Körosztási polinomok vizsgálata

Írta:

Borsányi Ákos

ELTE TTK, matematika BSc.

Témavezető:

Dr. Zábrádi Gergely

egyetemi docens

Algebra és Számelmélet Tanszék

2021

Bevezetés

Szakdolgozatom célja a körosztási polinomokra nagyobb rálátást nyújtani. Ezt részint saját eredmények és bizonyítások bemutatásával, részint a szakirodalom felhasználásával teszem. Az 1.1. szakaszban egybegyűjtöm a körosztási polinomok alapvető oszthatósági tulajdonságait, amelyek számos érdekes feladat megoldásához nyújtanak segítséget. Ezen rész megírására az is motivált, hogy a szakirodalomban ilyen jellegű összefoglalással eddig nem találkoztam. Az 1. fejezet 2. szakaszában önállóan látom be e polinomok $\mathbb{Q}$ feletti irredeucibilitását, melynek hasznos hozadéka az n-edik körosztási test diszkriminánsának kiszámolása. A bizonyítás teljes mértékben eltér az elsőéves algebraanyagban szereplő bizonyítástól. $\Phi_n(x)$ legnagyobb együttható-abszolútértékét $A(n)$-nel szokás jelölni, a körosztási polinomokkal kapcsolatban leggyakrabban ezt vizsgálják. A 2. fejezetben $A(n)$ felső, majd bizonyos n-ekre $A(n)$ alsó becslésével foglalkozom. Először összefoglalom azokat a tételeket, amelyeket saját gondolataim, illetve a szakirodalom alapján $\Phi_{pq}(x)$-ről érdemesnek tartok elmondani, majd ezt követően Bang 1895-ös eredményét javítom, mely szerint az $r < q < p$ prímekre $A(pqr) \leq r - 1$. Rámutatok arra az érdekes tényre, hogy $\Phi_n(x)$ együtthatói abszolútértékben az n két legnagyobb prímosztójától független korlát alatt vannak. Az $A(n)$-re vonatkozó alsó becsléseket bizonyos típusú körosztási polinomok egy-egy alkalmasan megválasztott együtthatójának kiszámolásával kezdem. Ezen tételek egyikéből kiderül, hogy a Marion Beiter által sejtett $A(pqr) \leq \frac{r+1}{2}$ becslés tovább nem élesíthető. (A Beiter-sejtés később hamisnak bizonyult, a korrigált sejtés $A(pqr) \leq \frac{2}{3}r$.) Az utolsó szakasz folytatásaként megmutatom, hogy az úgynevezett prímszám k-asok sejtéséből (2.3.6. sejtés) következik, hogy a 2.2.3. tétel állításánál erősebbet csak a konstansszorzók javításával mondhatunk. A szakdolgozatot egy, az analitikus számelmélet eszközeit is használó szép eredménnyel zárom, melynek lényeges (azaz nem konstansszorzókkal történő) javítása számomra nem ismeretes.

1.

1.1. A körosztási polinomok prímosztóiról

Legyen $n \geq 1$ egész, $\varepsilon = e^{\frac{2i\pi}{n}}$. Az n-edik körosztási polinomot a

$$\Phi_n(x) = \prod_{\substack{k=1 \\ (k,n)=1}}^{n} (x - \varepsilon^k) \tag{1}$$

szorzattal definiáljuk. Mivel $\eta \in \mathbb{C}$ pontosan akkor n-edik egységgyök, ha valamely $d|n$-re $o(\eta) = d$, továbbá (1)-ben ε^k az összes n-edik primitív egységgyökön fut végig, azért

$$x^n - 1 = \prod_{d|n} \Phi_d(x) \tag{2}$$

(2)-ből Möbius-transzformációval előáll a legtöbbet alkalmazott alábbi tétel.

1.1.1. Lemma.

$$\Phi_n(x) = \prod_{d|n} (x^{\frac{n}{d}} - 1)^{\mu(d)} \tag{3}$$

Bizonyítás. Legyen $x \in \mathbb{R}$. Ha $n \geq 3$, akkor $\Phi_n(x) \quad \frac{\varphi(n)}{2}$ darab nemnulla komplex norma szorzata lévén pozitív, így $x > 1$ esetén $\Phi_n(x) > 0$ minden $n \geq 1$-re. Legyen most $x > 1$ rögzített. Ekkor (2) logaritmusát Möbius-transzformálva

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

amiből

$$\Phi_n(x) = \prod_{d|n} (x^{\frac{n}{d}} - 1)^{\mu(d)} \tag{3'}$$

Mivel (3') mindkét oldalán polinomfüggvények hányadosa áll, a (3) polinomazonosság érvényes. □

Ebben a szakaszban a körosztási polinomokat a szokásosnál valamivel általánosabb alakban vizsgáljuk. Ezt készíti elő a következő jelölés bevezetése.

Definíció. *Jelölje $\Phi_n(x, y)$ azt a $\mathbb{C}[x, y]$-beli polinomot, amelyet a $\Phi_n(x)$-nek az y határozatlan segítségével $\varphi(n)$-edfokú homogén polinommá történő kiegészítésével kapunk, azaz legyen*

$$\Phi_n(x, y) = \prod_{\substack{k=1 \\ (k,n)=1}}^{n} (x - y\varepsilon^k) \tag{4}$$

(2)-vel azonosan nyilván

$$x^n - y^n = \prod_{d|n} \Phi_d(x, y) \tag{5}$$

Emellett korántsem meglepően igaz az 1.1.1. lemma megfelelő általánosítása, ami az alábbi módon fest.

1.1.2. Lemma.

$$\Phi_n(x, y) = \prod_{d|n} \left(x^{\frac{n}{d}} - y^{\frac{n}{d}}\right)^{\mu(d)} \tag{6}$$

Bizonyítás. (4)-ből, (1)-ből és (3)-ból

$$\Phi_n(x,y) = y^{\varphi(n)}\Phi_n\left(\frac{x}{y}\right) = y^{\varphi(n)}\prod_{d|n}\left(\left(\frac{x}{y}\right)^{\frac{n}{d}} - 1\right)^{\mu(d)} = \prod_{d|n}\left(x^{\frac{n}{d}} - y^{\frac{n}{d}}\right)^{\mu(d)}$$

s itt az utolsó egyenlőségnél felhasználtuk a $\varphi(n) = \sum_{d|n}\mu(d)\frac{n}{d}$ azonosságot. □

Előrebocsátjuk, hogy a továbbiakban p-vel mindíg pozitív prímszámot fogunk jelölni.

1.1.3. Következmény.

1. *a)* $\Phi_n(x) \in \mathbb{Z}[x]$

   b) $\Phi_n(x,y) \in \mathbb{Z}[x,y]$

2. *Ha* $\alpha \geq 1$ *és* $(n,p) = 1$, *akkor*

$$\Phi_{np^\alpha}(x,y) = \frac{\Phi_n(x^{p^\alpha}, y^{p^\alpha})}{\Phi_n(x^{p^{\alpha-1}}, y^{p^{\alpha-1}})} \tag{7}$$

   speciálisan

$$\Phi_{np^\alpha}(x) = \frac{\Phi_n(x^{p^\alpha})}{\Phi_n(x^{p^{\alpha-1}})} \tag{8}$$

3. *Legyen* $p|n$. *Ekkor*

$$\Phi_{np}(x,y) = \Phi_n(x^p, y^p) \tag{9}$$

   speciálisan

$$\Phi_{np}(x) = \Phi_n(x^p) \tag{10}$$

4. *Bármely* k *pozitív egészre*

$$\Phi_{nk}(x,y)|\Phi_n(x^k, y^k) \qquad \mathbb{Z}[x,y]\text{-}ban \tag{11}$$

Bizonyítás.

1. a) (3) baloldala véges, jobboldala egész együtthatós formális hatványsor $\mathbb{C}\big[[x]\big]$-ben.

   b) Közvetlenül adódik az a) pontból.

2. (6) alapján

$$\Phi_{np^\alpha}(x,y) = \prod_{\beta=0}^{\alpha}\prod_{d|n}\left(x^{p^{\alpha-\beta}\frac{n}{d}} - y^{p^{\alpha-\beta}\frac{n}{d}}\right)^{\mu(dp^\beta)} = \prod_{\beta=0}^{1}\prod_{d|n}\left(x^{p^{\alpha-\beta}\frac{n}{d}} - y^{p^{\alpha-\beta}\frac{n}{d}}\right)^{\mu(dp^\beta)}$$

   ami éppen (7) jobboldala.

3. Ismét (6) szerint

$$\Phi_{np}(x,y) = \prod_{d|n}\left(x^{\frac{np}{d}} - y^{\frac{np}{d}}\right)^{\mu(d)} \cdot \prod_{\substack{d|np\\ d\nmid n}}\left(x^{\frac{np}{d}} - y^{\frac{np}{d}}\right)^{\mu(d)}$$

   s itt a második szorzatban minden d-re $p^2|d$, amiért igaz (9) is.

4. Azonnal adódik a következmény 1. b), 2. és 3. pontjaiból. □

1.1.4. Lemmácska. *Legyen $n > 1$. Ekkor $\Phi_n(1) = e^{\Lambda(n)}$, ahol Λ az úgynevezett van Mangoldt-függvény, vagyis*
$\Lambda(n) = \begin{cases} \log p & \text{ha } n = p^\alpha \ (\alpha \geq 1) \\ 0 & \text{különben} \end{cases}$

Bizonyítás. Akár (1)-ből, akár (3)-ból

$$\Phi_{p^\alpha}(x) = \sum_{k=0}^{p-1} x^{p^{\alpha-1}k} \qquad\qquad \alpha \geq 1 \tag{12}$$

tehát $\Phi_{p^\alpha}(1) = p$, ha pedig $n = n_1 p^\alpha$, $n_1 > 1$, $p \nmid n_1$ és $\alpha \geq 1$, akkor (8)-ból $x = 1$ helyettesítéssel adódik a bizonyítandó $\Phi_n(1) = 1$ egyenlőség. □

A továbbiakban szükségünk lesz a rend fogalmának alábbi általánosítására. Legyen $x, y, m \in \mathbb{Z}$, $m \geq 1$, $(xy, m) = 1$. Az Euler–Fermat-tétel miatt $x^{\varphi(m)} \equiv y^{\varphi(m)} \pmod{m}$, így létezik az a legkisebb d pozitív egész, melyre $x^d \equiv y^d \pmod{m}$. Ezt a d-t az x és az y közös rendjének nevezzük $\bmod m$. Jelölése $o_m(x, y)$, röviden $o(x, y)$. Könnyen látható, hogy a rend ezen általánosítása szintén rendelkezik a korábbról megszokott oszthatósági tulajdonsággal, vagyis $x^k \equiv y^k \pmod{m}$ pontosan akkor teljesül, ha $o_m(x, y)|k$. Kézenfekvő föltenni a következő kérdést. Igaz-e, hogy ha x és y relatív prímek, akkor az $o_p(x, y) = n$ és a $p|\Phi_n(x, y)$ feltételek ekvivalensek egymással? A válasz lényegében igenlő. Ha $o_p(x, y) = n$, akkor a rend definíciója és (5) miatt $p|\Phi_n(x, y)$, másrészt ki fogjuk mutatni, hogy legfeljebb egy p prím kivételével $p|\Phi_n(x, y)$ esetén $o_p(x, y) = n$. Az ezután következő tételekben és definíciókban mindvégig feltesszük, hogy $(x, y) = 1$.

1.1.5. Lemma. *Legyen p a $\Phi_n(x, y)$ tetszőleges prímosztója. Ekkor az $o_p(x, y) \neq n$ és a $p|n$ feltételek ekvivalensek.*

Bizonyítás. Tegyük fel először, hogy $o_p(x, y) \neq n$. Ezen feltétel alapján létezik olyan $d|n$, $d > 1$, hogy $x^{\frac{n}{d}} \equiv y^{\frac{n}{d}} \pmod{p}$, ekkor pedig bármely $q|d$ prímre $x^{\frac{n}{q}} \equiv y^{\frac{n}{q}} \pmod{p}$. Emellett (11) szerint $p|\Phi_n(x, y)|\Phi_q(x^{\frac{n}{q}}, y^{\frac{n}{q}})$, amiből az előbbiek miatt $p|\Phi_q(x^{\frac{n}{q}}, x^{\frac{n}{q}}) = x^{\frac{n}{q}(q-1)} \cdot \Phi_q(1) = x^{\frac{n}{q}(q-1)} q$ adódik, tehát $(x, y) = 1$ miatt $p = q$. Tegyük most fel, hogy $p|n$, és legyen $n = n_1 p^\alpha$, ahol $(n_1, p) = 1$. Ekkor (11) és a kis Fermat-tétel értelmében $p|\Phi_n(x, y)|\Phi_{n_1}(x^{p^\alpha}, y^{p^\alpha}) \equiv \Phi_{n_1}(x, y) \pmod{p}$, vagyis $x^{n_1} \equiv y^{n_1} \pmod{p}$. □

Ide kívánkozik a következő definíció.

Definíció. *Ha $p|\Phi_n(x, y)$ és $p|n$, akkor p-t a $\Phi_n(x, y)$ kivételes prímosztójának nevezzük.*

A kivételes prímosztó fogalmának lényegileg az ellenkezőjét adja meg az alábbi elnevezés.

Definíció. *Ha $o_p(x, y) = n$, úgy p-t a $\Phi_n(x, y)$, illetve az $x^n - y^n$ primitív prímosztójának nevezzük.*

A kis Fermat-tételnek és a rend oszthatósági tulajdonságának közvetlen folyománya a soronlévő fontos és közismert kis észrevétel.

1.1.6. Lemmácska. *Ha $(x, y) = 1$, akkor $x^n - y^n$ minden primitív prímosztója $nk + 1$ alakú.* □

A következő segédtétel fő mondanivalója, hogy a körosztási polinomoknak legfeljebb egy kivételes prímosztója lehetséges.

1.1.7. Lemma. *Legyen p a $\Phi_n(x, y)$ kivételes prímosztója, és legyen $n = n_1 p^\alpha$, ahol $(n_1, p) = 1$. Ekkor $p \equiv 1 \pmod{n_1}$, és így p az n legnagyobb prímosztója.*

Bizonyítás. Az 1.1.5. lemma bizonyításában látottak szerint $p|\Phi_{n_1}(x, y)$, és mivel $p \nmid n_1$, azért szintén 1.1.5. miatt $o_p(x, y) = n_1$, vagyis 1.1.6. értelmében valóban $p \equiv 1 \pmod{n_1}$. □

A kivételes prímosztó másik lényeges tulajdonságát adja meg az alábbi segédtétel.

1.1.8. Lemma. *Legyen p a $\Phi_n(x, y)$ kivételes prímosztója. Ekkor az $n = p = 2$ eset kivételével $p||\Phi_n(x, y)$.*

Bizonyítás. Legyen először $p \geq 3$. $p|\Phi_p(x^{\frac{n}{p}}, y^{\frac{n}{p}})$ miatt elég a lemmát az $n = p$ esetben igazolni. Mivel ekkor $x^p \equiv y^p \pmod{p}$, azért a kis Fermat-tétel értelmében $x \equiv y \pmod{p}$, vagyis $x = y + tp$ valamilyen t egész számmal. A körosztási polinomba behelyettesítve kapjuk, hogy

$$\Phi_p(x, y) = \frac{(y + tp)^p - y^p}{tp} = \sum_{k=0}^{p-1} \binom{p}{k} y^k (tp)^{p-k-1} \tag{13}$$

Látható, hogy $0 \leq k \leq p - 3$ esetén (13)-ban a k-nak megfelelő tag osztható p^2-tel, valamint $p \geq 3$ miatt ugyanez igaz a $k = p - 2$-höz tartozó tagra is, (13) utolsó tagja viszont py^{p-1}, amivel lemmánk $p \geq 3$ esetét beláttuk. Legyen most $p = 2$. Ekkor a 2 kivételes volta és az 1.1.7. lemma miatt $n = 2^\alpha$ ($\alpha \geq 1$), ebben az esetben pedig $\Phi_n(x, y) = x^{2^{\alpha-1}} + y^{2^{\alpha-1}}$, s így $2 \nmid xy$, amiért $\alpha \geq 2$ esetén $x^{2^{\alpha-1}} + y^{2^{\alpha-1}} \equiv 2 \pmod{8}$, amivel az 1.1.8. lemma bizonyítását befejeztük. □

Most már igazolhatjuk a következő tételt, mely azt mondja ki, hogy különböző körosztási polinomok azonos helyeken felvett értékei majdnem mindig relatív prímek.

1.1.9. Lemma. *Legyenek x és y egészek, $(x, y) = 1$ és $n > k \geq 1$. Ekkor*

$$(\Phi_n(x, y), \Phi_k(x, y)) = \begin{cases} p & \text{ha } n = kp^\alpha \text{ és } p|\Phi_k(x, y) \\ 1 & \text{különben} \end{cases}$$

Bizonyítás. A rend egyértelműsége miatt $\Phi_k(x, y)$ primitív prímosztói páronként különböznek $\Phi_n(x, y)$ primitív prímosztóitól. Így ha p közös prímosztó, akkor p a $\Phi_n(x, y)$ és $\Phi_k(x, y)$ közül legalább az egyiknek kivételes prímosztója. Mivel $k < n$, azért ha p csak az egyik körosztási polinomnak kivételes prímosztója, akkor $o_p(x, y) = k$. Emellett $n = n_1 p^\alpha$ ($(n_1, p) = 1$), és így az 1.1.5. lemma bizonyításában látottak alapján $o_p(x, y) = n_1$, vagyis $n_1 = k$, tehát $n = kp^\alpha$. Ha p mindkét esetben kivételes prímosztó, akkor $n = n_1 p^\beta$, és $k = k_1 p^\gamma$, ahol $(n_1, p) = (k_1, p) = 1$, és az előbbiekhez hasonlóan látható, hogy $o_p(x, y) = n_1 = k_1$, amiből a lemma állítása kiolvasható, felhasználva az 1.1.8. lemmát. □

1.1.10. Állítás. *Legyen $p|n$. Ekkor $p|\Phi_n(x, y)$ akkor és csak akkor, ha $o_p(x, y) = n_1$, ahol $n = n_1 p^\alpha$ és $p \nmid n_1$.*

Bizonyítás. Ha $o_p(x, y) = n_1$, akkor a rend definíciója és (5) értelmében $p|\Phi_{n_1}(x, y)$, az 1.1.9. lemma miatt viszont ekkor $p|\Phi_n(x, y)$. Az ellenkező irányú implikációra nézve pedig lásd 1.1.7. bizonyítását. □

A kivételes prímosztóról mondottakból kitűnik, hogy primitív prímosztó majdnem mindig létezik, ezt fogalmazza meg pontosan a következő tétel.

1.1.11. Tétel. *Legyenek x, y, n pozitív egészek, $x > y$ és $(x, y) = 1$. Ekkor az alábbi esetektől eltekintve $x^n - y^n$-nek létezik primitív prímosztója.*

(i) $n = 1$ *és* $x = y + 1$

(ii) $n = 2$ *és* $x + y = 2^\alpha$, $\alpha \geq 2$ *egész*

(iii) $n = 6$, $x = 2$ *és* $y = 1$

Bizonyítás. A tételt Zsigmondy 1892-ben igazolta, én saját bizonyításomat közlöm rá. Az $n = 1$ eset triviális. Ha $n = 2$, akkor könnyen látható, hogy $x + y$ páratlan prímosztói a primitív prímosztók. Legyen ezután $n \geq 3$ és jelölje p az n legnagyobb prímosztóját. 1.1.7. és 1.1.8. miatt azt kell megmutatnunk, hogy $\Phi_n(x, y) > p$. Mivel $\Phi_n(x, y)$ $\frac{\varphi(n)}{2}$ darab komplex norma szorzata, azért nem-negatív, s így (4) a következőképpen módosítható.

$$\Phi_n(x, y) = \prod_{\substack{k=1 \\ (k,n)=1}}^{n} |x - y\varepsilon^k| \tag{14}$$

Ha $x \geq y+2$, akkor (14)-ből $\Phi_n(x,y) > 2^{\varphi(n)} \geq 2^{p-1} \geq p$ tehát ebben az esetben kész vagyunk. Tegyük most fel, hogy $x = y+1$. Ekkor a $p=2$ eset triviális, ennélfoga a továbbiakban kikötjük, hogy $p \geq 3$. (14)-ben az egyes tényezőkre a koszinusztételt alkalmazva $\Phi_n(y+1,y) \geq \Phi_n(2)$ adódik, egyenlőség $y=1$ esetén áll. Figyelembe véve, hogy $\varphi(n) = \sum_{d|n} d\mu(\frac{n}{d})$, az 1.1.1. lemmából kapjuk, hogy

$$\Phi_n(2) = 2^{\varphi(n)} \prod_{d|n} \left(1 - \frac{1}{2^d}\right)^{\mu\left(\frac{n}{d}\right)} > 2^{\varphi(n)} \prod_{k=1}^{\infty} \left(1 - \frac{1}{2^k}\right) \tag{15}$$

Belátjuk, hogy $\prod_{k=1}^{\infty}\left(1-\frac{1}{2^k}\right) > \frac{1}{4}$. Becslésünkhöz a triviálisan kiszámolható $\prod_{k=2}^{\infty}\left(1-\frac{1}{k^2}\right) = \frac{1}{2}$ határértéket használjuk fel. Teljes indukcióval azonnal látható, hogy ha $k \geq 8$, akkor $2^{k-2} \geq k^2$, amiből $\prod_{k=6}^{\infty}\left(1-\frac{1}{2^k}\right) \geq \prod_{k=8}^{\infty}\left(1-\frac{1}{k^2}\right)$, a hátralevő $\prod_{k=2}^{5}\left(1-\frac{1}{2^k}\right) > \prod_{k=2}^{7}\left(1-\frac{1}{k^2}\right)$ egyenlőtlenséget pedig némi számolással ellenőrizhetjük. Így $\prod_{k=2}^{\infty}\left(1-\frac{1}{2^k}\right) > \frac{1}{2}$, ami a bizonyítandó állítást jelenti, (15)-ből tehát $\Phi_n(2) > 2^{\varphi(n)-2}$. Vezessük be az $n = n_1 p$ jelölést. Mivel $\varphi(ab) \geq \varphi(a)\varphi(b)$, azért $n_1 \geq 3$ esetén $\varphi(n) \geq 2p-2$, amiből $p \geq 3$ miatt $\varphi(n) - 2 \geq p-1$, amivel az $x \geq y+2$ esetbelihez hasonlóan kész vagyunk. Hátra van az $n_1 = 1$ és az $n_1 = 2$ eset. Ha $n_1 = 1$, akkor $n = p$, és így $\Phi_n(2) = 2^p - 1 > p$. Legyen most $n_1 = 2$. Ekkor

$$\Phi_n(y+1,y) \geq \Phi_n(2) = \sum_{k=1}^{\frac{p-1}{2}} 2^{2k-1} + 1 \geq 2^{p-2} + 1 \geq p \tag{16}$$

(16)-ban mindegyik helyen egyenlőség az $y=1$, $p=3$ esetben áll, ekkor tehát nincs primitív prímosztó, minden más esetben (16)-ban valahol szigorú egyenlőtlenség érvényes, amivel 1.1.11.-et bebizonyítottuk. □

A következő három pontban n – úgy, mint az eddigiekben – rögzített pozitív egészet jelöl.

1.1.12. Állítás. *Minden $nk+1$ alakú p prím alkalmas x-re előáll $x^n - 1$ primitív prímosztójaként.*

Bizonyítás. p-nek tetszőleges g primitív gyökét véve $o_p(g^k) = n$, így az $x = g^k$ választás megfelel. □

1.1.13. Állítás. *Az $nk+1$ alakú prímek száma végtelen.*

Bizonyítás. A tétel a Dirichlet-tétel elsőéves törzsanyagban tárgyalt speciális esete, melyet a körosztási polinomok segítségével nem nehéz igazolni. Legyenek $q_1, \ldots, q_s$ ($s \geq 0$) $nk+1$ alakú prímek, és legyen $x = 4\prod_{i=1}^{s} q_i$. Ekkor az 1.1.11. tétel alapján $x^n - 1$-nek létezik primitív prímosztója, ami 1.1.6. szerint $nk+1$ alakú, továbbá a q_i-k mindegyikétől különbözik. Minden $s \geq 0$-ra van tehát $s+1$ darab $nk+1$ alakú prím, amivel 1.1.13.-at bizonyítottuk. □

Megjegyzés. 1.1.13. kimutatása az 1.1.11. tétel nélkül, pusztán az 1.1.5. lemma felhasználásával is történhet.

Szintén primitív prímosztók segítségével oldható meg az alábbi szép feladat.

1.1.14. Probléma. *Legyenek x és y tetszőleges pozitív egészek úgy, hogy $x > y$. Bizonyítsuk be, hogy*

$$n^{\frac{d(n)}{2}} | \varphi(x^n - y^n)$$

Megoldás. Először megjegyezzük, hogy $(x,y) = 1$ föltehető, ugyanis ha $(x,y) = d$, $x = dx_1$ és $y = dy_1$, akkor $x_1^n - y_1^n | x^n - y^n$ miatt $\varphi(x_1^n - y_1^n) | \varphi(x^n - y^n)$, és persze $(x_1, y_1) = 1$. A rend egyértelműsége miatt az n tetszőleges d_1, d_2 osztóira a $\Phi_{d_1}(x,y)$ primitív prímosztói páronként különböznek $\Phi_{d_2}(x,y)$ primitív prímosztóitól. Most 1.1.11. alapján megkülönböztetünk három esetet.

(i) x, y és n olyanok, hogy az n minden $d > 1$ osztójára $\Phi_d(x,y)$-nak van primitív prímosztója.

(ii) $2|n$ és $x + y = 2^\alpha$ ($\alpha \geq 2$)

(iii) $6|n$, $x = 2$ és $y = 1$.

A megoldáshoz a $\varphi(m)$ értékét megadó képletet és 1.1.6.-ot használjuk. Eszerint az (i) esetben

$$\prod_{\substack{d|n \\ d>1}} d = n^{\frac{d(n)}{2}} | \varphi(x^n - y^n)$$

ha pedig (ii) áll fenn, akkor mivel páros m esetén $2^\alpha \varphi(m) = \varphi(2^\alpha m)$, azért

$$2 \prod_{\substack{d|n \\ d\neq 2}} d = n^{\frac{d(n)}{2}} | \varphi(x^n - y^n)$$

vagyis az első két esetben kész vagyunk. Az (iii) esetben a hiányzó 6-os tényezőből a 3-at maga $\Phi_6(2) = 3$ pótolja (figyelembe vettük, hogy a 3 $\Phi_2(2)$-ből is előáll), a 2-t pedig $\varphi(2^3 - 1)$-ből nyerjük. □

A szakasz állításainak egy része közismert, viszont az 1.1.5., 1.1.7., 1.1.8., 1.1.9. lemmákkal, és az 1.1.10. állítással a szakirodalomban nem találkoztam, megfogalmazásuk és bizonyításuk saját munkám eredménye. Szintén önállóan bizonyítottam az 1.1.11. tételt, illetve adtam megoldást az 1.1.14. problémára. Megjegyzendő, hogy később [1]-ben olvastam 1.1.8. $n = p$ speciális esetének bizonyítását, továbbá szintén [1]-ben a szerző kimondja az 1.1.11. tételt.

1.2. Alternatív bizonyítás a körosztási polinom irreducibilitására

Ebben a szakaszban a körosztási polinomok $\mathbb{Q}$ feletti felbonthatatlanságát igazolom a Schönemann–Eisenstein-kritérium egy általánosításával. A bizonyításban lényeges szerephez jut Dedekind úgynevezett elágazási tétele, amelyet Károlyi Gyula előadásán hallottam.

1.2.1. Tétel. *A $\Phi_n(x)$ n-edik körosztási polinom minden $n \geq 1$ esetén irreducibilis $\mathbb{Q}$ felett.*

Bizonyítás. A bizonyításhoz szükségünk lesz néhány segédtételre.

1.2.2. Lemma (Schönemann–Eisenstein-kritérium)**.** *Legyen megadva az R kommutatív egységelemes gyűrű fölött az $f(x) = \sum_{k=0}^{n} a_k x^k$ polinom, és tegyük fel, hogy létezik az R-nek olyan P prímideálja, melyre $a_n \notin P$, $a_k \in P$ $(0 \leq k \leq n-1)$ és $a_0 \notin P^2$. Ekkor f nem esik szét $R[x]$-ben két legalább elsőfokú tényező szorzatára.*

Bizonyítás. Tegyük fel indirekte, hogy

$$f(x) = \left(\sum_{i=0}^{r} b_i x^i\right)\left(\sum_{j=0}^{s} c_j x^j\right) \qquad 1 \leq r, s \leq n-1 \tag{17}$$

Ekkor $a_0 = b_0 c_0 \in P$ miatt $b_0 \in P$ vagy $c_0 \in P$. Feltehetjük, hogy $c_0 \in P$ s így $a_0 \notin P^2$ miatt $b_0 \notin P$. Legyen most $1 \leq t \leq s$, és tegyük fel, hogy $c_j \in P$ minden $0 \leq j \leq t-1$ esetén. (17) szerint $a_t = \sum_{k=0}^{t} b_k c_{t-k}$, ahol $k \geq r+1$ esetén értelemszerűen $b_k = 0$ veendő. Mivel $t \leq s \leq n-1$, azért $a_t \in P$, vagyis $b_0 c_t = a_t - \sum_{k=1}^{t} b_k c_{t-k} \in P$, amiből $b_0 \notin P$ miatt $c_t \in P$. Azt nyertük tehát, hogy $c_s \in P$, ámde ez ellentmond annak, hogy $a_n = b_r c_s \notin P$, amivel a lemmát bebizonyítottuk. □

A következő két tételben legyen K n-edfokú bővítése $\mathbb{Q}$-nak, R pedig K algebrai egészeinek gyűrűje, továbbá K diszkriminánsát jelölje D_K.

1.2.3. Lemma (Dedekind elágazási tétele)**.** *Ha p tetszőleges prímszám, akkor a (p) főideál pontosan akkor bomlik négyzetmentesen az R ideáljai között, ha $p \nmid D_K$.*

1.2.1 bizonyításában Dedekind tételéből nekünk csak arra az implikációra van szükségünk, hogy ha $p \nmid D_K$, akkor (p) négyzetmentes. Ezt az irányt könnyebb bizonyítani, ezt igazoljuk. Álljon elő K $\mathbb{Q}$-ból a ϑ elem adjungálásával (mint ismeretes, ilyen ϑ létezik), és legyen ϑ ($\mathbb{Q}$ feletti) kanonikus polinomja f. Jelölje továbbá az f felbontási testét N, az N-ben levő algebrai egészek gyűrűjét pedig S. Tetszőleges $\gamma \in K$ esetén γ $K|Q$-nyomára használjuk az $T(\gamma)$ jelölést, azaz $T(\gamma) = \sum_{j=1}^{n} \gamma^{(j)}$, ahol $\gamma^{(j)}$ a γ szám j-edik konjugáltját jelenti. Itt rögtön megjegyezzük, hogy könnyen látható módon $T(\gamma) \in \mathbb{Q}$, $\gamma \in R$ esetén pedig $T(\gamma) \in \mathbb{Z}$. Végül bevezetjük még a következőket. Legyen $\omega_1, \ldots, \omega_n$ K-nak egészbázisa. Ekkor legyen $a_{ij} = T(\omega_i \omega_j)$, és $A = (a_{ij})_{n \times n}$, A_{ij} pedig legyen A-nak az a_{ij}-hez tartozó előjeles aldeterminánsa. Tegyük most fel, hogy léteznek olyan $P, Q \lhd R$ ideálok, melyekre P prím és $(p) = P^2 Q$. Legyen $\alpha \in PQ \setminus P^2 Q$ tetszőleges fix elem, megmutatjuk, hogy ekkor bármely $\beta \in R$ számra $p|T(\alpha\beta)$. Elegendő azt kimutatni, hogy $p|T^p(\alpha\beta)$. $\alpha^2 \in P^2Q^2 \subset (p)$ miatt $p|\alpha^2$ R-ben, és így S-ben is. A következő szakaszban oszthatóságon és kongruencián mindig S-beli oszthatóságot ill. kongruenciát értünk. A binomiális tétel ismételt alkalmazásával, felhasználva, hogy $1 \leq k \leq p-1$ esetén $p|\binom{p}{k}$, azt kapjuk, hogy

$$T^p(\alpha\beta) = \left(\sum_{j=1}^{n} (\alpha\beta)^{(j)} \right)^p \equiv \sum_{j=1}^{n} \left((\alpha\,\beta)^{(j)} \right)^p \qquad \mathrm{mod}\ p \tag{18}$$

Most észrevesszük, hogy (18) jobboldala tagonként osztható p-vel. A $p|\alpha^2$ oszthatóságból $p|(\alpha\beta)^p$, és így minden $1 \leq j \leq n$-re $p|\left((\alpha\beta)^p\right)^{(j)} = \left((\alpha\beta)^{(j)}\right)^p$. Ezzel megkaptuk, hogy $p|T^p(\alpha\beta)$ S-ben,vagyis $\frac{T^p(\alpha\beta)}{p} \in \mathbb{Q} \cap S = \mathbb{Z}$, amivel eljutottunk fenti oszthatóságunkhoz. Legyen α kanonikus előállítása $\alpha = \sum_{i=1}^{n} \lambda_i \omega_i$, $\lambda_i \in \mathbb{Z}$ $(1 \leq i \leq n)$. Mivel $\alpha \notin (p)$, azért alkalmas $1 \leq j \leq n$-re $p \nmid \lambda_j$. Rögzítsünk most egy ilyen j-t. Az előbb bizonyított állításunk szerint minden $1 \leq k \leq n$-re $p|T(\alpha\omega_k)$, továbbá $T(\alpha\omega_k) = T(\sum_{i=1}^{n} \lambda_i \omega_i \omega_k) = \sum_{i=1}^{n} \lambda_i T(\,\omega_i \omega_k) = \sum_{i=1}^{n} \lambda_i a_{ik}$, amiből

$$p| \sum_{k=1}^{n} A_{jk} T(\alpha\omega_k) = \sum_{k=1}^{n} A_{jk} \sum_{i=1}^{n} \lambda_i a_{ik} = \sum_{i=1}^{n} \lambda_i \sum_{k=1}^{n} A_{jk} a_{ik} \tag{19}$$

A ferde kifejtési tétel miatt $\sum_{k=1}^{n} A_{jk} a_{ik} = \delta_{ij} \det A$, így $p \nmid \lambda_j$ folytán (19)-ből $p|\det A$. Ha tekintjük a D_K definíciójában szereplő determinánst, akkor oszlop-oszlop szorzással meggyőződhetünk róla, hogy $\det A = D_K$, s ezzel 1.2.3.-nak azt az oldalát, ami számunkra szükséges, bebizonyítottuk. $\square$

1.2.4. Lemma. *Jelölje az $\alpha_1, \ldots, \alpha_n \in R$ elemek diszkriminánsát D. Ekkor $D_K | D$.*

*Bizonyítás.*Úgy, mint 1.2.3.-ban, legyen $\omega_1, \ldots, \omega_n$ K-nak egészbázisa. Akkor $\alpha_k = \sum_{i=1}^n \lambda_{k,i}\omega_i$, ahol $\lambda_{k,i} \in \mathbb{Z}$ minden k-ra és i-re. Ebből

$$\sqrt{D} = \begin{vmatrix} \sum_{i=1}^n \lambda_{1,i}\omega_i & \sum_{i=1}^n \lambda_{2,i}\omega_i & \ldots & \sum_{i=1}^n \lambda_{n,i}\omega_i \\ \sum_{i=1}^n \lambda_{1,i}\omega_i^{(2)} & \sum_{i=1}^n \lambda_{2,i}\omega_i^{(2)} & \ldots & \sum_{i=1}^n \lambda_{n,i}\omega_i^{(2)} \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{i=1}^n \lambda_{1,i}\omega_i^{(n)} & \sum_{i=1}^n \lambda_{2,i}\omega_i^{(n)} & \ldots & \sum_{i=1}^n \lambda_{n,i}\omega_i^{(n)} \end{vmatrix}$$

Tudjuk, hogy ha egy C determináns valamelyik oszlopában (ill. sorában) az elemeket $c_i = a_i + b_i$ alakba írjuk, akkor $C = A + B$, ahol A-t és B-t úgy kapjuk, hogy C-ben a c_i elemek helyett rendre az a_i, ill. a b_i elemeket írjuk. Ezt felhasználva (természetesen az oszlopok mentén bontva) az adódik, hogy

$$\sqrt{D} = \sum_f \begin{vmatrix} \lambda_{1,f(1)}\omega_{f(1)} & \lambda_{2,f(2)}\omega_{f(2)} & \ldots & \lambda_{n,f(n)}\omega_{f(n)} \\ \lambda_{1,f(1)}\omega_{f(1)}^{(2)} & \lambda_{2,f(2)}\omega_{f(2)}^{(2)} & \ldots & \lambda_{n,f(n)}\omega_{f(n)}^{(2)} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_{1,f(1)}\omega_{f(1)}^{(n)} & \lambda_{2,f(2)}\omega_{f(2)}^{(n)} & \ldots & \lambda_{n,f(n)}\omega_{f(n)}^{(n)} \end{vmatrix}$$

ahol az összegzés az összes $f : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ leképezésen fut végig. Nyilvánvaló, hogy ha f nem ínjektív, akkor valamelyik két oszlop lineárisan összefügg, így az f-hez tartozó tag nulla. Ha pedig f permutáció, akkor a hozzá tartozó determináns $\prod_{k=1}^n \lambda_{k,f(k)}(-1)^p\sqrt{D_K}$, ahol p az f paritása. Ha tehát T-vel jelöljük a

$$\begin{vmatrix} \lambda_{1,1} & \lambda_{1,2} & \ldots & \lambda_{1,n} \\ \lambda_{2,1} & \lambda_{2,2} & \ldots & \lambda_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_{n,1} & \lambda_{n,2} & \ldots & \lambda_{n,n} \end{vmatrix}$$

determinánst, akkor azt kapjuk, hogy $D = T^2 D_K$, így a lemmát igazoltuk. □

1.2.5. Tétel. *Legyen az $n > 1$ egész prímfelbontása $n = \prod_{t=1}^r p_t^{\alpha_t}, n_t = \frac{n}{p_t^{\alpha_t}}, \varepsilon = e^{\frac{2i\pi}{n}}$, D pedig az n-edik primitív egyéggyökök által generált Vandermonde-determináns négyzete. Ekkor*

$$|D| = \prod_{t=1}^r p_t^{\frac{\varphi(n)}{p_t - 1}(\alpha_t(p_t - 1) - 1)} \tag{20}$$

Bizonyítás. A körosztási polinom egész együtthatós volta és a szimmetrikus polinomok alaptétele miatt D egész. Ha tehát megmutatjuk, hogy D és (20) jobboldala egymás egységszeresei $\mathbb{Z}[\varepsilon]$-ban, akkor ebből az következik, hogy e két szám kölcsönösen osztja egymást $\mathbb{Z}$-ben is, ami pedig (20)-at jelenti.

Az asszociáltsági relációra bevezetjük a következő jelölést. Ha az R kommutatív egységelemes gyűrű α és β elemei (R-ben) egymás egységszeresei, akkor azt írjuk, hogy $\alpha \sim_R \beta$. Amennyiben világos, hogy az α és β elemek asszociáltsága mely gyűrűben értendő, úgy az $\alpha \sim \beta$ jelölést is használjuk. Előrebocsátjuk a következőt. Legyen p prím, $l \geq 1, p \nmid a$ egészek és $\eta = e^{\frac{2i\pi}{p^l}}$.Ekkor

$$1 - \eta \sim_{\mathbb{Z}[\eta]} 1 - \eta^a \tag{21}$$

és

$$(1 - \eta)^{p^{l-1}(p-1)} \sim p \quad , \tag{22}$$

továbbá $p^l | n$ esetén $\mathbb{Z}[\eta] \subset \mathbb{Z}[\varepsilon]$,s így ekkor értelemszerűen

$$1 - \eta \sim_{\mathbb{Z}[\varepsilon]} 1 - \eta^a \tag{23}$$

és

$$(1-\eta)^{p^{l-1}(p-1)} \sim_{\mathbb{Z}[\varepsilon]} p \tag{24}$$

(21) igazolása végett feltehetjük, hogy $a \geq 1$. $(p^l, a) = 1$ miatt alkalmas b pozitív egészre $ab \equiv 1 \mod p^l$, így az $1-\eta|1-\eta^a|1-\eta^{ab} = 1-\eta$ kölcsönös oszthatóság fennáll,vagyis (21) igaz.1.1.4. szerint pedig $\Phi_{p^l}(1) = p$ amiből (21) felhasználásával adódik (22). $\mathbb{Z}[\varepsilon]$-ban D nyilvánvalóan egységszerese a

$$D' = \prod_{\substack{j=1 \\ (j,n)=1}}^{n} \prod_{\substack{k=1 \\ (k,n)=1 \\ k \neq j}}^{n} (1-\varepsilon^{j-k})$$

számnak.Tekintsük az 1-től n-ig terjedő, n-hez relatív prímekből képezhető különböző elemű (j,k) rendezett párokat. Ezekre vonatkozóan most két esetet különböztetünk meg.

- 1. eset: $j \not\equiv k \mod n_t$ minden $1 \leq t \leq r$-re
- 2. eset: $j \equiv k \mod n_t$ valamely $1 \leq t \leq r$ esetén.

Az első esetben megadható olyan t_1 és t_2, amelyre $|j-k|$ prímfelbontásában p_{t_1} és p_{t_2} kitevője kisebb (esetleg 0), mint α_{t_1}, illetve α_{t_2}, így ekkor $\omega(o(\varepsilon^{j-k})) \geq 2$, ami miatt 1.1.4.-ből $1-\varepsilon^{j-k}|1$ adódik, azaz $1-\varepsilon^{j-k}$ egység ($\mathbb{Z}[\varepsilon]$-ban).

A második esetben mivel $j \not\equiv k \mod n$, azért pontosan egy olyan t létezik, amelyre $j \equiv k \mod n_t$. Most t-t rögzítjük, és egységszorzóban való eltérés erejéig kiszámoljuk a

$$P_t = \prod \left\{ (1-\varepsilon^{j-k}) | \quad 1 \leq j,k \leq n, j \neq k, (j,n) = (k,n) = 1, j \equiv k \mod n_t \right\}$$

szorzatot. Az eddigiekből világos, hogy

$$D' \sim \prod_{t=1}^{r} P_t \tag{25}$$

Az Euler-féle φ-függvény multiplikativitásának szokásos bizonyításakor látható, hogy ha $m_1, m_2 \in \mathbb{N}^+, (m_1, m_2) = 1$ és $m_1 m_2 = m$, akkor egy modulo m redukált maradékrendszer előáll $\varphi(m_1)$ darab modulo m_2 redukált maradékrendszer egyesítéseként úgy, hogy az egyes redukált maradékrendszereken belül az elemek páronként kongruensek egymással $\mod m_1$, és minden m_1-hez relatív prím s-hez létezik ezen felbontásban olyan (modulo m_2) redukált maradékrendszer, melynek számai s-sel kongruensek modulo m_1. Ezt az észrevételt az $m_1 = n_t, m_2 = p_t^{\alpha_t}$ esetre alkalmazzuk. Vegyük fel a következő jelöléseket. Legyen $(n_t, s) = 1$, $R_{t,s} = \{1 \leq k \leq n | \quad (n,k) = 1, \quad k \equiv s \mod n_t\}$

$$Q_{t,s} = \prod_{\substack{j,k \in R_{t,s} \\ j \neq k}} (1-\varepsilon^{j-k})$$

$\eta_t = e^{\frac{2i\pi}{p_t^{\alpha_t}}}$ és

$$Q_t = \prod_{\substack{j=1 \\ (j,p)=1}}^{p_t^{\alpha_t}} \prod_{\substack{k=1 \\ (k,p)=1 \\ k \neq j}}^{p_t^{\alpha_t}} (1-\eta_t^{j-k})$$

Nyilván

$$P_t = \prod_{\substack{s=1 \\ (n_t,s)=1}}^{n_t} Q_{t,s} \tag{26}$$

Mivel (23) alapján könnyen látható, hogy ha $j \equiv k \mod n_t$, akkor $1-\varepsilon^{j-k} \sim 1-\eta_t^{j-k}$, továbbá állításunk szerint $R_{t,s}$ redukált maradékrendszer modulo $p_t^{\alpha_t}$, azért

$$Q_{t,s} \sim Q_t \tag{27}$$

minden $(n_t, s) = 1$-re. Feladatunk tehát Q_t asszociáltság erejéig történő kiszámolása. t rögzített volta megengedi, hogy p_t, α_t, η_t és Q_t esetében a t indexet a következő gondolatmenet folyamán elhagyjuk, így egyszerűség kedvéért ezt megtesszük. Tetszőleges $a \in \mathbb{Z}$ és $\beta \in \mathbb{N}$ számokra jelölje $p^\beta || a$ azt, hogy $p^\beta | a$, de $p^{\beta+1} \nmid a$, és legyen

$$q_\beta = \prod_{\substack{j=1 \\ (j,p)=1}}^{p^\alpha} \prod_{\substack{k=1 \\ (k,p)=1 \\ p^\beta || j-k}}^{p^\alpha} (1-\eta^{j-k}) \qquad 0 \le \beta \le \alpha - 1$$

Ekkor értelemszerűen

$$Q = \prod_{\beta=0}^{\alpha-1} q_\beta \tag{28}$$

Mivel $p^\beta || j-k$ esetén (23) alapján $1-\eta^{j-k} \sim 1-\eta^{p^\beta}$ és (24) szerint $(1-\eta^{p^\beta})^{p^{\alpha-\beta-1}(p-1)} \sim p$, így célunk a q_β-ban szereplő tényezők leszámolása minden $0 \le \beta \le \alpha - 1$-re. q_β-nak annyi tényezője van, amennyi a

$$\{(j,k) | 1 \le j,k \le p^\alpha, (j,p) = (k,p) = 1, p^\beta || j-k\}$$

rendezett párok száma, ezen párokat kell leszámolni. Legyen β fix, ekkor j-t $p^{\alpha-1}(p-1)$ féleképpen rögzíthetjük. $\beta = 0$ esetén k-nak 1-től p^α-ig pontosan a $\mod p$ 0-val és j-vel inkongruens elemeket választhatjuk, ami $p^{\alpha-1}(p-1)$ $p^{\alpha-1}(p-2) = p^{2(\alpha-1)}(p-1)(p-2)$ darab megfelelő (j,k) párt jelent, tehát $q_0 \sim p^{p^{\alpha-1}(p-2)}$. Tegyük most fel, hogy $1 \le \beta \le \alpha - 1$. $(j,p) = 1$ miatt $k = j + lp^\beta$-ra is teljesül $(k,p) = 1$, így a szóban forgó (j,k) párok száma $p^{\alpha-1}(p-1)(p^{\alpha-\beta} - p^{\alpha-\beta-1})$, amiért most $q_\beta \sim p^{p^{\alpha-1}(p-1)}$. Figyelembe véve (28)-at, azt kapjuk, hogy $Q \sim p^{p^{\alpha-1}(\alpha(p-1)-1)}$. Az indexeket visszaírva:

$$Q_t \sim p_t^{p_t^{\alpha_t-1}(\alpha_t(p_t-1)-1)} \tag{29}$$

(29)-ből,(27)-ből és (26)-ból $P_t \sim p_t^{\varphi(n_t)p_t^{\alpha_t-1}(\alpha_t(p_t-1)-1)}$, majd ezután (25)-ből $D' \sim \prod_{t=1}^r p_t^{\varphi(n_t)p_t^{\alpha_t-1}(\alpha_t(p_t-1)-1)}$, amiből tekintetbe véve, hogy $D' \sim D$, azt nyerjük, hogy $D \sim \prod_{t=1}^r p_t^{\frac{\varphi(n)}{p_t-1}(\alpha_t(p_t-1)-1)}$, és ezzel megkaptuk (20)-at. □

1.2.6. Lemma. *Legyen az n-edik körosztási test diszkriminánsa Δ. Ekkor $p|\Delta$ esetén $p|n$.*

Bizonyítás. ε és D jelentése legyen ugyanaz, mint 1.2.5.-ben. Legyen ε foka s, és jelölje D^* az $1, \varepsilon, \ldots, \varepsilon^{s-1}$ egységgyökök diszkriminánsát. Akkor

$$D^* = \prod_{1 \le j < k \le s} (\varepsilon^{l_k} - \varepsilon^{l_j})^2 \tag{30}$$

ahol l_j $(1 \le j \le s)$ mindazon kitevőkön fut végig, melyekre ε és ε^{l_j} konjugáltak. Az 1.2.4. tételből $\Delta | D^*$, továbbá nyilvánvalóan $D^* | D$ $\mathbb{Z}[\varepsilon]$-ban, ami mivel D^* és D is egész, mint $\mathbb{Z}$-beli oszthatóság is fennáll. Innen azt kapjuk, hogy $\Delta | D$, 1.2.5. szerint pedig D prímosztói megegyeznek az n prímtényezőivel, amivel a lemmát beláttuk. □

Rátérünk az 1.2.1. tétel bizonyítására. A bizonyítást $\omega(n)$ értékére vonatkozó teljes indukcióval végezzük. Ha $\omega(n) = 0$, akkor $n = 1$, a $\Phi_1(x) = x - 1$ polinom pedig triviálisan irreducibilis. Legyen ezután $\omega(n) \ge 1$, p prímosztója n-nek, $n = mp^\alpha$, $(m,p) = 1$ és $\varepsilon = e^{\frac{2i\pi}{m}}$. Megmutatjuk,hogy

$$\Phi_n(x) = \prod_{\substack{a=1 \\ (a,m)=1}}^{m} \Phi_{p^\alpha}(x, \varepsilon^a) \tag{31}$$

Az $\eta = e^{\frac{2i\pi}{p^\alpha}}$ és $\zeta = e^{\frac{2i\pi}{n}}$ jelölésekkel (31) jobboldala (4) alapján az alábbi módon folytatható.

$$\prod_{\substack{a=1\\(a,m)=1}}^{m} \Phi_{p^\alpha}(x,\varepsilon^a) = \prod_{\substack{a=1\\(a,m)=1}}^{m} \prod_{\substack{b=1\\(b,p^\alpha)=1)}}^{p^\alpha} (x-\eta^b\varepsilon^a) =$$

$$= \prod_{\substack{a=1\\(a,m)=1}}^{m} \prod_{\substack{b=1\\(b,p^\alpha)=1)}}^{p^\alpha} (x-\zeta^{mb+p^\alpha a}) \tag{32}$$

Könnyen látható, hogy $\{mb+p^\alpha a | 1 \le a \le m, \quad 1 \le b \le p^\alpha, \quad (a,m) = (b,p^\alpha) = 1\}$ redukált maradékrendszer modulo n, amiért a (32)-beli második egyenlőség jobboldala a $\Phi_n(x)$-et definiáló (1) polinommal egyezik, tehát (31) igaz. Jelölje R a $\mathbb{Q}(\varepsilon)$ algebrai egészeinek gyűrűjét. A bizonyítás fő lépése azt kimutatni, hogy $\Phi_{p^\alpha}(x,\varepsilon^a)$ minden a-ra R felett irreducibilis, amiből majd rövid úton következni fog a $\mathbb{Q}(\varepsilon)$ feletti irreducibilitás is. $\Phi_{p^\alpha}(x,\varepsilon^a)$ irreducibilitása nyilván ekvivalens $\Phi_{p^\alpha}(x+\varepsilon^a,\varepsilon^a)$ felbonthatatlanságával, a Schönemann-kritériumot ez utóbbi polinomra tudjuk kényelmesen alkalmazni.

$$\Phi_{p^\alpha}(x+\varepsilon^a,\varepsilon^a) = \sum_{k=0}^{p-1}(x+\varepsilon^a)^{p^{\alpha-1}k}\varepsilon^{ap^{\alpha-1}(p-1-k)} = \sum_{k=0}^{p-1}\sum_{t=0}^{p^{\alpha-1}k}\binom{p^{\alpha-1}k}{t}x^t\varepsilon^{a(\varphi(p^\alpha)-t)} =$$

$$= \sum_{t=0}^{p^{\alpha-1}(p-1)} \varepsilon^{a(\varphi(p^\alpha)-t)} \left(\sum_{k=\left[\frac{t}{p^{\alpha-1}}\right]}^{p-1} \binom{p^{\alpha-1}k}{t} \right) x^t \tag{33}$$

Bebizonyítjuk, hogy az $R[x]$-beli (33) polinomra teljesül az 1.2.2.-ben kirótt feltétel. (33)-ban a legmagasabb, $\varphi(p^\alpha)$-adfokú tag együtthatója 1, továbbá (33) konstans tagja $p\varepsilon^{a\varphi(p^\alpha)}$, ami R-ben p-vel asszociált. Ha most Δ-val jelöljük $\mathbb{Q}(\varepsilon)$ diszkriminánsát, akkor $p \nmid m$ miatt az 1.2.6. lemma alapján $p \nmid \Delta$, amiből 1.2.3. értelmében $\left(p\varepsilon^{a\varphi(p^\alpha)}\right) = (p)$ prímideál felbontásában nincs többször előforduló ideál. Ezek szerint ha megmutatjuk, hogy $1 \le t \le p^{\alpha-1}(p-1)-1$ esetén (33)-ban x^t együtthatója R-ben osztható p-vel, akkor (33)-ra a Schönemann-kritérium (p) bármely prímideáltényezőjével alkalmazhatóvá válik. $\varepsilon^{a(\varphi(p^\alpha)-t)}$ egység, így amit igazolni kell, az a

$$p \left| \sum_{k=\left[\frac{t}{p^{\alpha-1}}\right]}^{p-1} \binom{p^{\alpha-1}k}{t} \right. \qquad (1 \le t \le p^{\alpha-1}(p-1)-1) \tag{34}$$

$\mathbb{Z}$-beli oszthatóság. (34)-ben két esetet különböztetünk meg.

1. eset. $p^{\alpha-1} \nmid t$. Itt azt látjuk be, hogy (34) tagonként teljesül, vagyis hogy $p|\binom{p^{\alpha-1}k}{t}$. A Legendre-formula felállításánál alkalmazott gondolatmenet szerint $\binom{p^{\alpha-1}k}{t}$ p-t a

$$\gamma = \sum_{\beta=1}^{\alpha-1}\left(\frac{p^{\alpha-1}k}{p^\beta} - \left[\frac{t}{p^\beta}\right] - \left[\frac{p^{\alpha-1}k-t}{p^\beta}\right]\right)$$

kitevőn tartalmazza. Tudjuk, hogy $x,y \in \mathbb{R}$ esetén $0 \le [x+y]-[x]-[y]$, továbbá ha $x+y \in \mathbb{Z}$, akkor egyenlőség pontosan akkor áll, ha x és y egészek. Emiatt a $\gamma > 0$ egyenlőtlenség akkor és csak akkor igaz, ha valamely $1 \le \beta \le \alpha-1$-re $p^\beta \nmid t$, azaz ha $p^{\alpha-1} \nmid t$, az 1.esetre tehát (34)-et beláttuk.

2. eset. $t = p^{\alpha-1}t', \quad t' \in \mathbb{Z}, \quad 1 \le t' \le p-2$. Most azt mutatjuk meg, hogy

$$\binom{p^{\alpha-1}k}{p^{\alpha-1}t'} \equiv \binom{k}{t'} \mod p \tag{35}$$

Ha ezt bebizonyítottuk, kész vagyunk, hiszen (35) fennálltakor a (34)-ben szereplő összegre

$$\sum_{k=t'}^{p-1}\binom{p^{\alpha-1}k}{p^{\alpha-1}t'}\equiv\sum_{k=t'}^{p-1}\binom{k}{t'}=\binom{p}{t'+1}\equiv 0 \mod p$$

Legyen $\mu,r,q\in\mathbb{N},\quad 0\le r\le q\le p-1$. Ekkor $\binom{p^\mu q}{p^\mu r}=\prod_{s=1}^{p^\mu r}\frac{p^\mu(q-r)+s}{s}$. $1\le s\le p^\mu r$ esetén írjuk s-et $p^{\nu(s)}s'$ alakba, ahol $(s',p)=1$. Ezen jelölésekkel

$$\binom{p^\mu q}{p^\mu r}=\prod_{s=1}^{p^\mu r}\frac{p^{\mu-\nu(s)}(q-r)+s'}{s'} \tag{36}$$

Tetszőleges $a\in\mathbb{Z}$ számra jelölje $[a]$ az a-t tartalmazó mod p maradékosztályt. $0\le\nu(s)\le\mu-1$ esetén triviálisan $p^{\mu-\nu(s)}(q-r)+s'\equiv s' \mod p$, így (36)-ot a $\mathbb{Z}_p$ maradékosztálytestben fölírva, majd tovább folytatva

$$\left[\binom{p^\mu q}{p^\mu r}\right]=\prod_{s=1}^{p^\mu r}\frac{[p^{\mu-\nu(s)}(q-r)+s']}{[s']}=\prod_{j=1}^{r}\frac{[q-r+j]}{[j]}=\left[\binom{q}{r}\right] \tag{37}$$

(37) két szélének egyenlősége pedig azt jelenti, hogy a (35) kongruencia teljesül. Igazoltuk tehát (34)-et, és ezzel azt, hogy $\Phi_{p^\alpha}(x+\varepsilon^a,\varepsilon^a)$, s vele együtt $\Phi_{p^\alpha}(x,\varepsilon^a)$ R felett irreducibilis. Most belátjuk, hogy $\Phi_{p^\alpha}(x,\varepsilon^a)$ $\mathbb{Q}(\varepsilon)$ felett is irreducibilis. Tegyük fel, hogy léteznek olyan $f(x),g(x)\in\mathbb{Q}(\varepsilon)[x]$ polinomok, melyekre $\mathrm{gr}f,\mathrm{gr}g\ge 1$ és $\Phi_{p^\alpha}(x,\varepsilon^a)=f(x)g(x)$. Mivel $\Phi_{p^\alpha}(x,\varepsilon^a)$ normált, azért ekkor megadhatók olyan f_1 és g_1 $\mathbb{Q}(\varepsilon)$ feletti normált polinomok is, melyekre f-hez és g-hez hasonlóan

$$\Phi_{p^\alpha}(x,\varepsilon^a)=f_1(x)g_1(x)\qquad \mathrm{gr}f_1,\mathrm{gr}g_1\ge 1 \tag{38}$$

$\Phi_{p^\alpha}(x,\varepsilon^a)$ gyökei egységgyökök lévén algebrai egészek, így (38) miatt f_1 és g_1 gyökei is azok, és ezért pedig f_1 és g_1 normáltsága folytán e két polinom együtthatói szintén algebrai egészek, vagyis $f_1(x),g_1(x)\in R[x]$. Ezáltal (38)-ban olyan egyenlet jelenik meg, amiről bebizonyítottuk, hogy lehetetlen, tehát $\Phi_{p^\alpha}(x,\varepsilon^a)$ minden a-ra felbonthatatlan $\mathbb{Q}(\varepsilon)$ felett.

Legyen $(a,m)=1$, és tekintsük a

$$\Psi_a\left(\sum_{k=0}^{\varphi(m)-1}b_k\varepsilon^k\right)=\sum_{k=0}^{\varphi(m)-1}b_k\varepsilon^{ak}\qquad(b_k\in\mathbb{Q},\quad 0\le k\le\varphi(m)-1)$$

hozzárendelést. Mivel az indukciófeltevés értelmében $\Phi_m(x)$ irreducibilis $\mathbb{Q}$ felett, azért az $\{\varepsilon^k|0\le k\le\varphi(m)-1\}$ egységgyökök $\mathbb{Q}$ felett lineárisan függetlenek, vagyis a körosztási polinom fokszámát is figyelembe véve $\mathbb{Q}(\varepsilon)$ minden β eleme egyértelműen előáll $\beta=\sum_{k=0}^{\varphi(m)-1}b_k\varepsilon^k$ alakban. Ennélfogva a Ψ_a hozzárendelés függvény, és értelmezési tartománya $\mathbb{Q}(\varepsilon)$. Triviális, hogy Ψ_a összegtartó, és hogy $\mathbb{Q}$ elemeit fixen hagyja. Ψ_a szorzattartása is könnyen ellenőrizhető, ez pedig az előbbiekkel együtt azt adja, hogy Ψ_a a $\mathbb{Q}(\varepsilon)$ endomorfizmusa. Nem használjuk fel, de az is könnyen látható – és persze közismert – hogy Ψ_a bijektív, és hogy a $\Gamma(\mathbb{Q}(\varepsilon)|\mathbb{Q})$ Galois- csoport automorfizmusai éppen az összes Ψ_a leképezés. Továbbmenve, a kézenfekvő

$$\Psi_a\left(\sum_{k=0}^{s}\beta_k x^k\right)=\sum_{k=0}^{s}\Psi_a(\beta_k)x^k\qquad(\beta_k\in\mathbb{Q}(\varepsilon),k=0,\dots,s)$$

értelmezéssel Ψ_a a $\mathbb{Q}(\varepsilon)[x]$ automorfizmusává terjed ki, ez szintén egyszerűen belátható, és egyben közismert.

Álljon elő most az n-edik körosztási polinom a

$$\Phi_n(x)=f(x)g(x)\qquad f(x),g(x)\in\mathbb{Q}[x] \tag{39}$$

alakban. Természetesen (39) mint $\mathbb{Q}(\varepsilon)$ feletti szorzattá alakítás is érvényes. Előrebocsátjuk, hogy a hátralevő részben az oszthatóságot $\mathbb{Q}(\varepsilon)[x]$-ben értjük. (31) alapján $\Phi_{p^\alpha}(x,\varepsilon)|\Phi_n(x)$. $\mathbb{Q}(\varepsilon)[x]$ euklideszi, így $\Phi_{p^\alpha}(x,\varepsilon)$ felbonthatalansága folytán $\Phi_{p^\alpha}(x,\varepsilon)$ prímeleme $\mathbb{Q}(\varepsilon)[x]$ -nek, vagyis osztja (39) jobboldalának valamelyik tényezőjét. Feltehetjük, hogy

$$\Phi_{p^\alpha}(x,\varepsilon)|f(x) \tag{40}$$

Mivel $\Psi_a(\varepsilon)=\varepsilon^a$, azért $\Psi_a\left(\Phi_{p^\alpha}(x,\varepsilon)\right)=\Phi_{p^\alpha}(x,\varepsilon^a)$, és ennélfogva (40)-ből

$$\Phi_{p^\alpha}(x,\varepsilon^a)|\Psi_a(f(x))=f(x) \tag{41}$$

A $\Phi_{p^\alpha}(x,\varepsilon^a)$ $(1\le a\le m,(a,m)=1)$ polinomok normáltak és páronként különbözőek, így egyikük sem asszociált a másikkal, tehát irreducibilitásuk folytán páronként relatív prímek, amiből (31) és (41) miatt

$$\Phi_n(x)|f(x) \tag{42}$$

(39) és (42) együttesen azt jelenti, hogy f foka $\varphi(n)$, vagyis g konstans. Ezzel bizonyításunk véget ért. □

A szakasz lemmái és tételei közül az 1.2.2., 1.2.3., és az 1.2.4. segédtételek egyetemi tanulmányaimhoz köthetők azzal a kiegészítéssel, hogy a Schönemann-kritérium eredeti változatán szükséges volt egy kézenfekvő általánosítást végrehajtani. Az 1.2.5., 1.2.6., valamint az 1.2.1. tétel bizonyítása pedig teljes mértékben önálló úton történt.

2. Körosztási polinomok együtthatóbecslése rögzített $\omega(n)$ érték esetén

Ebben a fejezetben rátérünk a körosztási polinomok együtthatóbecslésére, amivel jelen szakdolgozat elsősorban kíván foglalkozni. Idevonatkozó jelöléseinket mindjárt be is vezetjük. Jelentse $A(n)$ az n-edik körosztási polinom legnagyobb abszolútértékű együtthatójának abszolútértékét, $S(n)$ pedig jelölje $\Phi_n(x)$ együtthatóinak abszolútértékösszegét. Legyen n különböző prímosztóinak szorzata n_1, és legyen $n=n_1d$. Ekkor (10) ismételt alkalmazásával azt kapjuk, hogy $\Phi_n(x)=\Phi_{n_1}(x^d)$, vagyis az n-edik körosztási polinom együtthatóinak vizsgálatát elegendő négyzetmentes n-ekre végezni. Könnyen látható továbbá, hogy $2\nmid m$, $m>1$ esetén $\Phi_{2m}(x)=\Phi_m(-x)$, így ekkor $\Phi_{2m}(x)$ együtthatói rendre legfeljebb előjelben különböznek $\Phi_m(x)$ együtthatóitól. Ezen észrevételek birtokában a tézis hártalévő részében kikötjük, hogy n páratlan négyzetmentes pozitív egész. A körosztási polinomok együtthatóival kapcsolatos tételek bizonyításánál kétféle kiindulási lehetőségről van tudomásom. Az egyiknél, melyet a szerzők túlnyomó többsége követ, a körosztási polinomot (3) segítségével átírjuk formális hatványsorrá, a másiknál, mely saját ötlet, $\Phi_n(x)$-et olyan törtté alakítjuk át, melyben a nevező n alkalmas d pozitív osztójával x^d-1 alakú, javítva ezzel $\Phi_n(x)$ kezelhetőségét. A teljesség kedvéért megemlítjük, hogy $\Phi_1(x)$ és $\Phi_p(x)$ előállítása nyilvánvaló és közismert, utóbbira nézve lásd pl. (12)-t. Vizsgálódásainkat a legegyszerűbb nemtriviális $\omega(n)=2$ esettel kezdjük. Előrebocsátjuk, hogy a továbbiakban p-vel és q-val rögzített, egymástól különböző 2-nél nagyobb prímeket jelölünk.

2.1. $\Phi_{pq}(x)$-re vonatkozó állítások

2.1.1. Tétel. $A(pq)=1$. *(Más szavakkal mondva $\Phi_{pq}(x)$ minden együtthatója 0, 1 vagy -1).*

Bizonyítás. (8)-at alkalmazva, majd tovább írva

$$\Phi_{pq}(x)=\frac{\Phi_q(x^p)}{\Phi_q(x)}=\frac{\Phi_q(x^p)(x-1)}{x^q-1}=\frac{1}{x^q-1}\left(\sum_{t=0}^{q-1}x^{tp+1}-\sum_{t=0}^{q-1}x^{tp}\right) \tag{43}$$

Mivel $p\neq q$, azért $\{tp+1|0\le t\le q-1,t\in\mathbb{Z}\}$ és $\{tp|0\le t\le q-1,t\in\mathbb{Z}\}$ teljes maradékrendszerek modulo q. Jelölje ν $\{0,1,...,q-1\}$-nek azt a permutációját, amelyre $tp+1\equiv\nu(t)p \mod q$ minden $t\in\{0,1,...,q-1\}$ esetén. Ennek felhasználásával (43) a következőképpen folytatható.

$$\frac{1}{x^q-1}\left(\sum_{t=0}^{q-1}x^{tp+1}-\sum_{t=0}^{q-1}x^{tp}\right)=\sum_{t=0}^{q-1}\frac{x^{tp+1}-x^{\nu(t)p}}{x^q-1} \tag{44}$$

Nyilvánvaló, hogy $t \in \{0,1,...,q-1\}$, $t > \nu(t)$ fennálltakor

$$\frac{x^{tp+1}-x^{\nu(t)p}}{x^q-1} = \frac{x^{\nu(t)p}(x^{(t-\nu(t))p+1}-1)}{x^q-1} = x^{\nu(t)p} \sum_{k=0}^{\frac{(t-\nu(t))p+1}{q}-1} x^{kq} = \sum_{k=0}^{\frac{(t-\nu(t))p+1}{q}-1} x^{\nu(t)p+kq} \tag{45}$$

$t < \nu(t)$ esetén pedig

$$\frac{x^{tp+1}-x^{\nu(t)p}}{x^q-1} = -\frac{x^{tp+1}(x^{(\nu(t)-t)p-1}-1)}{x^q-1} = -x^{tp+1} \sum_{k=0}^{\frac{(\nu(t)-t)p-1}{q}-1} x^{kq} = -\sum_{k=0}^{\frac{(\nu(t)-t)p-1}{q}-1} x^{tp+kq+1} \tag{46}$$

Ennek alapján

$$\sum_{t=0}^{q-1} \frac{x^{tp+1}-x^{\nu(t)p}}{x^q-1} = \sum_{\substack{t=0 \\ t>\nu(t)}}^{q-1} \sum_{k=0}^{\frac{(t-\nu(t))p+1}{q}-1} x^{\nu(t)p+kq} - \sum_{\substack{t=0 \\ \nu(t)>t}}^{q-1} \sum_{k=0}^{\frac{(\nu(t)-t)p-1}{q}-1} x^{tp+kq+1} \tag{47}$$

A (45) és (46) jobb szélén álló polinomokban mindegyik tag kitevője kongruens $\nu(t)p$-vel modulo q, vagyis a (47) jobboldalán szereplő hatványkitevők páronként különbözőek, ezzel pedig 2.1.1.-et igazoltuk.

A 2.1. szakasz hátralévő részében legyen c a p $[1, q-1]$-be eső inverze mod q, továbbá legyen $a = q - c$ (vagyis a a p $[1, q-1]$-be eső ellentett inverze modulo q). Most ν megadásával felírjuk $\Phi_{pq}(x)$ explicit alakját.

2.1.2. Tétel.

$$\Phi_{pq}(x) = \sum_{t=0}^{c-1} \sum_{k=0}^{\frac{ap+1}{q}-1} x^{tp+kq} - \sum_{t=0}^{a-1} \sum_{k=0}^{\frac{cp-1}{q}-1} x^{tp+kq+1} \tag{48}$$

Bizonyítás. Könnyű észrevenni, hogy $\nu(a) = 0$, majd ezután hogy $a \le t \le q-1$ esetén $\nu(t) = t - a$. Ezenfelül nyilván $\nu(0) = c$, és ebből $0 \le t \le a-1$-re $\nu(t) = c+t$, amivel $\nu(t)$ értékét minden $t \in \{0,1,...,q-1\}$-re megmondtuk, ennek felhasználásával pedig (47) jobboldala átmegy (48)-ba. Annak megfelelően, ahogy (47)-ben, úgy a (48)-ban lévő kitevők is páronként különbözőek. □

2.1.3. Tétel. *$\Phi_{pq}(x)$-ben a $+1$ és a -1 együtthatójú tagok váltakozva követik egymást.*

Két bizonyítást adunk.

1. Bizonyítás. $n \in \mathbb{Z}$ esetén jelölje r_n a $|\{(t,k) : n = tp+kq\,;\, t,k \in \mathbb{N}\}|$ megoldásszámot. $(p,q) = 1$ miatt rögzített n egészre a $tp + kq = n$ $(t,k \in \mathbb{Z})$ egyenletben t és k modulo q illetve modulo p egyértelműen meghatározott, így ha $n \le pq-1$, akkor r_n értéke 0 vagy 1. Jelölje I_j $(j = 0,1,...,s)$ rendre azon „$\mathbb{Z}$-beli intervallumokat", melyekre a 0 illetve 1 r-értékeket adó számokból álló maximális hosszúságú egybefüggő sorozatok $[0, pq-1] \cap \mathbb{Z}$-t vágják. Nevezzük az I_j intervallumot jónak, ha j páros, és rossznak, ha j páratlan. A körosztási polinom együtthatóira a $\Phi_{pq}(x) = \sum_{n=0}^{pq-1} a_n x^n$ jelölést használva a következőt mutatjuk meg.

(i) $a_n = 1$, ha n egy jó intervallum első eleme.

(ii) $a_n = -1$, ha n egy rossz intervallum első eleme.

(i)-t bizonyítjuk, (ii) bizonyítása (i)-vel lényegében azonos gondolatmenettel történik. Mivel $r_0 = 1$, azért a jó intervallumok tartalmazzák azon n-eket, melyekre $r_n = 1$. Ha $n \in I_{2j}$, és az $n = tp + kq$ $(t,k \in \mathbb{N})$ előállításban $t \ge c$ vagy $k \ge \frac{ap+1}{q}$, akkor az

$$n - 1 = (t-c)p + (k + \frac{cp-1}{q})q$$

és az

$$n-1=(t+a)p+(k-\frac{ap+1}{q})q$$

lineáris kombinációk valamelyike konvex. Ha tehát n első elem egy jó intervallumban, akkor n úgy áll elő a fenti alakban, hogy $0\le t\le c-1$ és $0\le k\le \frac{ap+1}{q}-1$, ami (48) alapján azt jelenti, hogy $a_n=1$, figyelembe véve, hogy az ott szereplő kitevők páronként különböznek.

Legyen most $a_n=1$. Ekkor (48) szerint léteznek olyan t és k egészek, melyekre

$$n=tp+kq \qquad 0\le t\le c-1, \quad 0\le k\le \frac{ap+1}{q}-1 \tag{49}$$

ami nyilván azt is eredményezi, hogy alkalmas $j\in\{0,...,[s/2]\}$-re $n\in I_{2j}$. Tegyük fel indirekte, hogy n nem első eleme I_{2j}-nek. Ekkor $n-1\in I_{2j}$ és $0\le n-1\le pq-2$. Ebből

$$n-1=t'p+k'q \qquad 0\le t'\le q-1, \quad 0\le k'\le p-1 \tag{50}$$

(49)-ből pedig

$$n-1=(t-c)p+(k+\frac{cp-1}{q})q \qquad t-c<0, \quad 0\le k+\frac{cp-1}{q}\le p-1 \tag{51}$$

Mivel rögzített m egészre a $pu+qv=m$ $(u,v\in\mathbb{Z})$ egyenletben u és v modulo q illetve modulo p egyértelműen meghatározott, azért (50)-ből, és (51)-ből $k'=k+\frac{cp-1}{q}$, amiből $t'=t-c$, s ez pedig szintén (50)-re és (51)-re való tekintettel ellentmondás. □

2. Bizonyítás. Használjuk az első bizonyítás jelöléseit és fogalmait. Formális hatványsorok segítségével észrevesszük, hogy

$$\Phi_{pq}(x)=\sum_{n=0}^{pq-1}(r_n-r_{n-1})x^n \tag{52}$$

Az 1.1.1. lemmából kiindulva, majd tovább folytatva

$$\Phi_{pq}(x)=\frac{(1-x)(1-x^{pq})}{(1-x^p)(1-x^q)}=(1-x)(1-x^{pq})\sum_{t\ge0}\sum_{k\ge0}x^{tp+kq}\equiv$$

$$\equiv(1-x)\sum_{\substack{t,k\ge0\\ tp+kq\le pq-1}}x^{tp+kq}\equiv\sum_{n=0}^{pq-1}r_nx^n-\sum_{n=0}^{pq-2}r_nx^{n+1}\pmod{x^{pq}} \tag{53}$$

$\mathbb{Q}\big[[x]\big]$-ben. Mivel az (53) két szélén álló polinomok közül mindkettő foka kisebb, mint pq, továbbá $r_{-1}=0$, azért (52) igaz. (Ebből természetesen $A(pq)=1$ tüstént adódik). Ezután pedig $r_0=1$ és $r_{-1}=0$ figyelembe vételével megkapjuk, hogy $0\le n\le pq-1$ esetén

$$r_n-r_{n-1}=\begin{cases}1, & \text{ha } n \text{ egy jó intervallum legkisebb eleme}\\ -1, & \text{ha } n \text{ egy rossz intervallum legkisebb eleme}\\ 0, & \text{különben}\end{cases}$$ □

Bár $\Phi_{pq}(x)$ fokszáma $(p-1)(q-1)$, a benne szereplő nemnulla tagok sűrűségét az alábbi szerint látom helyesnek definiálni. Az együtthatókra alkalmazzuk a 2.1.3. tétel első bizonyításának jelölését. $\Phi_{pq}(x)$-hez hozzáadjuk az a_nx^n tagot minden $(p-1)(q-1)<n\le pq-1$ esetén. Ezáltal a körosztási polinomon nem változtatunk, hiszen a szóban forgó n-ekre $a_n=0$, viszont a $\Phi_{pq}(x)=\sum_{n=0}^{pq-1}a_nx^n$ felírásban az összegzés pontosan azokra az n-ekre terjed ki, amelyek együttesen a jó és a rossz intervallumokat adják, a polinom tagjainak száma pedig ekkor éppen pq. A tagsűrűség meghatározása tehát $A(pq)=1$ figyelembevételével a következő.

Definíció. *$\Phi_{pq}(x)$-ben a nemnulla tagok sűrűsége* $\frac{S(pq)}{pq}$.

Vezessük be a következő jelöléseket. Az I és J diszjunkt intervallumokra $I < J$, ha $\sup I \leq \inf J$. $b \in \mathbb{Z}$ esetén jelentse emellett $[b]$ a b-t tartalmazó modulo q maradékosztályt.

2.1.4. Tétel.

a) $\Phi_{pq}(x)$*-ben a* 0*-tól különböző tagok száma* $S(pq) = \frac{2cap}{q} + \frac{c-a}{q}$.

b) $\Phi_{pq}(x)$*-ben a* $\neq 0$ *tagok sűrűsége* $\frac{S(pq)}{pq} = 2\frac{c}{q}(1-\frac{c}{q}) + \frac{\vartheta}{pq} < \frac{1}{2}$*, ahol* $|\vartheta| < 1$.

c) Megadhatók olyan páronként diszjunkt $I_1 < I_2 < ... < I_{q-1}$ *intervallumok, továbbá az* $\{1, ..., q-1\}$*-nek olyan* σ *permutációja, hogy tetszőlegesen választott* $p_k \equiv k \mod q$ $(k \in \{1, ..., q-1\})$ *prímek esetén (ilyenek a Dirichlet-tétel miatt léteznek)* $\frac{S(p_k q)}{p_k q} \in I_{\sigma(k)}$.

d) $\sigma(2) = q-1$*, ezenfelül ha* $p \equiv 2 \mod q$*, akkor* $\frac{S(pq)}{pq} > \frac{1}{2} - \frac{1}{2q^2}$*. (Másképpen mondva* $\Phi_{pq}(x)$*-ben a* 0*-tól különböző tagok sűrűsége a* q *szerinti* $[2]$ *maradékosztályba eső* p *prímekre a legnagyobb).*

Bizonyítás.

a) Közvetlenül adódik a 2.1.2. tételből.

b) Az állítás első felét azonnal kapjuk a)-ból a $\vartheta = \frac{c-a}{q}$ jelölést alkalmazva, ugyanis c és a definíciója értelmében $1 \leq c, a \leq q-1$. Az egyenlőtlenség igazolásához vegyük fel c-t $\frac{q+2j-1}{2}$ alakban, ahol $\frac{3-q}{2} \leq j \leq \frac{q-1}{2}$. Ekkor

$$\frac{S(pq)}{pq} = \frac{2}{q^2}c(q-c) + \frac{c-(q-c)}{pq^2} = \frac{2}{q^2} \cdot \frac{q+2j-1}{2} \cdot \frac{q-(2j-1)}{2} + \frac{2j-1}{pq^2} = \frac{1}{2} - \frac{1}{q^2}\Big(\frac{(2j-1)^2}{2} - \frac{2j-1}{p}\Big)$$

Itt azt kell tehát látnunk, hogy $\frac{(2j-1)^2}{2} > \frac{2j-1}{p}$, ami nyilván igaz, ha $j \neq 1$. Mivel pedig a szakasz elején kikötöttük, hogy $p > 2$, azért egyenlőtlenségünk $j = 1$ esetén is fennáll.

c) Tekintsük továbbra is $\frac{S(pq)}{pq}$-t, és írjuk c-t ezután is $\frac{q+2j-1}{2}$ alakba. Először azt mutatjuk meg, hogy ha j-t úgy rögzítjük, hogy az $1 \leq j \leq \frac{q-1}{2}$ feltétel teljesüljön, akkor $\frac{(2j-1)^2}{2} - \frac{2j-1}{p}$ lehetséges értékei belefoglalhatók a $J_j := \Big[\frac{(2j-1)^2}{2} - \frac{(2j-1)^2}{q+2}, \frac{(2j-1)^2}{2}\Big)$ intervallumba. Ehhez a $\frac{q+2}{2j-1} \leq p$ egyenlőtlenséget kell igazolni. A $j = 1$ esetben $c = \frac{q+1}{2}$, vagyis $p \equiv 2 \mod q$, $p > 2$ miatt tehát ekkor készen vagyunk. Legyen most $j \geq 2$. Mivel $(2j-1, q) = 1$, azért $\{qm + 2 | 0 \leq m \leq 2j-2, m \in \mathbb{Z}\}$ teljes maradékrendszer modulo $2j-1$, emellett $j \geq 2$ miatt $2j-1 \nmid 2$, amikből azt kapjuk, hogy létezik pontosan egy olyan $1 \leq m_0 \leq 2j-2$ egész, melyre $\frac{qm_0+2}{2j-1} \in \mathbb{Z}$. Jelöljük ez utóbbi számot s-sel. Mármost $c \in [2j-1] \cdot [2]^{-1}$ folytán $p \in [2] \cdot [2j-1]^{-1}$, és így $p \equiv s \mod q$. Az m_0-ra vonatkozó korlátokat figyelembe véve $1 < \frac{q+2}{2j-1} \leq s < q$ adódik, amiből $1 < p < \frac{q+2}{2j-1}$ esetén $1 \leq s - p < q$ következik, és ez pedig $q | p - s$-sel együtt nem teljesülhet, vagyis valóban $\frac{q+2}{2j-1} \leq p$. Ezután rögzítsük j-t a $\frac{3-q}{2} \leq j \leq 0$ kikötés mellett. Most azt igazoljuk, hogy

$$\frac{(2j-1)^2}{2} - \frac{2j-1}{p} = \frac{(2j-1)^2}{2} + \frac{-2j+1}{p} \in J_j := \Big(\frac{(2j-1)^2}{2}, \frac{(2j-1)^2}{2} + \frac{(2j-1)^2}{q-2}\Big]$$

Bizonyítandó a $\frac{q-2}{-2j+1} \leq p$ egyenlőtlenség. A $j = 0$ eset triviális. Ha $\frac{3-q}{2} \leq j \leq -1$, akkor az előző gondolatmenethez hasonlóan alkalmas, egyértelműen meghatározott $1 \leq m_0 \leq -2j$ egészre $\frac{qm_0-2}{-2j+1} \in \mathbb{Z}$. Jelölje s ez utóbbi számot. Mivel $p \in [-2] \cdot [-2j+1]^{-1}$, azért $p \equiv s \mod q$, továbbá látható, hogy $1 \leq \frac{q-2}{-2j+1} \leq s < q$, tehát ismételten kész vagyunk. Utolsó lépésben belátjuk, hogy a J_j $(\frac{3-q}{2} \leq j \leq \frac{q-1}{2})$ intervallumok páronként diszjunktak.

$1 \le j \le \frac{q-1}{2}$ esetén $\sup J_j = \inf J_{1-j} = \frac{(2j-1)^2}{2}$, vagyis $J_j \cap J_{1-j} = \emptyset$, és $J_j < J_{1-j}$. Legyen most $1 \le j \le \frac{q-3}{2}$. Igazoljuk, hogy $\sup J_{1-j} < \inf J_{1+j}$. Azt kell látnunk, hogy

$$\frac{(2j-1)^2}{2} + \frac{(2j-1)^2}{q-2} < \frac{(2j+1)^2}{2} - \frac{(2j+1)^2}{q+2} \quad ,$$

ami rendezve a

$$\frac{(2j-1)^2}{q-2} + \frac{(2j+1)^2}{q+2} < 4j \tag{54}$$

alakot ölti, (54) viszont $2j-1 < q-2$ és $2j+1 < q+2$ miatt valóban igaz. Megkaptuk tehát, hogy $1 \le j \le \frac{q-3}{2}$ esetén $J_{1-j} < J_{j+1}$, ami azzal együtt, hogy $1 \le j \le \frac{q-1}{2}$-re $J_j < J_{1-j}$, a bizonyítandó állításunkat adja. Jelöljük most K_j-vel az $\frac{1}{2} - \frac{1}{q^2}J_j$ intervallumot. Ekkor a K_j-k is páronként diszjunktak, továbbá $\frac{S(pq)}{pq} = \frac{1}{2} - \frac{1}{q^2}\left(\frac{(2j-1)^2}{2} - \right.$ $\left. - \frac{2j-1}{p}\right) \in K_j$. (Itt emlékeztetünk rá, hogy a p prímre c jelöli annak $[1, q-1]$-be eső modulo q inverzét, valamint arra, hogy $j = c - \frac{q-1}{2}$). Jelölje ezután $\sigma_i (i = 1, 2, 3, 4)$ az alábbi leképezéseket.

$\sigma_1 : \{1, 2, ..., q-1\} \to \{1, 2, ..., q-1\}$, $\sigma_1(k) \cdot k \equiv 1 \mod q$;
$\sigma_2 : \{1, ..., q-1\} \to \{\frac{3-q}{2}, \frac{5-q}{2}, ..., \frac{q-1}{2}\}$, $\sigma_2(c) = c - \frac{q-1}{2}$;
$\sigma_3 : \{\frac{3-q}{2}, \frac{5-q}{2}, ..., \frac{q-1}{2}\} \to \{1, 2, ..., q-1\}$, $\sigma_3(j) = \begin{cases} 2j-1, & \text{ha } j \ge 1 \\ 2-2j, & \text{ha } j \le 0 \end{cases}$;
$\sigma_4 : \{1, .., q-1\} \to \{1, ..., q-1\}$, $\sigma_4(l) = q - l$.

Megmutatjuk, hogy az $I_{\sigma_4\sigma_3(j)} = K_j \quad (-\frac{q-3}{2} \le j \le \frac{q-1}{2})$ definíció mellett $I_1 < I_2 < ... < I_{q-1}$. Igazolnunk kell, hogy $\sigma_4\sigma_3(j_2) = \sigma_4\sigma_3(j_1) + 1$ esetén $I_{\sigma_4\sigma_3(j_1)} < I_{\sigma_4\sigma_3(j_2)}$, vagyis $K_{j_1} < K_{j_2}$. σ_4 valamint a K_j intervallumok értelmezése miatt azt kell belátnunk, hogy $\sigma_3(j_1) = \sigma_3(j_2) + 1$ fennálltakor $J_{j_2} < J_{j_1}$. Megkülönböztetünk két esetet az alábbiak szerint.

(i) $1 \le j_2 \le \frac{q-1}{2}$. Tegyük fel, hogy j_1 olyan, hogy $\sigma_3(j_1) = \sigma_3(j_2) + 1$. Mivel most $\sigma_3(j_2) = 2j_2 - 1$, azért $\sigma_3(j_1)$ páros, tehát σ_3 definíciója miatt $-\frac{q-3}{2} \le j_1 \le 0$, azaz $\sigma_3(j_1) = 2 - 2j_1$, ami figyelembe véve, hogy $\sigma_3(j_1) = 2j_2$, azt eredményezi, hogy $j_1 = 1 - j_2$. A tétel bizonyításának folyamán pedig már beláttuk, hogy esetünkben $J_{j_2} < J_{1-j_2} = J_{j_1}$.

(ii) $-\frac{q-3}{2} \le j_2 \le 0$. Tegyük fel újra, hogy $\sigma_3(j_1) = \sigma_3(j_2) + 1$. Ekkor $\sigma_3(j_1) = 3 - 2j_2 = 2j_1 - 1$, ahonnan $j_1 = 2 - j_2$, és $j_2 \ne -\frac{q-3}{2}$. Azt kell tehát látnunk, hogy

$$J_{j_2} < J_{2-j_2} \tag{55}$$

Vegyük ehhez föl j_2-t $1 - j$ alakban, ahol most $1 \le j \le \frac{q-3}{2}$. Ekkor (55) a $J_{1-j} < J_{1+j}$ alakot ölti, aminek igaz voltáról szintén meggyőződtünk. Legyen most $\sigma \quad \{1, 2, ..., q-1\}$-nek $\sigma_4\sigma_3\sigma_2\sigma_1$ által adott permutációja. Láttuk, hogy ha $p \equiv k \mod q$ prím, akkor $\frac{S(pq)}{pq} \in K_{\sigma_2\sigma_1(k)} = I_{\sigma_4\sigma_3\sigma_2\sigma_1(k)} = I_{\sigma(k)}$. Ezzel a 2.1.4. tétel $c)$ pontját bebizonyítottuk.

$d)$ Leolvasható a $c)$ pont bizonyításából. □

2.1.5. Állítás. *$\Phi_{pq}(x)$ középső, $\frac{1}{2}(p-1)(q-1)$-edfokú tagjának együtthatója $(-1)^a$.*

Bizonyítás. A 2.1.2. tételt használjuk, és a paritása szerint két esetre bontunk.

(i) $2|a$. Ekkor $2|c-1$ és $2|\frac{ap+1}{q}-1$. A $t = \frac{c-1}{2}$ és $k = \frac{1}{2}(\frac{ap+1}{q}-1)$ választás esetén $tp+kq = \frac{c-1}{2}p + \frac{1}{2}(\frac{ap+1}{q}-1)q = \frac{1}{2}(cp - p + ap + 1 - q) = \frac{1}{2}(p-1)(q-1)$, vagyis (48) miatt az $\frac{1}{2}(p-1)(q-1)$-edfokú tag együtthatója valóban 1.

(ii) $2 \nmid a$. Ekkor a $t = \frac{a-1}{2}$ és $k = \frac{1}{2}(\frac{cp-1}{q}-1)$ választással $tp+kq+1 = \frac{1}{2}(ap-p+cp-1-q+2) = \frac{1}{2}(p-1)(q-1)$, tehát (48) szerint most a középső tag együtthatója -1. □

2.1.6. Állítás. *Jelölje $m(pq)$ a $\Phi_{pq}(x)$-ben előforduló egymásutáni nemnulla tagok maximális számát. Ekkor*

$$m(pq) \leq \min(2c+1, 2a+1) \tag{56}$$

és $p \equiv 2 \mod q$ esetén (56) egyenlőséggel áll.

Bizonyítás. Tegyük fel, hogy $\Phi_{pq}(x)$-ben megadható $2c+2$ egymás utáni $\neq 0$ együtthatójú tag. Akkor a $\Phi_{pq}(x) = \sum_{n=0}^{(p-1)(q-1)} a_n x^n$ jelölést használva 2.1.3. értelmében alkalmas l-re $a_{l+2j} = 1$ minden $0 \leq j \leq c$ esetén. Továbbmenve, $c+1 \leq q$ miatt az $l+2j$ számok páronként inkongruensek modulo q, ami ellentmond annak, hogy a 2.1.2. tétel alapján a $+1$ együtthatójú tagok kitevői belefoglalhatók c darab modulo q maradékosztályba. Beláttuk tehát, hogy $m(pq) \leq 2c+1$, és ugyanígy látható be $m(pq) \leq 2a+1$ is. Legyen most $p = qm+2$ ($m \in \mathbb{N}$). Ekkor $c = \frac{q+1}{2}$, és $a = \frac{q-1}{2}$, vagyis q darab egymást követő $\neq 0$ együtthatót kell felmutatnunk $\Phi_{pq}(x)$-ben. Azt igazoljuk, hogy a polinom "közepén" elhelyezkedik q darab ilyen tag, azaz $0 \leq j \leq q-1$ esetén $a_{(p-2)\frac{q-1}{2}+j} \neq 0$. Mivel 2.1.5. miatt $a_{(p-1)\frac{q-1}{2}} = (-1)^{\frac{q-1}{2}}$, továbbá 2.1.3. szerint a szomszédos $\neq 0$ tagok együtthatói előjelben eltérnek, azért azt kell csak látnunk, hogy $0 \leq j \leq \frac{q-1}{2}$ esetén $a_{(p-2)\frac{q-1}{2}+2j} = 1$.

A 2.1.2. tétel szerint most

$$\Phi_{pq}(x) = \sum_{t=0}^{\frac{q-1}{2}} \sum_{k=0}^{\frac{q-1}{2}m} x^{tp+kq} - \sum_{t=0}^{\frac{q-3}{2}} \sum_{k=0}^{\frac{q+1}{2}m} x^{tp+kq+1} \tag{57}$$

(57) alapján garantálni akarjuk a

$$(p-2)\frac{q-1}{2} + 2j = tp + kq \quad (0 \leq t \leq \frac{q-1}{2}, \quad 0 \leq k \leq \frac{q-1}{2}m; \quad t,k \in \mathbb{Z}) \tag{58}$$

előállítást minden $0 \leq j \leq \frac{q-1}{2}$ egészre. $p \equiv 2 \mod q$ miatt (58) fennálltakor $t = j$, vagyis $kq = (p-2)(\frac{q-1}{2} - j) = mq(\frac{q-1}{2} - j)$, amiből $0 \leq k \leq m\frac{q-1}{2}$. Lépéseink megfordíthatók, tehát a $k = m(\frac{q-1}{2} - j)$, $t = j$ választással $(p-2)\frac{q-1}{2} + 2j$-nek (58)-beli előállítását nyerjük. □

Az ebben a részben foglalt bizonyítások döntő többsége tőlem származik, a kivételt 2.1.3.-ban a jó és rossz intervallumok bevezetésének ötlete képezi, melyet [2]-ben olvastam. Ennek ellenére a közölt eredmények zöme a szakirodalomban fellelhető, megtalálhatóságukat az alábbiakban ismertetem. 2.1.1. tétel: [3], 2.1.2. tétel: lényegében [2] (4), illetve [4] (22) sora tartalmazza. 2.1.4. tétel a) [2], 2.1.4. tétel $b) - d)$ saját eredmények. 2.1.5. állítás [5], 2.1.6. állítás saját eredmény.

2.2. Felső becslések $A(n)$-re

Ebben a szakaszban két eredményt mutatunk be. Előbb Bang [6] klasszikus becslését javítjuk, mely szerint ha $r < q < p$ prímek, akkor $A(pqr) \leq r-1$, majd általánosságban állapítunk meg $A(n)$-re olyan felső korlátot, melynek értéke nem függ az n két legnagyobb prímosztójától.

2.2.1. Tétel. *Legyenek $2 < r < q < p$ prímek. Ekkor $A(pqr) \leq \frac{3r-1}{4}$.*

Lényegében ezt az eredményt érte el Marion Beiter [7] is, én saját bizonyításomat adom a tételre. Mielőtt a bizonyításhoz hozzákezdenénk, előrebocsátunk egy kis segédtételt.

2.2.2. Lemmácska. *Legyen $f(x) = \sum_{j=0}^{m} a_j x^j \in \mathbb{C}[x]$ és $d \in \mathbb{N}^+$. Ekkor $x^d - 1 | f(x)$ pontosan akkor teljesül, ha minden $0 \leq b \leq d-1, b \in \mathbb{N}$ esetén* $\sum\limits_{\substack{j=0 \\ j \equiv b(d)}}^{m} a_j = 0$.

Bizonyítás. Legyen $0 \le b \le d-1$ rögzített egész. Ekkor $j \in \mathbb{N}$, $j \equiv b(d)$ esetén $x^d - 1 | x^j - x^b$, vagyis

$$\sum_{\substack{j=0 \\ j\equiv b(d)}}^{m} a_j x^j \equiv (\sum_{\substack{j=0 \\ j\equiv b(d)}}^{m} a_j) x^b \mod x^d - 1 \quad \text{, amiből}$$

$$f(x) = \sum_{j=0}^{m} a_j x^j = \sum_{b=0}^{d-1} \sum_{\substack{j=0 \\ j\equiv b(d)}}^{m} a_j x^j \equiv \sum_{b=0}^{d-1} (\sum_{\substack{j=0 \\ j\equiv b(d)}}^{m} a_j) x^b \mod x^d - 1 \tag{59}$$

Jelöljük az (59) jobb szélén álló polinomot $g(x)$-szel. Ekkor (59) miatt az $x^d - 1 | f(x)$ és az $x^d - 1 | g(x)$ oszthatóságok ekvivalensek, s mivel g foka legfeljebb $d-1$, azért $x^d - 1 | g(x)$ pontosan akkor igaz, ha $g(x) \equiv 0$, amivel lemmácskánkat igazoltuk.

Rátérünk 2.2.1. tétel bizonyítására. Jelölje p^* illetve q^* a p és a q azon inverzét modulo r, melyre $|p^*| \le \frac{r-1}{2}$ és $|q^*| \le \frac{r-1}{2}$. A bizonyítás során $|p^*|$ és $|q^*|$ nagyságától függően az alábbi két esetet különböztetjük meg.

1. eset. $|p^*| \le \frac{r-1}{4}$ vagy $|q^*| \le \frac{r-1}{4}$

2. eset. $|p^*| \ge \frac{r+1}{4}$ és $|q^*| \ge \frac{r+1}{4}$

Az első esetben formális hatványsorok használata, a másodikban pedig a körosztási polinom megfelelő átalakítása visz célhoz. A bizonyítás érdekessége, hogy a használt két módszer kiegészíti egymást abban az értelemben, hogy amint az egyik már nem adja a kívánt eredményt, a másik éppen alkalmazhatóvá válik.

Az 1. eset tárgyalása. Legyen $n, \alpha \in \mathbb{N}$; $\varepsilon_1, \varepsilon_2 \in \{0,1\}$, és jelölje $m_n(\alpha, \varepsilon_1, \varepsilon_2)$ azon (β, γ, λ) hármasok számát, melyekre

$$\alpha pq + \beta pr + \gamma qr + \lambda + \varepsilon_1 p + \varepsilon_2 q = n, \qquad \beta, \gamma, \lambda \in \mathbb{N}; \lambda \le r-1 \tag{60}$$

$\Phi_{pqr}(x)$-et az 1.1.1. lemma alapján felírva, majd $\mathbb{Q}\big[[x]\big]$-ben továbbalakítva

$$\Phi_{pqr}(x) = \frac{(1-x^{pqr})(1-x^r)(1-x^q)(1-x^p)}{(1-x)(1-x^{pq})(1-x^{pr})(1-x^{qr})} =$$

$$= (1-x^{pqr}) \sum_{\alpha\ge 0} \sum_{\beta\ge 0} \sum_{\gamma\ge 0} \sum_{\lambda=0}^{r-1} \sum_{\varepsilon_1=0}^{1} \sum_{\varepsilon_2=0}^{1} (-1)^{\varepsilon_1+\varepsilon_2} x^{\alpha pq+\beta pr+\gamma qr+\lambda+\varepsilon_1 p+\varepsilon_2 q} \tag{61}$$

Mivel $\varphi(pqr) + 1 = (r-1)(q-1)(p-1) + 1 < (r-1)pq < pqr$, azért (61)-ből

$$\Phi_{pqr}(x) \equiv \sum_{\alpha=0}^{r-2} \sum_{\beta\ge 0} \sum_{\gamma\ge 0} \sum_{\lambda=0}^{r-1} \sum_{\varepsilon_1=0}^{1} \sum_{\varepsilon_2=0}^{1} (-1)^{\varepsilon_1+\varepsilon_2} x^{\alpha pq+\beta pr+\gamma qr+\lambda+\varepsilon_1 p+\varepsilon_2 q} \mod x^{\varphi(pqr)+1} \tag{62}$$

$\mathbb{Q}\big[[x]\big]$-ben. A körosztási polinom együtthatóira a $\Phi_{pqr}(x) = \sum_{n=0}^{\varphi(pqr)} a_n x^n$ jelölést alkalmazva (62)-ből a következőt kapjuk.

$$a_n = \sum_{\alpha=0}^{r-2} m_n(\alpha,0,0) + \sum_{\alpha=0}^{r-2} m_n(\alpha,1,1) - \sum_{\alpha=0}^{r-2} m_n(\alpha,0,1) - \sum_{\alpha=0}^{r-2} m_n(\alpha,1,0) \quad 0 \le n \le \varphi(pqr) \tag{63}$$

Könnyen látható, hogy ha $0 \le n \le \varphi(pqr)$ rögzített egész, továbbá $\alpha \in \mathbb{N}, \varepsilon_1, \varepsilon_2 \in \{0,1\}$ ugyancsak fixek, akkor (60)-ben β, γ és λ helyébe legfeljebb egy-egy szám írható, így ezen feltételek teljesülésekor $m_n(\alpha, \varepsilon_1, \varepsilon_2)$ értéke 0 vagy 1. Mivel a körosztási polinom reciprokpolinom (ez pl. abból látható, hogy $n \ge 2$ esetén (6) jobboldala nem változik, ha x-et és y-t felcseréljük), azért az a_n becslésénél feltehetjük, hogy $n \le \frac{\varphi(pqr)}{2}$. Ekkor viszont $\alpha \ge \frac{r-1}{2}$ esetén nyilván $m_n(\alpha, \varepsilon_1, \varepsilon_2) = 0, (\varepsilon_1, \varepsilon_2 \in \{0,1\})$ vagyis (63) az alábbival helyettesíthető.

$$a_n = \sum_{\alpha=0}^{\frac{r-3}{2}} m_n(\alpha,0,0) + \sum_{\alpha=0}^{\frac{r-3}{2}} m_n(\alpha,1,1) - \sum_{\alpha=0}^{\frac{r-3}{2}} m_n(\alpha,0,1) - \sum_{\alpha=0}^{\frac{r-3}{2}} m_n(\alpha,1,0) \quad 0 \le n \le \frac{\varphi(pqr)}{2} \tag{64}$$

amiből egyébként $m_n(\alpha, \varepsilon_1, \varepsilon_2)$ lehetséges értékeit figyelembe véve közvetlenül adódik [6].

Tegyük fel, hogy p-re és q-ra az 1. esetbeli feltétel teljesül. Ez az alábbi esetek valamelyikének fennállását jelenti.

(i) $1 \le p^* \le \frac{r-1}{4}$

(ii) $-\frac{r-1}{4} \le p^* \le -1$

(iii) $1 \le q^* \le \frac{r-1}{4}$

(iv) $-\frac{r-1}{4} \le q^* \le -1$

A bizonyítást (i)-re, majd (ii)-re hajtjuk végre, a másik két esetben a tétel verifikációja analóg. Tekintsük az (i) esetet, és legyen $p^*p = rk+1$. Ekkor az $n = \alpha pq+\beta pr+\gamma qr+\lambda+\varepsilon_1 p$ $(0 \le n \le \frac{\varphi(pqr)}{2}; n, \alpha, \beta, \gamma, \lambda \in \mathbb{N}, \lambda \le r-1, \varepsilon_1 \in \{0,1\})$ előállításból $n = (\alpha - p^*)pq + \beta pr + (\gamma + k)qr + \lambda + \varepsilon_1 p + q$, ami $\alpha \ge p^*$ esetén $k \in \mathbb{N}$ miatt szintén az n (60) típusú előállítása, így ha $p^* \le \alpha \le \frac{r-3}{2}$, akkor

$$m_n(\alpha, 0, 0) - m_n(\alpha - p^*, 0, 1) \neq 1 \tag{65}$$

és

$$m_n(\alpha, 1, 0) - m_n(\alpha - p^*, 1, 1) \neq 1 \tag{66}$$

Legyen most $0 \le n \le \frac{\varphi(pqr)}{2}$ rögzített, és $1 \le j \le 8$ esetén definiáljuk s_j-t a következők szerint.

$$s_1 = \sum_{\alpha=0}^{p^*-1} m_n(\alpha,0,0), \quad s_2 = \sum_{\alpha=p^*}^{\frac{r-3}{2}} m_n(\alpha,0,0), \quad s_3 = \sum_{\alpha=0}^{\frac{r-3}{2}-p^*} m_n(\alpha,1,1), \quad s_4 = \sum_{\alpha=\frac{r-1}{2}-p^*}^{\frac{r-3}{2}} m_n(\alpha,1,1),$$

$$s_5 = \sum_{\alpha=0}^{\frac{r-3}{2}-p^*} m_n(\alpha,0,1), \quad s_6 = \sum_{\alpha=\frac{r-1}{2}-p^*}^{\frac{r-3}{2}} m_n(\alpha,0,1), \quad s_7 = \sum_{\alpha=0}^{p^*-1} m_n(\alpha,1,0), \quad s_8 = \sum_{\alpha=p^*}^{\frac{r-3}{2}} m_n(\alpha,1,0)$$

(64)-et az s_j-k segítségével írva fel

$$a_n = \sum_{j=1}^{4} s_j - \sum_{j=5}^{8} s_j \tag{67}$$

(65) miatt pedig

$$s_2 - s_5 = \sum_{\alpha=p^*}^{\frac{r-3}{2}} (m_n(\alpha,0,0) - m_n(\alpha-p^*,0,1)) \le 0,$$

emellett $s_1 \le p^*, s_3 + s_4 \le \frac{r-1}{2}$, és persze $s_6, s_7, s_8 \ge 0$, amiért (67)-ből

$$a_n \le \frac{r-1}{2} + p^* \le \frac{3(r-1)}{4} \tag{68}$$

(66)-ból ugyanígy

$$s_3 - s_8 = \sum_{\alpha=p^*}^{\frac{r-3}{2}} (m_n(\alpha-p^*,1,1) - m_n(\alpha,1,0)) \ge 0,$$

emellett $s_5 + s_6 \le \frac{r-1}{2}$, $s_7 \le p^*$ és $s_1, s_2, s_4 \ge 0$, amiért megint (67)-ből

$$a_n \ge -\frac{r-1}{2} - p^* \ge -\frac{3(r-1)}{4} \tag{69}$$

(68) és (69) egybevetéséből pedig $|a_n| \leq \frac{3(r-1)}{4}$ minden rögzített $0 \leq n \leq \frac{\varphi(pqr)}{2}$ esetén, vagyis $A(pqr) \leq \frac{3(r-1)}{4} < \frac{3r-1}{4}$.

Vizsgáljuk most (ii)-t, és legyen $p' = -p^*$. Ekkor $1 \leq p' \leq \frac{r-1}{4}$ és $p'p = rk - 1$, ahol $k \in \mathbb{N}$.

$$\text{Az } n = \alpha pq + \beta pr + \gamma qr + \lambda + \varepsilon_1 p + q \quad (n, \alpha, \beta, \gamma, \lambda \in \mathbb{N}, n \leq \frac{\varphi(pqr)}{2}, \lambda \leq r-1, \varepsilon_1 \in \{0,1\})$$

felírásból $n = (\alpha - p')pq + \beta pr + (\gamma + k)qr + \lambda + \varepsilon_1 p$, ami $\alpha \geq p'$ fennálltakor szintén (60) alakú előállítása az n számnak, tehát $p' \leq \alpha \leq \frac{r-3}{2}$ esetén

$$m_n(\alpha, 1, 1) - m_n(\alpha - p', 1, 0) \neq 1 \tag{70}$$

és

$$m_n(\alpha, 0, 1) - m_n(\alpha - p', 0, 0) \neq 1 \tag{71}$$

(i)-hez hasonlóan legyen $0 \leq n \leq \frac{\varphi(pqr)}{2}$ újból rögzített, és $1 \leq j \leq 8$ esetén definiáljuk az s'_j összeget az alábbiak szerint.

$$s'_1 = \sum_{\alpha=0}^{\frac{r-3}{2}-p'} m_n(\alpha, 0, 0), \quad s'_2 = \sum_{\alpha=\frac{r-1}{2}-p'}^{\frac{r-3}{2}} m_n(\alpha, 0, 0), \quad s'_3 = \sum_{\alpha=0}^{p'-1} m_n(\alpha, 1, 1), \quad s'_4 = \sum_{\alpha=p'}^{\frac{r-3}{2}} m_n(\alpha, 1, 1),$$

$$s'_5 = \sum_{\alpha=0}^{p'-1} m_n(\alpha, 0, 1), \quad s'_6 = \sum_{\alpha=p'}^{\frac{r-3}{2}} m_n(\alpha, 0, 1), \quad s'_7 = \sum_{\alpha=0}^{\frac{r-3}{2}-p'} m_n(\alpha, 1, 0), \quad s'_8 = \sum_{\alpha=\frac{r-1}{2}-p'}^{\frac{r-3}{2}} m_n(\alpha, 1, 0)$$

Értelemszerűen $a_n = \sum_{j=1}^{4} s'_j - \sum_{j=5}^{8} s'_j$, és (70)-ből $s'_4 - s'_7 \leq 0$, (71)-ből pedig $s'_1 - s'_6 \geq 0$, így $|a_n| \leq \frac{3(r-1)}{4}$, s vele együtt $A(pqr) \leq \frac{3r-1}{4}$ jelen esetben is igaz.

A tétel bizonyítása a 2. esetben. Jelölje c a q $[1, r-1]$-be eső inverzét modulo r, és legyen $a = r - c$. A (8) képlet háromszori alkalmazásával a körosztási polinomra az alábbit kapjuk.

$$\Phi_{pqr}(x) = \frac{\Phi_{qr}(x^p)(x^q - 1)\sum_{j=0}^{r-1} x^j}{x^{qr} - 1} \tag{72}$$

A 2.1.2. tétel alapján (72) jobboldalának számlálója pedig

$$(\sum_{t=0}^{c-1} \sum_{k=0}^{\frac{aq+1}{r}-1} x^{(tq+kr)p} - \sum_{t=0}^{a-1} \sum_{k=0}^{\frac{cq-1}{r}-1} x^{(tq+kr+1)p})(x^q - 1)\sum_{j=0}^{r-1} x^j \tag{73}$$

A 2.2.2. lemmácska és amiatt, hogy (72)-ből következően $x^{qr} - 1$ osztja a (73) polinomot, a (73)-beli szorzás elvégzése után (az esetleges azonos kitevőjű tagok összevonása előtt; ilyenek pontosan akkor léteznek, ha $p < q + r$) minden $[b]$ modulo qr maradékosztály esetén a $[b]$-be eső kitevőjű $+1$ együtthatójú tagok és a $[b]$-be eső kitevőjű -1 együtthatójú tagok száma megegyezik. Jelölje ezt a számot m_b. Eszerint minden $0 \leq b \leq qr - 1$ egészhez léteznek olyan $0 \leq s_{b,1} \leq s_{b,2} \leq ... \leq s_{b,m_b}$ és olyan $0 \leq t_{b,1} \leq t_{b,2} \leq ... \leq t_{b,m_b}$ egészek, melyekre $s_{b,j} \equiv t_{b,j} \equiv b \mod qr$ minden $1 \leq j \leq m_b$-re, és amelyekkel (73) a

$$\sum_{b=0}^{qr-1} \sum_{j=1}^{m_b} x^{s_{b,j}} - \sum_{b=0}^{qr-1} \sum_{j=1}^{m_b} x^{t_{b,j}}$$

alakban írható. Mármost ekkor (72)-ből

$$\Phi_{pqr}(x) = \sum_{b=0}^{qr-1} \sum_{j=1}^{m_b} \frac{x^{s_{b,j}} - x^{t_{b,j}}}{x^{qr}-1}$$

Legyen $f_b(x) = \sum_{j=1}^{m_b} \frac{x^{s_{b,j}} - x^{t_{b,j}}}{x^{qr}-1}$, és jelölje $A_{pqr}^{(b)}$ az $f_b(x)$ legnagyobb abszolútértékű együtthatójának abszolútértékét $(b = 0, 1, ..., qr-1)$. Az $\frac{x^{s_{b,j}} - x^{t_{b,j}}}{x^{qr}-1}$ polinomnak $s_{b,j} > t_{b,j}$ esetén minden $\neq 0$ együtthatója $+1$, ha $s_{b,j} < t_{b,j}$, akkor pedig -1, amiért $A_{pqr}^{(b)} \leq m_b$. Be lehet látni, hogy tetszőleges b, i, j esetén $s_{b,i} \neq t_{b,j}$, ennek meggondolását az olvasóra bízzuk. Könnyen látható továbbá, hogy $\frac{x^{s_{b,j}} - x^{t_{b,j}}}{x^{qr}-1}$ minden $\neq 0$ tagjának kitevője kongruens b-vel modulo qr, így ugyanez igaz $f_b(x)$-re is, amiből $A(pqr) = \max_{0 \leq b \leq qr-1} A_{pqr}^{(b)} \leq \max_{0 \leq b \leq qr-1} m_b$. Nyilvánvaló, hogy $\max_{0 \leq b \leq qr-1} m_b$ megegyezik azzal a legkisebb M egésszel, melyre az $\{s_{b,j} | 0 \leq b \leq qr-1, 1 \leq j \leq m_b\}$ kitevőrendszer belefoglalható M darab modulo qr teljes maradékrendszerbe. Ha tehát azt az elemrendszert, ami a (73) szorzás elvégzése után a kapott $+1$ együtthatójú tagok kitevőinek felsorolásakor fellép, elegendően kicsi számú (azaz $[\frac{3r-1}{4}]$ darab) modulo qr teljes maradékrendszerbe bele tudjuk foglalni, a bizonyítással kész vagyunk.

Vezessük be a következőket. Ha az egész számokból álló A elemrendszer olyan, hogy alkalmas m, s egészekre $y \equiv s \mod m$ minden $y \in A$ esetén, akkor erre az $A \equiv s \mod m$ jelölést használjuk. Ha $A \equiv s \mod m$ mellett még valamely B elemrendszerre $B \equiv s \mod m$ is fennáll, úgy ezt a $A \equiv B \mod m$ írásmóddal tűntetjük fel. Jelölje rögzített $0 \leq t_1 \leq c-1$ és $0 \leq t_2 \leq a-1$ esetén H_{1,t_1} valamint H_{2,t_2} a következő halmazokat.

$$H_{1,t_1} = \{(t_1 q + kr)p + q | 0 \leq k \leq \frac{aq+1}{r} - 1\} \text{ és } H_{2,t_2} = \{(t_2 q + kr + 1)p | 0 \leq k \leq \frac{cq-1}{r} - 1\}$$

Ekkor a fent említett kitevőrendszer:

$$\begin{aligned} \{s_{b,j} | 0 \leq b \leq qr-1, 1 \leq j \leq m_b\} &= (\cup_{t_1=0}^{c-1} H_{1,t_1}) \cup (\cup_{t_2=0}^{a-1} H_{2,t_2}) + \{0, 1, ..., r-1\} = \\ &= \cup_{t_1=0}^{c-1} (H_{1,t_1} + \{0, 1, ..., r-1\}) \cup \cup_{t_2=0}^{a-1} (H_{2,t_2} + \{0, 1, ..., r-1\}) \end{aligned} \tag{74}$$

ahol $A + B$ a szokásos komplexusösszeadást jelenti $\mathbb{Z}$-ben. Ezen rendszert akarjuk minél kevesebb modulo qr teljes maradékrendszerbe belefoglalni. Nyilvánvaló, hogy H_{1,t_1} illetve H_{2,t_2} elemei páronként inkongruensek modulo q, modulo r viszont azonos maradékokat adnak, így a $H_{1,t_1} + \{0, 1, ..., r-1\}$ és a $H_{2,t_2} + \{0, 1, ..., r-1\}$ halmazok részei egy-egy modulo qr teljes maradékrendszernek. Könnyen látható ezen túlmenően, hogy $H_{1,t_1} \cup H_{2,t_2}$ teljes maradékrendszer modulo q (ugyanis H_{1,t_1} és H_{2,t_2} helyett nyilván tekinthető a $H'_{1,t_1} = \{kr | 0 \leq k \leq \frac{aq+1}{r} - 1\}$ illetve a $H'_{2,t_2} = \{kr + 1 | 0 \leq k \leq \frac{cq-1}{r} - 1\}$, majd H'_{2,t_2} helyett a

$$H''_{2,t_2} = \{(k + \frac{aq+1}{r})r | 0 \leq k \leq \frac{cq-1}{r} - 1\} = \{kr | \frac{aq+1}{r} \leq k \leq q-1\}$$

halmaz), így $H_{1,t_1} \equiv H_{2,t_2} \mod r$ esetén $H_{1,t_1} \cup H_{2,t_2} + \{0, 1, ..., r-1\}$ teljes maradékrendszer modulo qr. Végül az is rögtön látható, hogy a $H_{1,t_1} \equiv H_{2,t_2} \mod r$ feltétel a kezelhetőbb $p^* - q^* \equiv t_2 - t_1 \mod r$ alakkal ekvivalens, hiszen a $H_{1,t_1} \equiv H_{2,t_2} \mod r$ kongruencia a $t_1 qp + q \equiv t_2 qp + p \mod r$ feltétel teljesülését jelenti, amit átrendezve, majd $p^* q^*$-gal szorozva a kívánt formához jutunk. Jelölje most $M_r(p, q)$ azon kiválasztható (t_1, t_2) párok számát, melyekre $0 \leq t_1 \leq c-1, 0 \leq t_2 \leq a-1$, és $p^* - q^* \equiv t_2 - t_1 \mod r$ teljesül. Megjegyezzük, hogy nyilvánvalóan $0 \leq t'_1 \leq c-1, t_2 - t_1 \equiv t_2 - t'_1 \mod r$-ből $t'_1 = t_1$, és ugyanígy $0 \leq t'_2 \leq a-1, t_2 - t_1 \equiv t'_2 - t_1 \mod r$-ből $t'_2 = t_2$ következik. Mivel t_1 és t_2 együttesen összesen r értéket vesz fel, azért az összes H_{i,t_i} halmazok száma is r, vagyis (74) az eddigiek miatt belefoglalható $r - M_r(p, q)$ darab modulo qr teljes maradékrendszerbe. A bizonyítás befejezéséhez elegendő tehát a következőt megmutatni.

Állítás. $M_r(p, q) = \min(|p^*|, |q^*|)$

Állításunk bizonyítása végett jelöljük I-vel a $\{t_2 - t_1 | 0 \leq t_1 \leq c-1, \quad 0 \leq t_2 \leq a-1, \quad t_1, t_2 \in \mathbb{Z}\} = [1-c, a-1] \cap \mathbb{Z}$ "intervallumot". Ekkor $p^* \not\equiv 0 \mod r$ miatt létezik olyan $j \in I$, melyre $p^* - q^* \equiv j \mod r$, vagyis $M_r(p,q) \geq 1$, ahonnan Bang[6] eredménye ismételten következik. Mivel I elemei páronként inkongruensek modulo r, azért j egyértelműen meghatározott. Célunk igazolni hogy j-t $\min(|p^*|, |q^*|)$-féleképpen lehet $t_2 - t_1$ alakban előállítani, ahol $t_1, t_2 \in \mathbb{N}$, $t_1 \leq c-1$, $t_2 \leq a-1$.

Tegyük fel először, hogy $q^* > 0$. Ekkor $c = q^* \leq \frac{r-1}{2} < a$. Megkülönböztetjük az alábbi négy esetet.

(i) $1 - c \leq j \leq 0$

(ii) $0 \leq j \leq \frac{a-c-1}{2}$

(iii) $\frac{a-c+1}{2} \leq j \leq a - c$

(iv) $a - c \leq j \leq a - 1$

A felsorolt esetekben verifikáljuk állításunkat.

(i) $t_2 - t_1 = j$-ből $t_2 \geq 0$ miatt $-j \leq t_1 \leq c-1$, s ezen t_1 számok mindegyikéhez párosítható megfelelő $t_2 = t_1 + j$ érték, hiszen $0 \leq t_1 + j \leq c-1 < a-1$. Esetünkben tehát $M_r(p,q) = c+j$. Másrészt $p^* \equiv q^* + j = c + j \mod r$, s minthogy $-\frac{r-1}{2} \leq p^* \leq \frac{r-1}{2}$ és $1 \leq c + j \leq c \leq \frac{r-1}{2}$, azért $p^* = c + j$, ahonnan $q^* = c$ figyelembevételével kívánt eredményünk leolvasható.

(ii) Most $0 \leq t_1 \leq c-1$ esetén $0 \leq t_1 + j \leq c - 1 + \frac{a-c-1}{2} \leq \frac{r-3}{2} < a - 1$, vagyis minden $t_1 \in [0, c-1] \cap \mathbb{Z}$-hez található olyan $t_2 \in [0, a-1] \cap \mathbb{Z}$, melyre $j = t_2 - t_1$, azaz $M_r(p,q) = c$. Másrészt $p^* \equiv c + j \mod r$ és $1 \leq c + j \leq \frac{r-1}{2}$ egybevetéséből $p^* = c + j$, így állításunk helyessége most is leolvasható.

(iii) Azonos módon (ii)-vel $M_r(p,q) = c$, másrészt most $\frac{r+1}{2} \leq c + j \leq a \leq r - 1$, vagyis $p^* = c + j - r = j - a$, tehát $|p^*| = a - j \geq c = q^*$, készen vagyunk.

(iv) $t_1 + j = t_2 \leq a-1$-ből $t_1 \leq a-1-j \leq c-1$, és megfordítva, minden $0 \leq t_1 \leq a-1-j$-hez megadható a megfelelő $j \leq t_2 \leq a-1$ érték, azaz $M_r(p,q) = a - j$. Másrészt $\frac{r+1}{2} \leq a \leq c + j \leq r - 1$ miatt $p^* = c + j - r = j - a$, vagyis $|p^*| = a - j \leq c = q^*$, készen vagyunk.

Tegyük most fel, hogy $q^* < 0$. Ekkor $q^* = c - r$, $|q^*| = a \leq \frac{r-1}{2} < c$. Itt a következő esetekre bontunk.

(i) $1 - c \leq j \leq a - c$

(ii) $a - c \leq j \leq \frac{a-c-1}{2}$

(iii) $\frac{a-c+1}{2} \leq j \leq 0$

(iv) $0 \leq j \leq a - 1$

A mostani esetek a fentiekhez hasonló gondolatmenettel intézhetők el. Igazoltuk tehát, hogy $M_r(p,q) = \min(|p^*|, |q^*|)$, továbbá feltevésünk szerint most $\min(|p^*|, |q^*|) \geq \frac{r+1}{4}$, ennélfogva a (74) elemrendszer belefoglalható legfeljebb $r - \frac{r+1}{4} = \frac{3r-1}{4}$ darab modulo qr teljes maradékrendszerbe. Ez pedig a korábban leírtak szerint azt jelenti, hogy $A(pqr) \leq \frac{3r-1}{4}$.□

Az elvégzett bizonyítás 1. esetének alapötlete Marion Beiter[8] cikkéből származik, míg a 2. eset tárgyalása kizárólag saját elgondolásokon nyugszik.

A következőkben $\omega(m) \geq 4$ esetén adunk $A(m)$-re felső becslést.

2.2.3. Tétel. *Legyen $k \geq 4$ és $2 < p_1 < p_2 < ... < p_k$ prímek. Ekkor*

a) $A(p_1 p_2 p_3 p_4) < \frac{3}{4} p_1^3 p_2$

b) $k \geq 5$ esetén

$$A(\prod_{l=1}^{k} p_l) < \left(\frac{3}{8}\right)^{2^{k-5}} \prod_{l=1}^{k-2} p_l^{2^{k-1-l}-1} \tag{75}$$

A bizonyításhoz szükségünk lesz néhány segédtételre.

2.2.4. Lemma. *Ha $2 < r < q < p$ prímek, akkor $S(pqr) < \frac{pqr^2}{2}$*

Bizonyítás. Használjuk a 2.2.1. igazolásánál alkalmazott jelöléseket és gondolatokat. Legyen $1 \leq j \leq \frac{r-1}{2}$ egész, és tegyük fel, hogy $(j-1)pq \leq n \leq jpq-1$. Ekkor $a_n = \sum_{\alpha=0}^{j-1} (m_n(\alpha,0,0) + m_n(\alpha,1,1) - m_n(\alpha,0,1) - m_n(\alpha,1,0))$, amiből $|a_n| \leq 2j$. Mivel $\frac{1}{2}\varphi(pqr) \leq \frac{r-1}{2}pq - 1$, azért $\sum_{n=0}^{\varphi(pqr)/2} |a_n| \leq 2pq \sum_{j=1}^{\frac{r-1}{2}} j = pq\frac{r^2-1}{4}$, és innen felhasználva, hogy $\Phi_{pqr}(x)$ reciprokpolinom, kapjuk, hogy $S(pqr) \leq pq\frac{r^2-1}{2} < \frac{pqr^2}{2}$.

Most a körosztási polinomot együtthatóbecslés leolvasására alkalmas alakra hozzuk.

2.2.5. Lemma. *Legyen $k \geq 2$ és $p_1 < ... < p_k$ prímek. Ekkor*

$$\Phi_{p_1 \dots p_k}(x) = \frac{\Phi_{p_1 \dots p_{k-1}}(x^{p_k}) \prod_{j=0}^{k-2} \Phi_{p_1 \dots p_j}(x^{p_{j+2} \cdots p_{k-1}})}{x^{p_1 \cdots p_{k-1}} - 1} \tag{76}$$

Bizonyítás. A bizonyítás során k-szor alkalmazzuk (8)-at, először az eredeti körosztási polinomra, majd minden további lépésben az aktuális tört nevezőjére. Teljes indukcióval megmutatjuk, hogy minden $1 \leq i \leq k$-ra az i-edik átalakítás után

$$\Phi_{p_1 \dots p_k}(x) = \frac{\Phi_{p_1 \dots p_{k-1}}(x^{p_k}) \prod_{j=1}^{i-1} \Phi_{p_1 \dots p_{k-j-1}}(x^{p_{k-j+1} \cdots p_{k-1}})}{\Phi_{p_1 \dots p_{k-i}}(x^{p_{k-i+1} \cdots p_{k-1}})} \tag{77}$$

Állításunk $i = 1$-re (8) segítségével közvetlenül adódik. Legyen most $1 \leq i \leq k-1$, és tegyük fel, hogy (77) igaz i-re. Az $n = \prod_{l=1}^{k-i-1} p_l$, $p = p_{k-i}$ választás mellett a nevezőre (8)-at alkalmazva

$$\Phi_{p_1 \dots p_k}(x) = \frac{\Phi_{p_1 \dots p_{k-1}}(x^{p_k}) \Phi_{p_1 \dots p_{k-i-1}}(x^{p_{k-i+1} \cdots p_{k-1}}) \prod_{j=1}^{i-1} \Phi_{p_1 \dots p_{k-1-j}}(x^{p_{k+1-j} \cdots p_{k-1}})}{\Phi_{p_1 \dots p_{k-i-1}}(x^{p_{k-i} p_{k-i+1} \cdots p_{k-1}})} =$$

$$= \frac{\Phi_{\prod_{l=1}^{k-1} p_l}(x^{p_k}) \prod_{j=1}^{i} \Phi_{p_1 \dots p_{k-1-j}}(x^{\prod_{l=k+1-j}^{k-1} p_l})}{\Phi_{\prod_{l=1}^{k-1-i} p_l}(x^{\prod_{j=k-i}^{k-1} p_j})},$$

ami $\Phi_{p_1 \dots p_k}(x)$-nek szintén (77) alakú felírása, csak éppen i helyett $i+1$-re. Ebből azt kapjuk, hogy (77) minden $1 \leq i \leq k$-ra helyes, az $i = k$ esetben pedig (77) könnyen láthatóan átmegy (76)-ba. Ezzel lemmánkat igazoltuk.

2.2.6. Lemma. *Legyen $k \geq 2$ és $p_1 < ... < p_k$ prímek. Ekkor*

$$A(p_1 ... p_k) \leq A(p_1 ... p_{k-1}) \prod_{j=0}^{k-2} S(p_1 ... p_j)$$

Bizonyítás. Vezessük be a $\Phi_m(x) = \sum_{n=0}^{\varphi(m)} a(m,n)x^n$ jelölést. (76) jobboldalát $\mathbb{Z}\big[[x]\big]$-ben tovább alakítva

$$\Phi_{p_1 .. p_k}(x) = -\Phi_{p_1 \dots p_{k-1}}(x^{p_k}) \Big(\prod_{j=0}^{k-2} \Phi_{p_1 \dots p_j}(x^{p_{j+2} \cdots p_{k-1}})\Big) \sum_{t \geq 0} x^{t p_1 \cdots p_{k-1}} \tag{78}$$

Az együtthatókra (78)-ból az alábbi összefüggést nyerjük.

$$a(\prod_{l=1}^{k} p_l, n) = - \sum_{r=0}^{\varphi(\prod_{l=1}^{k-1} p_l)} \sum_{s_0=0}^{1} ... \sum_{s_j=0}^{\varphi(\prod_{l=1}^{j} p_l)} ... \sum_{s_{k-2}=0}^{\varphi(\prod_{l=1}^{k-2} p_l)} \sum_{t=0}^{p_k - 1}$$

$$\{a(\prod_{l=1}^{k-1} p_l, r) \prod_{j=0}^{k-2} a(\prod_{l=1}^{j} p_l, s_j) \Big| rp_k + \sum_{j=0}^{k-2} s_j \prod_{l=j+2}^{k-1} p_l + t \prod_{l=1}^{k-1} p_l = n\} \quad (0 \le n \le \varphi(\prod_{l=1}^{k} p_l)),$$

amiből

$$|a(\prod_{l=1}^{k} p_l, n)| \le \sum_{s_0=0}^{1} \dots \sum_{s_j=0}^{\varphi(\prod_{l=1}^{j} p_l)} \dots \sum_{s_{k-2}=0}^{\varphi(\prod_{l=1}^{k-2} p_l)} \sum_{r=0}^{\varphi(\prod_{l=1}^{k-1} p_l)} \sum_{t=0}^{p_k-1}$$

$$\{|a(\prod_{l=1}^{k-1} p_l, r)| \prod_{j=0}^{k-2} |a(\prod_{l=1}^{j} p_l, s_j)| \Big| rp_k + \sum_{j=0}^{k-2} s_j \prod_{l=j+2}^{k-1} p_l + t \prod_{l=1}^{k-1} p_l = n\} \quad (0 \le n \le \varphi(\prod_{l=1}^{k} p_l)), \tag{79}$$

s itt végrehajottunk $k-1$ darab szummacserét. Ha most n mellett az s_j $(0 \le j \le k-2)$ számok értékét is előírjuk, akkor az

$$rp_k + \sum_{j=0}^{k-2} s_j \prod_{l=j+2}^{k-1} p_l + t \prod_{l=1}^{k-1} p_l = n \qquad r, t \in \mathbb{Z}, \quad 0 \le t \le p_k - 1 \tag{80}$$

egyenlet alapján t egyértelműen meghatározott lesz modulo p_k, amely észrevétel $0 \le t \le p_k - 1$ miatt t-t mint egész számot is rögzíti. Ebből pedig már r értéke is következik, noha az s_j-k fixálása után (80)-ban r nem feltétlenül lesz nemnegatív. Jelöljük az s_j-k rögzítése után (80)-ból r-re kapott értéket $r_n(s_0, s_1, ..., s_{k-2})$-vel. Ennek segítségével (79) jobboldalát valamivel egyszerűbb alakba írhatjuk, és ezáltal

$$|a(\prod_{l=1}^{k} p_l, n)| \le \sum_{s_0=0}^{1} \dots \sum_{s_j=0}^{\varphi(\prod_{l=1}^{j} p_l)} \dots$$

$$\dots \sum_{s_{k-2}=0}^{\varphi(\prod_{l=1}^{k-2} p_l)} \{|a(\prod_{l=1}^{k-1} p_l, r_n(s_0, ..., s_{k-2}))| \prod_{j=0}^{k-2} |a(\prod_{l=1}^{j} p_l, s_j)| \Big| r_n(s_0, s_1, ..., s_{k-2}) \ge 0\} \tag{81}$$

Ezután (81) jobboldalát triviálisan becsülve a következőt kapjuk.

$$|a(\prod_{l=1}^{k} p_l, n)| \le A(\prod_{l=1}^{k-1} p_l) \sum_{s_0=0}^{1} \dots \sum_{s_j=0}^{\varphi(\prod_{l=1}^{j} p_l)} \dots \sum_{s_{k-2}=0}^{\varphi(\prod_{l=1}^{k-2} p_l)} \prod_{j=0}^{k-2} |a(\prod_{l=1}^{j} p_l, s_j)| = A(\prod_{l=1}^{k-1} p_l) \prod_{j=0}^{k-2} S(\prod_{l=1}^{j} p_l),$$

vagyis $A(\prod_{l=1}^{k} p_l) \le A(\prod_{l=1}^{k-1} p_l) \prod_{j=0}^{k-2} S(\prod_{l=1}^{j} p_l)$. $\square$

Megjegyezzük, hogy a 2.2.6. lemma $k = 2$ és $k = 3$ esete érdektelen, hiszen ekkor segédtételünk a korábban bizonyítottaknál gyengébb eredményeket szolgáltat.

Most már a megfelelő eszközök birtokában igazoljuk a 2.2.3. tételt. Legyen $k \ge 4$, és tekintsük adottnak a $2 < p_1 < < p_2 < ... < p_k$ prímeket.

a) Figyelembe véve, hogy $S(1)S(p_1) = 2p_1$, 2.2.6., 2.2.1. és 2.1.4. b) szerint

$$A(p_1p_2p_3p_4) \le A(p_1p_2p_3)S(1)S(p_1)S(p_1p_2) \le \frac{3p_1 - 1}{4} \cdot 2p_1 \cdot \frac{p_1p_2 - 1}{2} < \frac{3}{4} p_1^3 p_2.$$

b) Teljes indukciót alkalmazunk k-ra vonatkozóan. Első lépésben ellenőrizzük, hogy (75) igaz $k = 5$-re. Tekintetbe véve, hogy $S(1)S(p_1) = 2p_1$, 2.2.6., 2.2.3. a), 2.1.4. b) és 2.2.4. alapján

$$A(p_1p_2p_3p_4p_5) \le A(p_1p_2p_3p_4)S(1)S(p_1)S(p_1p_2)S(p_1p_2p_3) < \frac{3}{4} p_1^3 p_2 \cdot p_1^2 p_2 \cdot \frac{1}{2} p_1^2 p_2 p_3 = \frac{3}{8} p_1^7 p_2^3 p_3,$$

amit látni akartunk. Legyen ezután $k \geq 6$, és tegyük fel, hogy (75)-ben k helyére j-t írva (75) igaz minden $5 \leq j \leq k-1$ esetén. 2.2.6.-ot, az indukciófeltételt, 2.1.4. b)-t, 2.2.4.-et, valamint $\omega(m) \geq 4$ esetén a triviális $S(m) < mA(m)$ becslést használva

$$A(\prod_{l=1}^{k} p_l) \leq A(\prod_{l=1}^{k-1} p_l) \prod_{j=0}^{k-2} S(\prod_{l=1}^{j} p_l) < \left(\frac{3}{8}\right)^{2^{k-6}} (\prod_{l=1}^{k-3} p_l^{2^{k-2-l}-1}) \cdot \frac{1}{2} p_1^4 p_2^2 p_3 \cdot \frac{3}{4} p_1^3 p_2 p_1 p_2 p_3 p_4 \cdot \prod_{j=5}^{k-2} ((\prod_{l=1}^{j} p_l) A(\prod_{l=1}^{j} p_l)) <$$

$$< \left(\frac{3}{8}\right)^{2^{k-6}+1} p_1^8 p_2^4 p_3^2 p_4 (\prod_{l=1}^{k-3} p_l^{2^{k-2-l}-1}) \cdot \prod_{j=5}^{k-2} \left(\frac{3}{8}\right)^{2^{j-5}} p_{j-1} p_j \prod_{l=1}^{j-2} p_l^{2^{j-1-l}} =$$

$$= \left(\frac{3}{8}\right)^{2^{k-5}} p_1^8 p_2^4 p_3^2 p_4 (\prod_{l=1}^{k-2} p_l^{2^{k-2-l}-1}) \cdot \prod_{j=5}^{k-2} p_j \prod_{l=1}^{j-1} p_l^{2^{j-1-l}} \tag{82}$$

Vezessük be a

$$p_1^8 p_2^4 p_3^2 p_4 (\prod_{l=1}^{k-2} p_l^{2^{k-2-l}-1}) \cdot \prod_{j=5}^{k-2} p_j \prod_{l=1}^{j-1} p_l^{2^{j-1-l}} = \prod_{t=1}^{k-2} p_t^{r_t} \tag{83}$$

jelölést. Egybevetve (82)-t, (83)-at és (75)-öt, most azt kell látnunk, hogy $1 \leq t \leq k-2$ esetén $r_t = 2^{k-1-t} - 1$. Legyen először $1 \leq t \leq 4$. Ekkor (83)-ból $r_t = 2^{4-t} + 2^{k-2-t} - 1 + \sum_{j=5}^{k-2} 2^{j-1-t} = 2^{4-t} + 2^{k-2-t} - 1 + 2^{4-t} \sum_{j=5}^{k-2} 2^{j-5} = 2^{4-t} + 2^{k-2-t} - 1 + 2^{4-t}(2^{k-6} - 1) = 2^{k-1-t} - 1$. Legyen másodszorra $5 \leq t \leq k-2$. Esetünkben (83) alapján $r_t = 2^{k-2-t} - 1 + 1 + \sum_{j=t+1}^{k-2} 2^{j-1-t} = 2^{k-2-t} + 2^{k-2-t} - 1 = 2^{k-1-t} - 1$. Ezzel megkaptuk, hogy (75) igaz k-ra, így a 2.2.3. tétel bizonyítást nyert. $\square$

Megjegyezzük, hogy ha a 2.2.4. becslés felállításánál elég nagy n-re az $|a_n| \leq [\frac{3r-1}{4}]$ eredményt alkalmazzuk, úgy 2.2.4. helyett némi számolással a valamivel élesebb $S(pqr) \leq \frac{15}{32} pqr^2$ becsléshez jutunk, ami a (75)-ben szereplő $\frac{3}{8}$-ot $\frac{45}{128}$-ra módosítja.

2.2.7. Következmény. *Legyen $n \in \mathbb{N}$, $\omega(n) = k \geq 1$. Ekkor $A(n) \leq n^{\frac{2^{k-1}}{k}-1}$.*

A következmény bizonyítását az Olvasóra bízzuk.

A 2.2.5., 2.2.6. lemmák, a 2.2.7. következmény, és lényegében a 2.2.3. tétel [9]-ben olvasható, utóbbinak konstans szorzókkal való élesítése viszont tőlem származik. A 2.2.4. lemma gondolata pedig a 2.2.1. tétel bizonyításából kézenfekvően adódik.

2.3. $A(n)$-re vonatkozó alsó becslések

Az $A(n)$ alsó becslésére irányuló kutatások a szakirodalom szerint az 1930-as években indultak. Az első egyszerű, ugyanakkor szép eredmény 1931-ből való és I. Schur-tól származik, aki azt egy Landauhoz írott levelében közölte, és amelyet az alábbiakban ismertetünk. A körosztási polinomok együtthatóira a továbbiakban is használni fogjuk a 2.2.6. lemma bizonyításában bevezetett jelölést.

2.3.1. Tétel. *Legyen $k \geq 3$ páratlan, $p_1 < p_2 < ... < p_k < p_1 + p_2$ prímek, és legyen $m = \prod_{j=1}^{k} p_j$. Ekkor $a(m, p_k) = 1 - k$, vagyis $\Phi_m(x)$-ben x^{p_k} együtthatója $1 - k$.*

Megjegyezzük, hogy a prímszámtétel értelmében minden $k \geq 3$ egészhez létezik olyan $x_0 \in \mathbb{R}$, hogy bármely $p_1 \geq x_0$ prím esetén a $p_2, ..., p_k$ prímek a fenti tulajdonsággal megadhatók, így a tétel közvetlen folyománya, hogy $A(n)$ nem korlátos.

Bizonyítás. k páratlansága és $p_k < p_1 + p_2$ miatt $\mathbb{Q}\big[[x]\big]$-ben

$$\Phi_m(x) = \prod_{d|m} (1 - x^d)^{\mu(\frac{m}{d})} \equiv \frac{1}{1-x} \prod_{j=1}^{k} (1 - x^{p_j}) \mod x^{p_k+1} \tag{84}$$

(84)-et folytatva, szintén $p_k < p_1 + p_2$ következtében

$$\frac{1}{1-x}\prod_{j=1}^{k}(1-x^{p_j}) = (\sum_{i=0}^{p_k-1} x^i)\prod_{j=1}^{k-1}(1-x^{p_j}) \equiv (\sum_{i=0}^{p_k-1} x^i)(1-\sum_{j=1}^{k-1} x^{p_j}) \mod x^{p_k+1} \tag{85}$$

Legyen $f_m(x) = (\sum_{i=0}^{p_k-1} x^i)(1-\sum_{j=1}^{k-1} x^{p_j})$. Ekkor (84) és (85) összevetéséből adódóan $\Phi_m(x)$ és $f_m(x)$ első p_k+1 tagja megegyezik, $f_m(x)$-ben pedig x^{p_k} együtthatója láthatóan $-(k-1)$. □

Szintén bizonyos körosztási polinomok valamely konkrét együtthatójának megállapításával nyert két majdnem azonos eredményt Emma Lehmer 1936-ban illetve Herbert Möller 1971-ben az alábbi tételekkel.

2.3.2. Tétel. *Legyenek $r < q < p$ olyan prímek, melyekre $q = rk + 2$ és $p = (qrm-1)/2 \quad (k, m \in \mathbb{N}, 2 \nmid m)$. Ekkor $a(pqr, \frac{r-3}{2}(pq+1)) = \frac{r-1}{2}$, vagyis $A(pqr) \geq \frac{r-1}{2}$.*

2.3.3. Tétel. *Legyenek $3 < r < q < p$ olyan prímek, melyekre $q = rk + 2$ és $p = (qrm-1)/2 \quad (k, m \in \mathbb{N}, 2 \nmid m)$. Ekkor $a(pqr, \frac{r-1}{2}(pq+1)) = \frac{r+1}{2}$, amiért $A(pqr) \geq \frac{r+1}{2}$.*

A Dirichlet-tétel szerint adott r páratlan prímhez végtelen sok a fenti tételekben említett tulajdonságú (q, p) prímpár létezik. A 2.3.3. tételt bizonyítjuk, 2.3.2. bizonyítására nézve lásd [10]. A (8) képlet alkalmazásával

$$\Phi_{pqr}(x) = \frac{\Phi_{qr}(x^p)}{\Phi_{qr}(x)}, \tag{86}$$

emellett 1.1.1.-et használva

$$\frac{1}{\Phi_{qr}(x)} = \frac{(1-x^r)(1-x^q)}{(1-x)(1-x^{qr})} = (1-x^q)(\sum_{j=0}^{r-1} x^j)\sum_{k\geq 0} x^{qrk} =: \sum_{k\geq 0} b_k x^k \tag{87}$$

$\mathbb{Q}\big[[x]\big]$-ben. (87)-ből pedig leolvashatjuk, hogy

$$b_k = \begin{cases} 1 & \text{ha } k \equiv j \quad (qr) \text{ és } 0 \leq j \leq r-1 \\ -1 & \text{ha } k \equiv j \quad (qr) \text{ és } q \leq j \leq q+r-1 \\ 0 & \text{különben} \end{cases} \tag{88}$$

Bevezetve a $h = \frac{r-1}{2}(pq+1)$ jelölést, szintén (86)-ból és (87)-ből

$$a(pqr, h) = \sum\{a(qr, i)b_k | 0 \leq i \leq \varphi(qr), k \geq 0, k + ip = h\} = \sum_{i=0}^{[\frac{h}{p}]} a(qr, i)b_{h-ip},$$

ami a nyilvánvaló $[\frac{h}{p}] = \frac{r-1}{2}q$ egyenlőség miatt az

$$a(pqr, h) = \sum_{i=0}^{\frac{r-1}{2}q} a(qr, i)b_{h-ip} \tag{89}$$

alakot ölti. A folytatás ötletét az az észrevétel adja, hogy $2p + 1 \equiv 0 \ (qr)$ miatt az $i_0 = \frac{r-1}{2}(q-2)$ jelöléssel egyrészt $h - i_0 p = \frac{r-1}{2}(2p+1) \equiv 0 \ (qr)$, másrészt továbbmenve $h - (i_0 + 2l)p \equiv l \ (qr)$, amivel b_{h-ip} értéke könnyen megállapíthatóvá válik. Most tehát i lehetséges értékeit tekintve három esetre bontunk.

(i) $i = i_0 + 2l$, ahol $0 \leq l \leq \frac{r-1}{2}$

(ii) $i = i_0 + 2l$, ahol $-\frac{i_0}{2} \leq l \leq -1$

(iii) $i = i_0 + 2l - 1$, ahol $-\frac{i_0-1}{2} \leq l \leq \frac{r-1}{2}$

Megjegyezzük, hogy (ii)-ben az első egyenlőtlenségnél csak $4k+1$ alakú r esetén állhat egyenlőség, míg (iii) első egyenlőtlenségénél egyenlőség csak $4k-1$ alakú r esetén lehetséges.

Az (i) esetben a 2.1.6. állítás bizonyításában látottak alapján $a(qr,i) = a(qr,i_0+2l) = 1 \quad (0 \leq l \leq \frac{r-1}{2})$, emellett $h - ip = h - i_0p - 2pl \equiv l\ (qr)$, amiből $0 \leq l \leq \frac{r-1}{2} \leq r-1$ miatt (88) figyelembevételével $b_{h-ip} = 1$. Ezután megmutatjuk, hogy a másik két esetben $b_{h-ip} = 0$, ami (89)-re való tekintettel az előbbiekkel együtt kívánt eredményünket fogja adni. (ii) fennállásakor legyen $s = l + qr$, vagyis ekkor $h - ip \equiv s\ (qr)$. Mivel ezen túlmenően $q + r - 1 < 2q < \frac{3}{4}qr < qr - \frac{r-1}{4}(q-2) = qr - \frac{i_0}{2} \leq s \leq qr - 1$, azért (88) miatt most valóban $b_{h-ip} = 0$. Tegyük most fel, hogy i-re a (iii)-ban foglalt feltétel teljesül, és legyen $s = \frac{qr-1}{2} + l$. Mivel $p \equiv \frac{qr-1}{2}\ (qr)$, azért $h - ip = h - i_0p - 2lp + p \equiv p + l \equiv s\ (qr)$, továbbá $\frac{qr-i_0}{2} \leq s \leq \frac{qr-1}{2} + \frac{r-1}{2}$, vagyis

$$\frac{1}{4}(2qr - (r-1)(q-2)) \leq s \leq \frac{q+1}{2}r - 1 \leq qr - 1.$$

(88) miatt már csak azt kell látnunk, hogy $q + r \leq \frac{1}{4}(2qr - (r-1)(q-2))$, azaz $qr - 3q - 2r - 2 \geq 0$, vagyis $(q-2)(r-3) \geq 8$. Legutóbbi egyenlőtlenségünk pedig $q > r \geq 5$ miatt valóban igaz. □

A 2.3.3. tétel állítása $r = 3$-ra nem igaz, sőt $q \equiv -1\ (3)$ és $p \equiv \frac{3q-1}{2}\ (3q)$ esetén a 2 nem áll elő $\Phi_{3pq}(x)$ együtthatójaként (a -2 viszont igen).

A 2.2.7. következmény illetve a 2.2.3. tétel megfordítását foglalja magába a következő megoldatlan probléma és állításának folyománya.

2.3.4. Sejtés. *Minden $k \geq 1$ egészhez megadható olyan $c_k > 0$ konstans, melyre található végtelen sok olyan $n \in \mathbb{N}$, hogy $\omega(n) = k$ és $A(n) > c_k n^{\frac{2^{k-1}}{k}-1}$.*

2.3.5. Következmény. *Minden $k \geq 1$ egészhez létezik olyan $c_k > 0$ konstans, melyhez megadható végtelen sok $p_1 < p_2 < ... < p_k$ prímszám k-as úgy, hogy $A(\prod_{j=1}^{k} p_j) > c_k \prod_{j=1}^{k-2} p_j^{2^{k-1-j}-1}$.*

2.3.5. ugyanúgy következik 2.3.4.-ből, mint ahogyan 2.2.7. a 2.2.3 tételből. Az alábbiakban bebizonyítjuk, hogy a 2.3.4. sejtés levezethető egy híres megoldatlan számelméleti problémából, amely a következőképpen hangzik.

2.3.6. Sejtés (Prímszám k-asok sejtése)**.** *Legyenek megadva az $a_1, a_2, .., a_k$ pozitív egészek, és a $b_1, ..., b_k$ egészek azzal a tulajdonsággal, hogy bármely p prímre*

$$\prod_{j=1}^{k} (a_j x + b_j) \equiv 0 \mod p \tag{90}$$

kongruenciának p-nél kevesebb megoldása van. Ekkor végtelen sok $t \in \mathbb{N}$ esetén az $a_j t + b_j \quad (1 \leq j \leq k)$ számok mind prímek.

Megjegyezzük, hogy a Dirichlet-tétel a sejtés $k = 1$-hez tartozó speciális esete.

2.3.7. Tétel. *2.3.4. következménye a 2.3.6. sejtésnek.*

A bizonyításhoz igénybe vesszük az alábbi segédtételt.

2.3.8. Lemma. *Legyenek $r \geq 5$ és $k \geq 1$ egészek, továbbá $1 \leq j \leq k$-ra p_j legyen olyan prím, melyre $p_j \equiv 2r \pm 1\ (4r)$, végül legyen $n = \prod_{j=1}^{k} p_j$ és $\varepsilon = e^{\frac{i\pi}{2r}}$. Ekkor*

$$|\Phi_n((-1)^{k-1}\varepsilon)| = \left(ctg\frac{\pi}{4r}\right)^{2^{k-1}} > \left(\frac{5}{4}r\right)^{2^{k-1}}. \tag{91}$$

A lemma bizonyítása. Az 1.1.1. lemma miatt

$$|\Phi_n((-1)^{k-1}\varepsilon)| = \prod_{d|n} |1-((-1)^{k-1}\varepsilon)^d|^{\mu(\frac{n}{d})} = \prod_{\substack{d|n \\ 2\nmid\omega(d)}} |1+(-1)^k\varepsilon^d|^{\mu(\frac{n}{d})} \cdot \prod_{\substack{d|n \\ 2|\omega(d)}} |1+(-1)^k\varepsilon^d|^{\mu(\frac{n}{d})}. \quad (92)$$

Legyen először $\omega(n)=k$ páratlan. (92)-ből

$$|\Phi_n(\varepsilon)| = \frac{\prod\limits_{\substack{d|n \\ 2\nmid\omega(d)}} |1-\varepsilon^d|}{\prod\limits_{\substack{d|n \\ 2|\omega(d)}} |1-\varepsilon^d|}. \quad (93)$$

Mivel $a,b \equiv 2r\pm 1\ (4r)$ és $u,v\equiv\pm 1\ (4r)$ esetén $ab\equiv\pm 1\ (4r)$, $uv\equiv\pm 1\ (4r)$ és $au\equiv 2r\pm 1\ (4r)$, továbbá $\varepsilon^{2r+1}=-\varepsilon$ és $|1\pm\varepsilon^{-1}|=|1\pm\varepsilon|$, azért (93)-ból

$$|\Phi_n(\varepsilon)| = \frac{\prod\limits_{\substack{d|n \\ 2\nmid\omega(d)}} |1+\varepsilon|}{\prod\limits_{\substack{d|n \\ 2|\omega(d)}} |1-\varepsilon|} = \frac{|1+\varepsilon|^{2^{k-1}}}{|1-\varepsilon|^{2^{k-1}}} = \left(\operatorname{ctg}\frac{\pi}{4r}\right)^{2^{k-1}}.$$

Legyen most $\omega(n)=k$ páros. Ismét (92)-ből, majd a fentebbi meggondolásokból

$$|\Phi_n(-\varepsilon)| = \frac{\prod\limits_{\substack{d|n \\ 2|\omega(d)}} |1+\varepsilon^d|}{\prod\limits_{\substack{d|n \\ 2\nmid\omega(d)}} |1+\varepsilon^d|} = \frac{\prod\limits_{\substack{d|n \\ 2|\omega(d)}} |1+\varepsilon|}{\prod\limits_{\substack{d|n \\ 2\nmid\omega(d)}} |1-\varepsilon|} = \frac{|1+\varepsilon|^{2^{k-1}}}{|1-\varepsilon|^{2^{k-1}}} = \left(\operatorname{ctg}\frac{\pi}{4r}\right)^{2^{k-1}}.$$

Ezzel (91)-ben az egyenlőséget igazoltuk. Az egyenlőtlenség megállapításához pedig elég látni, hogy $\sin\frac{\pi}{4r}<\frac{\pi}{4r}$, és $r\geq 5$ miatt $\cos\frac{\pi}{4r}>\frac{\pi}{3,2}$. Utóbbit számolással ellenőrizhetjük, például abból kiindulva, hogy $2\cos\frac{\pi}{5}=\frac{1+\sqrt{5}}{2}$, majd kétszer használva a $2\cos\frac{\alpha}{2}=\sqrt{2+2\cos\alpha}$ azonosságot. □

A 2.3.8. lemma alkalmazásával gyakran használt és hatékony eszközhöz nyúlunk az $A(n)$ alsó becslésére. Ha ugyanis $z\in\mathbb{C}$, $|z|=1$ esetén $|\Phi_n(z)|$-et alulról tudjuk becsülni, azzal $|z^m|=1$ $(m\in\mathbb{N})$ és a háromszög-egyenlőtlenség miatt $S(n)$-re, és így $A(n)$-re is becslést adunk. Kiemelendő az a speciális eset, amikor z egységgyök, hiszen ekkor $|\Phi_n(z)|$ kongruenciákkal kezelhető, ami sokszor további segítségünkre válik.

Rátérünk a 2.3.7. tétel bizonyítására. Vezessük be a $Q_k=\prod\limits_{\substack{2<q\leq k \\ q\text{ prím}}} q$ jelölést, ahol $k\geq 1$ egész, és legyen $a_j=\begin{cases}2jQ_k & \text{ha } 2\nmid j\\ 2(j-1)Q_k & \text{ha } 2|j\end{cases}$, valamint $b_j=(-1)^j$ $(1\leq j\leq k)$. Nyilvánvaló, hogy ekkor (90)-nek $p\leq k$ esetén nincs megoldása, ha pedig $p>k$, akkor $(a_j,p)=1$ miatt (90)-nek legfeljebb k megoldása van, és mellékesen az is könnyen látható, hogy a megoldásszám éppen k. 2.3.6. állítása szerint tehát végtelen sok olyan $t\in\mathbb{N}$ létezik, melyre $\{a_jt+b_j|1\leq j\leq k\}$ minden eleme prím. Rögzítsünk most egy ilyen t-t, és legyen $p_j=a_jt+b_j$ $(1\leq j\leq k)$,

$n = \prod_{j=1}^{k} p_j$, $r = Q_k t$ és $\varepsilon = e^{\frac{i\pi}{2r}}$. Mivel $1 \le j \le k$ esetén $\frac{a_j}{Q_k} \equiv 2 \mod 4$, azért a $p_j \equiv 2r \pm 1 \mod 4r$ kongruenciák fennállnak, így a háromszög-egyenlőtlenség és a 2.3.8. lemma miatt

$$nA(n) \ge (\varphi(n)+1)A(n) \ge S(n) > |\Phi_n((-1)^{k-1}\varepsilon)| > \left(\frac{5}{4}r\right)^{2^{k-1}}. \tag{94}$$

Az a_j-k definíciójából leolvasható, hogy $p_j < 2jQ_k t = 2jr$, azaz $r > \frac{p_j}{2j}$, innen pedig $r^k > \frac{n}{2^k \cdot k!}$, vagyis

$$r^{2^{k-1}} > \frac{n^{\frac{2^{k-1}}{k}}}{2^{2^{k-1}}(k!)^{\frac{2^{k-1}}{k}}},$$

azaz

$$\left(\frac{5}{4}r\right)^{2^{k-1}} > \frac{n^{\frac{2^{k-1}}{k}}}{1,6^{2^{k-1}}(k!)^{\frac{2^{k-1}}{k}}}. \tag{95}$$

Felvéve a $c_k = \frac{1}{1,6^{2^{k-1}}(k!)^{\frac{2^{k-1}}{k}}}$ jelölést, (94)-ből és (95)-ből $nA(n) > c_k n^{\frac{2^{k-1}}{k}}$ adódik, amiért valóban $A(n) > > c_k n^{\frac{2^{k-1}}{k}-1}$. □

Észrevehetjük, hogy a 2.3.6. sejtés igen sokat állít, az ikerprímsejtés azonnal következik belőle. Megmutatjuk azonban, hogy 2.3.4. és 2.3.5. állítását némiképpen gyengítve olyan eredményekhez juthatunk, amelyek igazolásához az eszközeink már megvannak. A következőt bizonyítjuk.

2.3.9. Tétel. *Minden $k \ge 1$ egészhez létezik végtelen sok olyan $p_1 < p_2 < ... < p_k$ prímszám k-as, melyre az $n = \prod_{j=1}^{k} p_j$ jelölés mellett $A(n) > \frac{p_k^{2^{k-1}-k}}{(4k\log p_1)^{2^{k-1}}}$.*

A bizonyításhoz szükség van több segédtételre, amelyeket az alábbiakban ismertetünk. Legyen $y \in \mathbb{R}$, $y \ge 2$, $a, m \in \mathbb{N}^+$ és $(a,m) = 1$. Ekkor $\pi(y,m,a)$ jelöli a $[2,y]$ intervallumba eső modulo m a-val kongruens prímek számát.

2.3.10. Lemma. *Ha $a, m \in \mathbb{N}^+$, $(a,m) = 1$, és $y > e^{m^{\frac{2}{3}}}$, akkor*

$$\pi(y,m,a) = \frac{1}{\varphi(m)} \int_2^y \frac{dt}{\log t} + \mathcal{O}\left(\frac{y}{\log^{100} y}\right), \tag{96}$$

és itt az $\mathcal{O}$ jelben foglalt konstans értéke független m-től ás a-tól.

A lemma állítása könnyen levezethető [11] (36)-ban írt formulájából.

2.3.11. Lemma. *Létezik olyan δ szám, melyre $y \ge 2$ esetén*

$$\sum_{\substack{q=1 \\ 2 \nmid q}}^{[y]} \frac{1}{\varphi(q)} = \frac{105\zeta(3)}{2\pi^4}\log y + \delta + \mathcal{O}\left(\frac{\log y}{y}\right).$$

A lemma bizonyítására nézve lásd [12]-t.

2.3.12. Lemma. *Minden k pozitív egészhez létezik végtelen sok pozitív egész r szám, melyre megadhatók a $p_1, p_2, ..., p_k$ prímek a következő tulajdonsággal.*

$$p_j \equiv 2r+1 \mod 4r, \quad p_j < 5kr\log r \quad (1 \le j \le k). \tag{97}$$

Bizonyítás. Legyen a bizonyítás során k rögzített. Definiáljuk $x > 1$ esetén a $P(x)$, $Q(x)$ és $M(x)$ halmazokat a következőképpen.

$$P(x) = \{p \text{ prím}| \quad p \equiv -1 \mod 4, \quad x < p \leq 7x\}$$
$$Q(x) = \{q \in \mathbb{N}| \quad 2 \nmid q, \quad \frac{4}{5}k \log x < q \leq \frac{12}{5}k \log x\}$$
$$M(x) = \{(p,q)|p \in P(x), q \in Q(x), p \equiv 1 \mod q\}$$

Most a 2.3.10., és 2.3.11. lemmák segítségével elegendően nagy x esetén alsó becslést adunk $|M(x)|$-re. Mivel az $a \equiv -1 \mod 4$, $a \equiv 1 \mod q$ szimultán kongruenciarendszer megoldása $a \equiv 2q+1 \mod 4q$, azért

$$|M(x)| = \sum_{q \in Q(x)} |\{p \text{ prím}|p \equiv 2q+1 \mod 4q, x < p \leq 7x\}| = \sum_{q \in Q(x)} (\pi(7x, 4q, 2q+1) - \pi(x, 4q, 2q+1)). \quad (98)$$

2.3.10. szerint $4q < \log^{\frac{3}{2}} x$ fennálltakor

$$\sum_{q \in Q(x)} (\pi(7x, 4q, 2q+1) - \pi(x, 4q, 2q+1)) =$$

$$= \sum_{q \in Q(x)} \left(\frac{1}{2\varphi(q)} \int_2^{7x} \frac{dt}{\log t} + \mathcal{O}\left(\frac{7x}{\log^{100} 7x}\right) - \frac{1}{2\varphi(q)} \int_2^{x} \frac{dt}{\log t} + \mathcal{O}\left(\frac{x}{\log^{100} x}\right)\right) =$$

$$= \sum_{q \in Q(x)} \left(\frac{1}{2\varphi(q)} \int_x^{7x} \frac{dt}{\log t} + \mathcal{O}\left(\frac{x}{\log^{100} x}\right)\right). \quad (99)$$

Könnyen látható, hogy $4q < \log^{\frac{3}{2}} x$ teljesül, ha $x > e^{92,16k^2}$. Ismeretes, és egyben könnyű belátni, hogy $\int_2^x \frac{dt}{\log t} = \frac{x}{\log x} + \mathcal{O}(\frac{x}{\log^2 x})$, továbbá $|Q(x)| = \mathcal{O}(\log x)$, és ezért

$$\sum_{q \in Q(x)} \left(\frac{1}{2\varphi(q)} \int_x^{7x} \frac{dt}{\log t} + \mathcal{O}\left(\frac{x}{\log^{100} x}\right)\right) = \frac{1}{2}\left(\frac{6x}{\log x} + \mathcal{O}\left(\frac{x}{\log^2 x}\right)\right) \sum_{q \in Q(x)} \frac{1}{\varphi(q)} + \mathcal{O}\left(\frac{x}{\log^{99} x}\right). \quad (100)$$

A 2.3.11. lemma miatt $\sum_{q \in Q(x)} \frac{1}{\varphi(q)} = \frac{105\zeta(3)\log 3}{2\pi^4} + \mathcal{O}\left(\frac{\log\log x}{\log x}\right)$, és így (98), (99) és (100) szerint

$$|M(x)| = \frac{315\zeta(3)\log 3}{2\pi^4} \cdot \frac{x}{\log x} + \mathcal{O}\left(\frac{x \log\log x}{\log^2 x}\right) > 2,1\frac{x}{\log x}, \quad (101)$$

amint x elég nagy. Értelmezzük ezután $M(x)$-en az f_x függvényt a következőképpen. $p \in P(x)$ és $q \in Q(x)$ esetén legyen $f_x(p,q) = \frac{p-1}{2q}$. Jelölje f_x értékkészletét $R(x)$, az $(\frac{x-1}{4,8k\log x}, \frac{7x-1}{1,6k\log x})$ intervallumot $I(x)$, egy tetszőleges J intervallum hosszát pedig $\lambda(J)$. Ekkor a $P(x)$, $Q(x)$ és $M(x)$ halmazok definíciója folytán $R(x) \subset I(x) \cap \mathbb{Z}$, és $f_x(p,q)$ páratlan, amiknél fogva

$$|R(x)| \leq \frac{1}{2}\lambda(I(x)) + \mathcal{O}(1) = \frac{1}{2} \cdot \frac{20x-2}{4,8k\log x} + \mathcal{O}(1) = \frac{25}{12k} \cdot \frac{x}{\log x} + \mathcal{O}(1),$$

vagyis (101) miatt elegendően nagy x-re

$$|M(x)| > k|R(x)|. \quad (102)$$

Legyen $x_0 \in \mathbb{R}$ olyan, hogy $x > x_0$ esetén (102) valamint

$$5k \log x < x^{0,038} \quad (103)$$

teljesül, és legyen $x > x_0$ rögzített. A skatulya-elv szerint van olyan $r \in R(x)$, melyhez megadható k (sőt valójában $k+1$) darab $(p,q) \in M(x)$ pár úgy, hogy $\frac{p-1}{2q} = r$ fennálljon. Fixáljunk egy ilyen r-et, és válasszuk ki a $(p_j, q_j) \in M(x)$ párokat a

$$\frac{p_j - 1}{2q_j} = r \quad (1 \leq j \leq k) \tag{104}$$

követelménynek megfelelően. Ekkor a p_j-k nyilván páronként különbözőek, hiszen $p_i = p_j$ maga után vonná $q_i = q_j$-t is. Mivel $1 \leq j \leq k$ esetén q_j páratlan, azért a

$$p_j \equiv 2r + 1 \mod 4r$$

kongruenciafeltétel teljesül, és most megmutatjuk, hogy

$$p_j < 5kr \log r \quad (1 \leq j \leq k).$$

(104)-ből és $q_j \in Q(x)$-ből adódóan

$$p_j = 2q_j r + 1 \leq 4,8kr \log x + 1, \tag{105}$$

emellett (103) miatt $x \geq 500$, amiért $r \in I(x)$-et is figyelembe véve

$$\frac{x}{5k \log x} < \frac{x-1}{4,8k \log x} < r, \tag{106}$$

továbbá most már (106)-ra is tekintettel

$$1 \leq \frac{0,01kx \log x}{5k \log x} < 0,01kr \log x. \tag{107}$$

(105)-öt és (107)-et egybevetve látjuk, hogy a

$$4,81kr \log x < 5kr \log r$$

egyenlőtlenséget kell igazolni, ami helyett (106) miatt elég látni, hogy

$$\frac{4,81}{5} < \frac{\log x - \log 5k - \log \log x}{\log x},$$

ez utóbbi fennállását pedig éppen (103) jelenti. Beláttuk tehát, hogy $x > x_0$ esetén létezik olyan $r \in \mathbb{N}$, melyre $\frac{x}{5k \log x} < r < \frac{35x}{8k \log x}$, és amelyhez megadhatók a $p_1, p_2, ..., p_k$ prímek a (97) tulajdonságokkal. Legyen most $x_1 > x_0$, és $i \in \mathbb{Z}$, $i \geq 1$ esetén válasszuk x_{i+1}-et úgy, hogy $\frac{35x_i}{8 \log x_i} < \frac{x_{i+1}}{5 \log x_{i+1}}$ teljesüljön, $r_i \in R(x_i)$ pedig legyen olyan, hogy a $(p_{ij}, q_{ij}) \in M(x_i) \quad (1 \leq j \leq k)$ párok megadhatók legyenek a $\frac{p_{ij}-1}{2q_{ij}} = r_i$ követelménynek eleget téve. Ekkor $\frac{x_i}{5k \log x_i} < r_i < \frac{35x_i}{8k \log x_i}$ minden i-re történő fennállása, és az x_i-k megválasztása miatt $r_i < \frac{35x_i}{8k \log x_i} < \frac{x_{i+1}}{5k \log x_{i+1}} < r_{i+1}$. Mivel a látottak szerint minden $i \geq 1$-re és $1 \leq j \leq k$-ra $p_{ij} \equiv 2r_i + 1 \mod 4r_i$, és $p_{ij} < 5kr_i \log r_i$, segédtételünket bebizonyítottuk. □

Most már a szükséges lemmák birtokában igazolhatjuk a 2.3.9. tételt. Legyen $k \geq 1$ egész, és legyenek a $p_1 < < p_2 < ... < p_k$ prímek úgy megadva, hogy alkalmas $r \geq 5$ mellett (97) teljesüljön, továbbá legyen $n = \prod_{j=1}^{k} p_j$. (97) következtében $p_k < 5kr \log r < 5kr \log p_1$, vagyis $\frac{p_k}{5k \log p_1} < r$, amiből a 2.3.8. lemmát is használva

$$\frac{p_k^{2^{k-1}}}{(4k \log p_1)^{2^{k-1}}} < \left(\frac{5}{4}r\right)^{2^{k-1}} < |\Phi_n((-1)^{k-1}\varepsilon)|. \tag{108}$$

A háromszög-egyenlőtlenséget figyelembe véve pedig

$$|\Phi_n((-1)^{k-1}\varepsilon)| < S(n) \leq (\varphi(n)+1)A(n) \leq nA(n) \leq p_k^k A(n). \tag{109}$$

Végül (108) és (109) összekapcsolásával

$$\frac{p_k^{2^{k-1}-k}}{(4k\log p_1)^{2^{k-1}}} < A(n), \tag{110}$$

s mivel a 2.3.12. lemma folytán végtelen sok $p_1 < p_2 < ... < p_k$ prímszám k-as felírható úgy, hogy az $n = \prod_{j=1}^{k} p_j$ jelölés mellett (110) fennálljon, a 2.3.9. tételt bebizonyítottuk. □

Az alábbi két tétel 2.3.9. közvetlen folyománya.

2.3.13. Következmény. *Minden $k \geq 1$ egészre megadható végtelen sok olyan $p_1 < p_2 < ... < p_k$ prímszám k-as úgy, hogy az $n = \prod_{j=1}^{k} p_j$ jelöléssel $A(n) > \frac{\prod_{j=1}^{k-2} p_j^{2^{k-1-j}-1}}{(4k\log p_1)^{2^{k-1}}}$.* □

2.3.14. Következmény. *Minden $k \geq 1$ egészhez létezik végtelen sok $n \in \mathbb{N}$, melyre $\omega(n) = k$ és $A(n) > \frac{n^{\frac{2^{k-1}}{k}-1}}{(4\log n)^{2^{k-1}}}$.* □

A szakaszban közölt állítások közül 2.3.1. bizonyítása [10]-ben olvasható, a 2.3.3. tételt pedig [4] nyomán igazoltam. A 2.3.4.-2.3.14. pontok mindegyike [9]-ben szerepel.

Jelölések

Ebben a listában azok a jelölések szerepelnek, amelyek a szakdolgozatban több helyen (tétel, lemma bizonyítása, stb.) előfordulnak, továbbá amelyek a tézisben nincsenek ismertetve, de megítélésem szerint mégsem tartoznak a legközismertebb fogalmak közé. Azon jelölések bevezetését, amelyek csak egyetlen tételnél, lemmánál, stb. jönnek elő, a megadott pont (tétel, lemma, stb.) alatt kell keresni.

$\Phi_n(x)$	lásd 3. oldal, (1) sor.
$o(\varepsilon)$	az ε komplex egységgyök rendje, vagyis az a legkisebb n pozitív egész, melyre $\varepsilon^n = 1$.
$\mu(n)$	Möbius-függvény, azaz $$\mu(n) = \begin{cases} (-1)^r & \text{ha } n = \prod_{i=1}^{r} p_i \ (p_1 < p_2 < ... < p_r) \\ 0 & \text{ha valamely } p \text{ prímre } p^2 \mid n \end{cases}$$
$\varphi(n)$	Euler-féle φ-függvény
$\Phi_n(x, y)$	lásd 3. oldal, (4) sor és a fölötte levő definíció
$o_m(x, y)$	lásd 5. oldal, 1.1.5. lemma fölött
$\omega(n)$	n különböző prímosztóinak száma
$p^\beta \mid\mid a$ (p prím, $\beta \in \mathbb{N}$, $a \in \mathbb{Z}$)	$p^\beta \mid a$, de $p^{\beta+1} \nmid a$ (a $\beta = 0$ eset hozzávétele miatt egy árnyalatnyival más, mint a szokásos definíció, lásd a 12. oldal).
$o_m(a)$	$(a, m) = 1$ esetén az a szám rendje modulo m
$d(n)$	n pozitív osztóinak száma
$\alpha \sim \beta$, $\alpha \sim_R \beta$	lásd 10. oldal, 1.2.5. tétel bizonyítása, (21) és (22) sorok között
$[x]$	az $x \in \mathbb{R}$ szám egész része. Megjegyezzük, hogy a szögletes zárójelet maradékosztály jelölésére is használjuk, de ezt a szövegben mindig előre jelezzük.
$\Psi_a(\beta)$	lásd 14. oldal, 1.2.1. tétel bizonyítása, (38) és (39) sorok közötti kiemelt sor.
$\Gamma(N\|K)$	az N test K test feletti relatív automorfizmusainak csoportja (Galois csoport).
$A(n)$	lásd 15. oldal, 2. fejezetet bevezető szöveges rész, 2. sor.
$S(n)$	lásd 15. oldal, 2. fejezetet bevezető szöveges rész, 3. sor.
c, a (a 2.1. szakaszban használt jelölés)	lásd 16. oldal, a 2.1.1. tétel bizonyítása után.
$K\big[[x]\big]$, $R\big[[x]\big]$	a K test, illetve az R gyűrű feletti formális hatványsorok gyűrűje
$m_n(\alpha, \varepsilon_1, \varepsilon_2)$	lásd 21. oldal, (60) sor fölött
$M_r(p, q)$	lásd 24. oldal, alulról a 7. sor.
$a(m, n)$	lásd 26. oldal, 2.2.6. lemma bizonyításának eleje
$\pi(y, m, a)$	lásd 32. oldal, 2.3.9. tétel kimondása alatt

Hivatkozások

[1] Győry Kálmán, *Az $a^n \pm b^n$ alakú számok osztóiról két számelméleti feladat kapcsán*, Középiskolai Matematikai Lapok, 1991/5. 193-201.

[2] L. Carlitz, *The number of terms in the cyclotomic polynomial $F_{pq}(x)$*, Amer. Math. Monthly 73 (1966), 979-981.

[3] A. Migotti, *Zur Theorie der Kreisteilungsgleichung*, Sitz, Akad. Wiss. Wien (Math.) (2) 87 (1883), 7-14.

[4] Herbert Möller, *Über die Koeffizienten des n-ten Kreisteilungspolynoms*, Math. Zeitschrift 119 (1971), 33-40

[5] Marion Beiter, *The midterm coefficient of the cyclotomic polynomial $F_{pq}(x)$*, Amer. Math. Monthly 71 (1964), 769-770.

[6] A. S. Bang, *Om Ligningen $\Phi_n(x) = 0$*, Nyt Tidsskrift for Mathematik 6 (1895), 6-12.

[7] Marion Beiter, *Magnitude of the coefficients of the cylotomic polynomial F_{pqr}, II*, Duke Math. J. 38 (1971), 591-594.

[8] Marion Beiter, *Magnitude of the coefficients of the cylotomic polynomial $F_{pqr}(x)$*, Amer. Math. Monthly 75 (1968), 370-372.

[9] P. T. Bateman, C. Pomerance, R. C. Vaughan, *On the size of the coefficients of the cyclotomic polynomial*, Colloquia Mathematica Societatis János Bolyai 34. Topics in classical number theory, 171-202.

[10] Emma Lehmer, *On the magnitude of the coefficients of the cyclotomic polynomial*, Bulletin of the American Mathematical Society 42 (1936), 389-392.

[11] A. Page, *On the number of primes in an arithmetic progression*, Proc. London Math. Soc. (2) 39 (1935), 116-141.

[12] E. Landau, *On a Titchmarsh-Estermann sum*, J. London Math. Soc. 11 (1936), 242-245.