 2$ vagy 3. Ahhoz, hogy egy általánosítható bizonyítást találjunk, tekintsük a $\Phi_{12}(x+c) = (x+c)^4 - (x+c)^2 + 1$ polinomot. Ennek konstans tagja, azaz $\Phi_{12}(c)$ osztható p-vel. Tegyük fel, hogy a fenti szorzatban még egy másik tényező is osztható p-vel. Ezt jelölje $\Phi_m(c)$, ahol tehát $m \in \{1, 2, 3, 4, 6\}$. Ekkor $\Phi_m(x + c)$ konstans tagja is osztható p-vel.

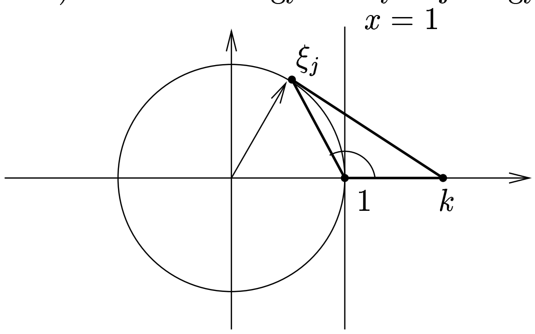
Ha ezt a két polinomot összeszorozzuk, akkor a konstans tagjuk már p^2-tel is osztható lesz, de nekünk nem ez a fontos, hanem az, hogy a szorzatban *az x-es tag együtthatója p-vel osztható!* Ez számolással ellenőrizhető. Ha azonban valaki hajlandó $\mathbb{Z}_p$ felett gondolkodni, akkor számolnia sem kell: ha egy polinom konstans tagja p-vel osztható, akkor a polinom $\mathbb{Z}_p$ felett osztható x-szel, és így két ilyen polinom szorzata már x^2-tel is osztható lesz, azaz nem lesz benne x-es tag sem mod p. Természetesen ez a tulajdonság megmarad akkor is, ha e két polinom szorzatát további, tetszőleges polinomokkal szorozzuk.

De tudjuk, hogy $\Phi_{12}(x + c)\Phi_m(x + c) \mid (x + c)^{12} - 1$. Márpedig a binomiális tételből azonnal látszik, hogy ebben az x-es tag együtthatója $12c^{11}$, ami nem lehet p-vel osztható, hiszen feltettük, hogy $p \nmid 12$, és tudjuk azt is, hogy $p \mid c^{12} - 1$, azaz $p \nmid c$. Ezzel az ellentmondással az új bizonyítást is befejeztük, és ez már általánosíthatónak tűnik, például meg van magyarázva, hogyan jön be a $p \mid 12$. Az „igazi" gondolatmenet természetesen a 3.10. Tétel bizonyítása (ahol a binomiális tétel helyett deriválást alkalmaztunk).

4.6. Legyen $k > 2$ valós szám. Ekkor $\Phi_n(k) = (k - \xi_1) \cdot \ldots \cdot (k - \xi_r)$, ahol $\xi_1, \ldots, \xi_r$ az összes primitív n-edik komplex egységgyök. Ezért

$$|\Phi_n(k)| = |k - \xi_1| \cdot \ldots \cdot |k - \xi_r|\,.$$

A ξ_j szám az $x = 1$ függőleges egyenestől balra helyezkedik el, és ezért a $k\xi_j 1$ háromszögben az 1-nél tompaszög van. A tompaszöggel szemközti oldal nagyobb, mint a másik kettő bármelyike, és ezért $|k - \xi_j| \geq |k - 1| = k - 1 > 1$. Természetesen a $|k - \xi_j| > 1$ egyenlőtlenség akkor is igaz, ha a háromszög elfajuló, azaz $\xi_j = \pm 1$. Ezért a fenti (nem üres) szorzat mindegyik tényezője nagyobb, mint 1.



4.7. Tegyük fel, hogy véges sok $ak + b$ alakú prím van, legyenek ezek $p_1, \ldots, p_s$. Válasszuk az n kitevőt olyan nagyra, hogy $a^n + b$ már nagyobb legyen, mint $p_1, \ldots, p_s$ mindegyike, és tekintsük az $a^n k + b$ sorozatot. Itt $(a^n, b) = 1$, és így feltevésünk szerint van legalább egy prím ebben a sorozatban. Ez nyilván $ak + b$ alakú is, és nagyobb, mint a $p_1, \ldots, p_s$ bármelyike, ami ellentmondás.

4.8. Nyilván $a^n - 1 \nmid a^k - 1$, ha $k < n$ (hiszen ekkor $a^n - 1 > a^k - 1$), de persze $a^n - 1 \mid a^n - 1$. Vagyis n a legkisebb olyan pozitív k szám, melyre $a^k \equiv 1 \ (a^n - 1)$. Ezért $o_{a^n - 1}(a)$ értelmes, és értéke n. Az Euler-Fermat tétel miatt tehát $n \mid \varphi(a^n - 1)$.

Tegyük fel, hogy csak véges sok $kp + 1$ alakú prím van, legyenek ezek $p_1, \ldots, p_s$. Tekintsük a $N = (pp_1 \ldots p_s)^p - 1$ számot. Az előző bekezdésben bizonyított állítás miatt $p \mid \varphi(N)$. Az Euler-függvény képletéből következően tehát az N számnak van olyan q prímosztója, hogy $p = q$ vagy $p \mid q - 1$. Mivel N nyilván relatív prím a p-hez, és a p_j számokhoz is, ezért $q \neq p$ és mindegyik j-re $q \neq p_j$. Így $p \mid q - 1$, azaz q egy „új” $kp + 1$ alakú prím. Ez az ellentmondás bizonyítja az állítást.

4.9. Csak akkor, ha $p = 2$ és $n = 2$, ekkor például $c = 3$ jó. Tegyük fel, hogy $p^2 \mid \Phi_n(c)$, ahol $n = pm$. A rekurziós képlet miatt $\Phi_{pm}(x) \mid (x^{pm} - 1)/(x^m - 1)$, és így $\mathbb{Z}_p$ felett

$$\Phi_{pm}(x) \;\Big|\; \frac{x^{pm} - 1}{x^m - 1} = \frac{(x^m - 1)^p}{x^m - 1} = (x^m - 1)^{p-1}\,.$$

Ide $\overline{c}$-t helyettesítve azt kapjuk, hogy $p \mid (c^m - 1)^{p-1}$, azaz c^m felírható $ap + 1$ alakban, ahol $a \in \mathbb{Z}$. Ezt behelyettesítve, a binomiális tétel szerint (immár $\mathbb{Z}$-ben számolva,

$c^m \neq 1$ azaz $c \neq \pm 1$ esetén)

$$\frac{c^{pm}-1}{c^m-1} = \frac{\left(\sum\limits_{j=0}^{p}\binom{p}{j}(ap)^j\right)-1}{ap+1-1} =$$
$$= (ap)^{p-1} + \binom{p}{p-1}(ap)^{p-2} + \cdots + \binom{p}{2}ap + \binom{p}{1},$$

hiszen az 1 a számlálóban is kiesik. Ha $p > 2$, akkor az itt fellépő tagok mindegyike osztható p^2-tel, kivéve az utolsót, hiszen ekkor $p \mid \binom{p}{2}$, és $\binom{p}{1} = p$. Ez ellentmondás, mert az összegről tudjuk, hogy osztható p^2-tel.

A $p = 2$ esetben azt tudjuk, hogy $4 \mid \Phi_n(c)$. Ha c páros, akkor $\Phi_n(c) \mid c^n - 1$ páratlan szám, ez nem lehet. Ha viszont c páratlan, akkor $c \equiv \pm 1$ (4), és így $4 \mid \Phi_n(1)$, vagy $4 \mid \Phi_n(-1)$. Tehát mindenképpen a $c = \pm 1$ esetet kell már csak elintéznünk (tetszőleges p-re). A 2.12. és 2.17. Feladatok szerint $\Phi_n(\pm 1)$ értéke prímszám, vagy ± 1, tehát nem osztható p^2-tel, kivéve a $\Phi_1(1) = \Phi_2(-1) = 0$ eseteket. Mivel $p \mid n$, nekünk csak a $p = n = 2$ felel meg.

4.10. Ilyen c szám csak nagyon ritkán létezik, általában $(\Phi_m(c), \Phi_n(c)) = 1$. Belátjuk, hogy ez a legnagyobb közös osztó, ha nem 1, akkor csak egy p prímszám lehet, és ilyenkor m és n csak a p egy hatványában különbözhet (speciálisan tehát valamelyik osztható p-vel). Pontosabban, $m = p^\alpha k$, $n = p^\beta k$ alakban írható alkalmas $\alpha, \beta \geq 0$ és $k \geq 1$ egészekkel, ahol még $k \mid p - 1$ is teljesül. Megfordítva, az ilyen alakú m és n számokhoz mindig létezik a kívánt c.

Tegyük fel először, hogy $(\Phi_m(c), \Phi_n(c)) \neq 1$. Ekkor van olyan p prímszám, ami a $\Phi_m(c)$, $\Phi_n(c)$ számokat osztja. Legyen $m = p^\alpha k$, $n = p^\beta \ell$, ahol már $p \nmid k$ és $p \nmid \ell$ (itt α és β elvileg nulla is lehet). A 3.9. Feladat miatt $\mathbb{Z}_p$ felett $\Phi_n = \Phi_k^{\varphi(p^\alpha)}$, és ezért $p \mid \Phi_k(c)$. A 3.10. Tétel miatt tehát $o_p(c) = k$ (és innen $k \mid p-1$). Ugyanígy $o_p(c) = \ell$, tehát $k = \ell$.

Megfordítva, tegyük fel, hogy m és n ilyen alakban írható. Legyen c egy olyan egész szám, melyre $o_p(c) = k$. Ilyen szám létezik: ha g primitív gyök mod p, akkor $g^{(p-1)/k}$ megfelelő. A 3.10. Tétel miatt $\bar{c}$ gyöke $\mathbb{Z}_p[x]$-ben $\Phi_k(x)$-nek. Az előző bekezdésben írtak miatt tehát $p \mid (\Phi_m(c), \Phi_n(c))$.

Hátra van még annak bizonyítása, hogy $(\Phi_m(c), \Phi_n(c))$ értéke, ha nem 1, akkor prímszám. Tegyük fel, hogy van egy közös p prímosztó. Ez egyértelműen meghatározott, hiszen m és n kanonikus alakjában csak egy kitevőben van eltérés. Azt kell megmutatni, hogy p^2 nem közös osztó. Ha az lenne, akkor a 4.9. Feladat miatt $p = 2$, és az n, m számok közül amelyik páros, az kettővel egyenlő. Ezért csak az lehet, hogy n és m egyike kettő, a másik 1. Azaz $4 \mid (\Phi_1(c), \Phi_2(c)) = (c-1, c+1)$, ami lehetetlen.

A körosztási polinom irreducibilitása

5.3. $\mathbb{Z}$ felett a körosztási polinomok az irreducibilis tényezők:

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

A $\mathbb{Z}_2$ felett ez tovább bomlik a következőképpen:

$$\Phi_4(x) = (x+1)^2\,, \quad \Phi_{12}(x) = (x^2+x+1)^2\,,$$

azaz $x^{12} - 1 = (x+1)^4(x^2+x+1)^4$. A $\mathbb{Z}_3$ felett

$$\Phi_3(x) = (x-1)^2\,, \quad \Phi_6(x) = (x+1)^2\,, \quad \Phi_{12}(x) = (x^2+1)^2\,,$$

azaz $x^{12} - 1 = (x-1)^3(x+1)^3(x^2+1)^3$ (az x^2+1 irreducibilis $\mathbb{Z}_3$ felett, hiszen másodfokú, és nincs gyöke $\mathbb{Z}_3$-ban). Végül $\mathbb{Z}_5$ felett

$$\Phi_4(x) = (x-2)(x+2)\,, \quad \Phi_{12}(x) = (x^2+2x-1)(x^2-2x-1)\,.$$

A kapott eredményeket érdemes összevetni a 3.9. és 5.4. Feladatok állításaival és a 4.3. Gyakorlat megoldásával is.

5.4. Legyen $f \in \mathbb{Z}_p[x]$ irreducibilis osztója $\overline{\Phi_n} \in \mathbb{Z}_p[x]$-nek, és k az f foka. Ismeretes, hogy a $T = \mathbb{Z}_p[x]/(f)$ faktorgyűrű test, mely $\mathbb{Z}_p$-nek k-adfokú bővítése, és benne az f-nek már van egy ε gyöke, melyre $T = \mathbb{Z}_p(\varepsilon)$. Lagrange tétele szerint ε rendje a T multiplikatív csoportjában (ami a 3.14. Gyakorlat szerint pont n) osztója e csoport rendjének, ami $p^k - 1$. Azaz $p^k \equiv 1\ (n)$, és így $o_n(p) \mid k$.

Legyen $\ell = o_n(p)$, ekkor $n \mid p^\ell - 1$. Mivel ε rendje n, ezért innen $\varepsilon^{p^\ell} = \varepsilon$. Tehát ε gyöke az $x^{p^\ell} - x$ polinomnak, melynek gyökei nyilván résztestet alkotnak. De ε generálja T-t, ezért ez a résztest maga a T. Ennek a polinomnak legfeljebb annyi gyöke lehet T-ben, mint a foka, és ezért $|T| = p^k \le p^\ell$. Vagyis $k \le \ell = o_n(p)$. Ezzel megmutattuk, hogy $k = o_n(p)$, amivel az állítást beláttuk.

Alternatív bizonyításként a következőre is gondolhatunk. Az $\ell = o_n(p)$ a legkisebb olyan pozitív egész, melyre a p^ℓ elemű T véges test multiplikatív csoportjának rendje osztható n-nel, azaz — mivel ez ciklikus csoport —, amelyre a T-ben van egy n rendű ε elem. A T testben ekkor rögtön $\varphi(n)$ darab n rendű elem van (már ε hatványai között is), és ezért T-ben Φ_n lineáris tényezőkre bomlik. Ezért $T = \mathbb{Z}_p(\alpha)$ minden n rendű α elemre, és így mindegyik ilyen α minimálpolinomja ℓ-edfokú. Ez az előzőnél talán rövidebb, de több előismeretet használó bizonyítás.

— *Mit keres ez a toprongyos ember királyi udvaromban?*
— *Ő Felséged udvari csillagásza.*
— *Mi dolga az én udvari csillagászomnak?*
— *Ő csinálja Felséged kalózkapitányainak a tengeri térképet.*
— *Miért ilyen toprongyos ez a fontos ember?*
— *Mert mindössze évi öt aranyat kap Felséged kincstárából.*
— *Többet érdemel. Legyen mától fogva száz arany a fizetése.*
— *Bátorkodom Felséged figyelmét alázatosan arra felhívni, hogy akkor Felséged udvari csillagászának a státuszát soha többé nem fogja csillagász betölteni.*