Polinomok Newton-poligonjai

Matematika BSc szakdolgozat

Szerző:
Sarró Mihály

Témavezető:
Dr. Waldhauser Tamás

Szegedi Tudományegyetem Bolyai Intézet

2015

Tartalomjegyzék

Bevezető

Szakdolgozatomban polinomok racionális számtest fölötti irreducibilitását vizsgálom. Mindig feltehetjük, hogy a polinom egész együtthatós, hiszen ha a polinom együtthatói racionális számok, a nevezők legkisebb közös többszörösével beszorozva egész együtthatós polinomot kapunk. A Gauss-lemma alapján ha egy egész együtthatós polinom $\mathbb{Q}$ fölött felbomlik kisebb fokú polinomok szorzatára, akkor $\mathbb{Z}$ fölött is felbomlik ilyen módon. Ezért a továbbiakban mindig $\mathbb{Z}$ fölötti polinomokat tekintünk, és felbontáson mindig két kisebb fokszamú egész együtthatós polinom szorzatára való felbontást értünk.

A Kronecker módszer [8] általános eljárás polinomok irreducibilitásának vizsgálatára, viszont „nagy” polinomok esetén rengeteg számolással jár, ami még a mai számítógépeknek is túl hosszadalmas. Ezért hasznosak az irreducibilitási kritériumok, melyek egyszerű elégséges feltételeket adnak polinomok irreducibilitására. Irreducibilitási kritériumokról és azok történetéről bővebb áttekintés található Dorwart [3] és Oleinikov [11] cikkében.

Dolgozatom egyik fő témája a Newton-poligon. A numerikus analízisben a Newton-módszer (más néven a Newton-Raphson-módszer) az egyik legismertebb módszer, amivel valós függvények esetén jól közelíthetjük a zérushelyeket. Létezik egy kevésbé ismert Newton-módszer is, melyben Newton $f(x, y) = 0$ alakú egyenletből y-t fejezte ki x segítségével sorfejtéssel. Ennek során a sor egy-egy újabb tagjának meghatározásához használt poligonokat, melyek az $f(x, y)$ kétváltozós polinomfüggvény monomjainak ábrázolásából adódnak. A szakdolgozatomban taglalt Newton-poligon az ebben a módszerben szereplő poligonhoz hasonló, később ezért nevezték el Newton tiszteletére Newton-poligonnak. Christensen cikkében [1] pontos leírás található Newton módszeréről.

Szakdolgozatomban kulcsszerep jut Dumas tételének, melynek erejét mutatja, hogy segítségével tömegesen „gyárthatunk” irreducibilitási kritériumokat. Ilyen például a híres Schönemann–Eisenstein-féle irreducibilitási kritérium, mely Dumas tételének egy triviális következménye. A 3. fejezetben további kritériumokat is bemutatok, melyek Dumas tételének egyszerű következményei. Dumas tételének segítségével komoly tételek is bizonyíthatóak, például Schur egy, a dolgozatomban is tárgyalt tétele, mely irreducibilis polinomok egész családját adja. E tétel alapján a $\sin(x)$, $\cos(x)$, e^x Taylor-polinomjai irreducibilisek, továbbá az $L_n = \frac{e^x}{n!} \frac{d^n}{dx^n} \left(e^{-x} x^n\right) = \sum_{k=0}^{n} (-1)^k \cdot \binom{n}{k} \cdot \frac{x^k}{k!}$ formulákkal definiált *Laguerre-polinomok* is.

1. Newton-poligon

Ebben a fejezetben definiáljuk a Newton-poligont, majd egy példán mutatjuk be, hogyan konstruáljuk meg egy adott polinomnak adott p prímszámhoz tartozó Newton-poligonját. Ehhez először egész számok egy speciális felbontását vizsgáljuk, melyben egy rögzített p prímszám legnagyobb hatványát kiemelve szorzattá alakítjuk a számot. Legyen $m \neq 0$ egész szám, p prímszám, és bontsuk fel m-et $m = p^\alpha a$ alakban, ahol $p \nmid a$. Jelölje $\nu_p(m)$ az α kitevőt. Technikai okokból használjuk a $\nu_p(0) = \infty$ megállapodást.

A következő lemma kimondja, mi történik ezzel a kitevővel, ha két természetes szám összegét, vagy szorzatát bontjuk fel. Erre a későbbiekben szükségünk lesz, így bizonyítjuk is.

1.1. Lemma. *Legyen $u, v \in \mathbb{Z}$ és p tetszőleges prím. Ekkor*

1. $\nu_p(uv) = \nu_p(u) + \nu_p(v)$;

2. $\nu_p(u+v) \geq \min(\nu_p(u), \nu_p(v))$;

3. ha $\nu_p(u) \neq \nu_p(v)$, akkor $\nu_p(u+v) = \min(\nu_p(u), \nu_p(v))$.

Bizonyítás. Ha u, v valamelyike 0, akkor mindhárom állítás triviális, ezért a továbbiakban feltesszük, hogy $u, v \neq 0$. Legyen $u = p^\alpha a$, $v = p^\beta b$, ahol $p \nmid a$ és $p \nmid b$.

1. A szorzatot felírhatjuk $uv = p^\alpha a p^\beta b = p^{\alpha+\beta} ab$ alakban. Ekkor $\nu_p(uv) = \alpha + \beta = \nu_p(u) + \nu_p(v)$, hiszen p prím, így a prímtulajdonság alapján $p \nmid ab$.

2. Az általánosság megszorítása nélkül feltehetjük, hogy $\alpha \leq \beta$. Ekkor $u + v = p^\alpha a + p^\beta b = p^\alpha(a + p^{\beta-\alpha} b)$, ezért $\nu_p(u+v) \geq \alpha = \min(\nu_p(u), \nu_p(v))$.

3. Az általánosság megszorítása nélkül feltehetjük, hogy $\alpha < \beta$. A fenti gondolatmenethez hasonlóan $u + v = p^\alpha(a + p^{\beta-\alpha} b)$. Mivel $p \nmid a$ és $p \mid p^{\beta-\alpha} b$, így $p \nmid a + p^{\beta-\alpha} b$. Ezért $\nu_p(u+v) = \alpha = \min(\nu_p(u), \nu_p(v))$.

□

1.2. Megjegyzés. Figyeljük meg, hogy ha $\nu_p(u) = \nu_p(v)$, akkor $u+v$ felbontásában tetszőlegesen nagy kitevő is szerepelhet, tehát tetszőleges $n \in \mathbb{N}$ és $N \geq n$ esetén létezik olyan u, v, hogy $\nu_p(u) = \nu_p(v) = n$ és $\nu_p(u+v) = N$. Például ha $u = p^n \cdot (p^{N-n} - 1)$ és $v = p^n \cdot 1$, akkor $u + v = p^n(p^{N-n} - 1 + 1) = p^n p^{N-n} = p^N \cdot 1$.

Ezek után definiálhatjuk egy polinom p-hez tartozó Newton-poligonját, melyhez a polinom minden monomjának együtthatóját felbontjuk a fenti módon, majd ábrázoljuk a megfelelő kitevőket. Összekötjük a kapott pontokat és a töröttvonal fölötti halmaz konvex burkának alsó határa lesz a Newton-poligon.

1.3. Definíció. Legyen p egy rögzített prímszám, $f = \sum_{i=0}^{n} A_i x^i \in \mathbb{Z}[x]$ és tegyük fel, hogy $A_0 \neq 0$ és $A_n \neq 0$. Ábrázoljuk a síkon az $(i, \nu_p(A_i))$ pontokat, amennyiben $A_i \neq 0$, majd kössük össze őket és tekintsük az így kapott töröttvonal „fölötti" halmazt. Az f polinom p-hez tartozó Newton-poligonja ezen halmaz konvex burkának alsó határa. Legyenek $P_0, P_1, \ldots$ azok az ábrázolt pontok, amelyek csúcsai a Newton-poligonnak. A $P_j P_{j+1}$ szakaszokat a Newton-poligon oldalainak nevezzük. Legyen $P_j = (i_1, \alpha_1)$, $P_{j+1} = (i_2, \alpha_2)$, ekkor az $i_2 - i_1$ mennyiséget a $P_j P_{j+1}$ oldal „vízszintes hosszának", röviden v-hosszának nevezzük.

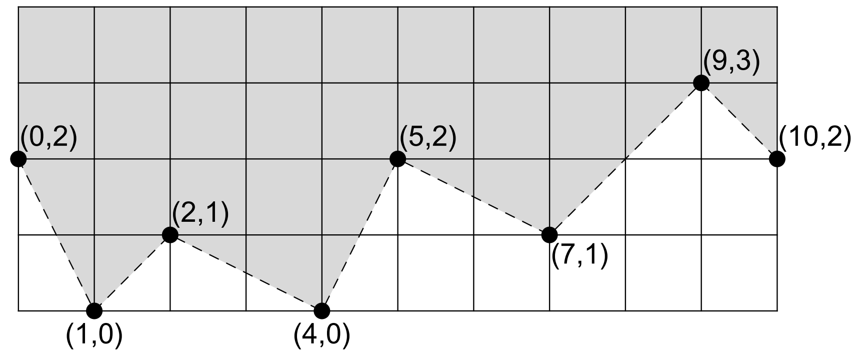
Nézzünk egy példát, melyben konkrét f polinomra és p prímszámra határozzuk meg a Newton-poligont.

1.4. Példa. Legyen $f = 36 + 2x + 6x^2 + 2x^4 + 18x^5 + 3x^7 + 54x^9 + 18x^{10}$ és $p = 3$. Ekkor

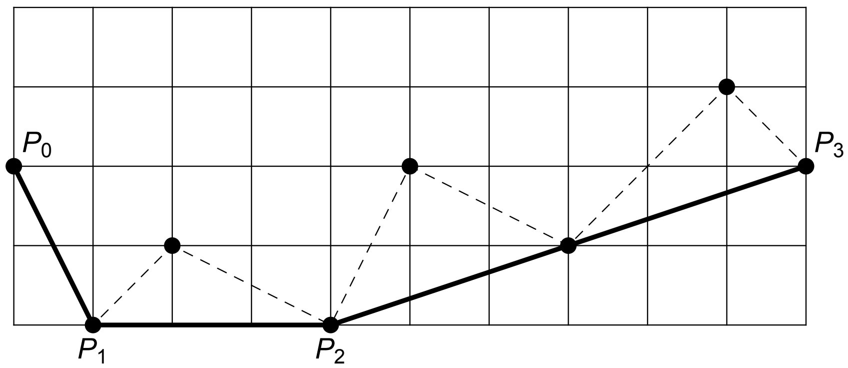
$$f = 3^2 \cdot 4 + 3^0 \cdot 2x + 3^1 \cdot 2x^2 + 3^0 \cdot 2x^4 + 3^2 \cdot 2x^5 + 3^1 \cdot 1x^7 + 3^3 \cdot 2x^9 + 3^2 \cdot 2x^{10}.$$

A felbontásból leolvasható, hogy a következő pontokat kell ábrázolnunk:

$$(0, 2),\ (1, 0),\ (2, 1),\ (4, 0),\ (5, 2),\ (7, 1),\ (9, 3),\ (10, 2).$$



Tekintsük a szaggatott vonal fölötti halmaz konvex burkának alsó határát. Ez a töröttvonal az f polinom $p = 3$-hoz tartozó Newton-poligonja.



Figyeljük meg, hogy az ábrázolt 8 pont közül csupán a

$$P_0 = (0, 2),\ P_1 = (1, 0),\ P_2 = (4, 0),\ P_3 = (10, 2)$$

pontok lesznek csúcsai a Newton-poligonnak. A $(7, 1)$ koordinátájú pont nem csúcsa a Newton-poligonnak, annak ellenére hogy szerepelt a fent ábrázolt pontok között. Előfordulhat olyan eset is, amikor a Newton-poligon egy oldalára olyan rácspont esik, amely nem szerepelt az ábrázolt pontok között. Az ábrán például a P_1P_2 oldalon találhatóak a $(2, 0)$ és $(3, 0)$ rácspontok, amelyeket természetesen szintén nem tekintjük a Newton-poligon csúcsainak.

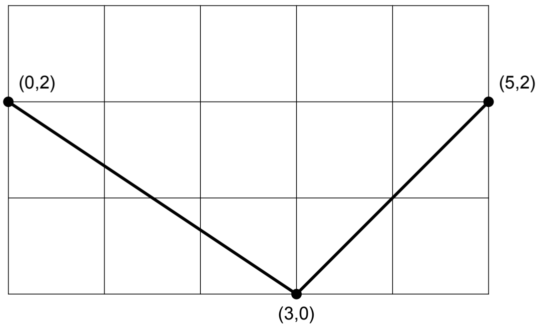
2. Dumas tétele

A következőkben Dumas tételét [4] és bizonyítását [13] ismertetjük. Ez a tétel kimondja, hogy ha egy f polinom előáll két alacsonyabb fokszámú polinom szorzataként, akkor ezen tényezők Newton-poligonjainak összeillesztésével megkapható f Newton-poligonja. Ennek segítségével a későbbiekben különböző irreducibilitási kritériumokat fogunk belátni. Mielőtt precízen kimondanánk és bizonyítanánk a tételt, tekintsük a következő példát.

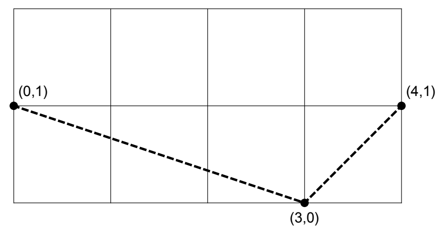
2.1. Példa. Legyen

$$f = 27000 + 5430x^3 + 27375x^4 + 125x^5 + 6x^6 + 105x^7 + 400x^8 + 125x^9.$$

Az f polinom felbomlik a következő g és h irreducibilis polinomok szorzatára: $g = 5400 + 6x^3 + 75x^4 + 25x^5$, $h = 5 + x^3 + 5x^4$. Tekintsük a g és h polinomok $p = 5$-höz tartozó Newton poligonját.

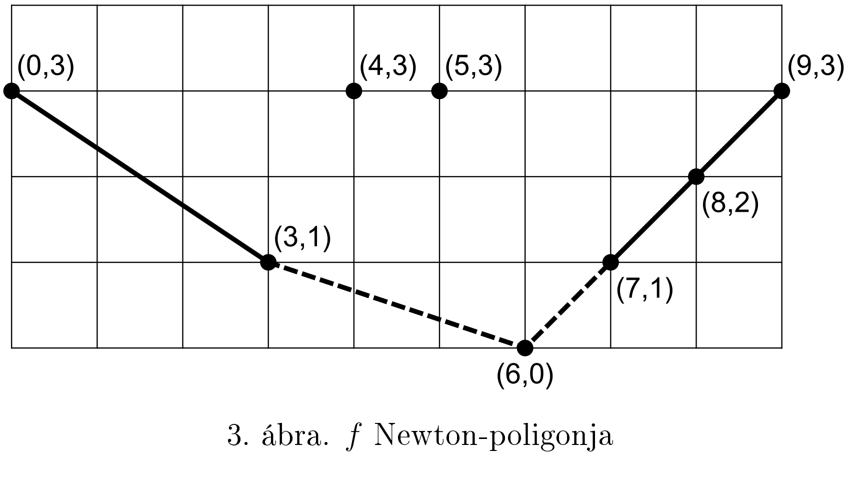


1. ábra. g Newton-poligonja



2. ábra. h Newton-poligonja

Dumas tétele alapján g és h Newton-poligonjából megkapható f Newton-poligonja. Vegyük a g és h polinom Newton-poligonjában található összes oldalt, majd rendezzük őket meredekségük szerint növekvő sorrendbe. A Newton-poligon konvexitása miatt az oldalak meredeksége balról jobbra haladva nő, így g és h Newton-poligonjaiból egyértelműen megkapható f Newton-poligonja, hiszen csak a meredekség szerint növekvő sorrendbe rendezett oldalakat kell sorban egymás után összefűzni. Az ábrán folytonos vonal jelöli azokat az oldalakat, melyek g Newton-poligonjából származnak, míg a szaggatott vonallal jelölt oldalakat h Newton-poligonjából vettük.



3. ábra. f Newton-poligonja

2.2. Tétel (Dumas tétele). *Legyen $f, g, h \in \mathbb{Z}[x]$ és $f = g \cdot h$. Ekkor f Newton-poligonja előáll g és h Newton-poligonja oldalainak összeillesztésével.*

Bizonyítás. Legyen $f = \sum_{i=0}^{n} A_i x^i$, $g = \sum_{j=0}^{m} B_j x^j$ és $h = \sum_{k=0}^{n-m} C_k x^k$. Tekintsük az f polinom nemnulla együtthatójú tagjait, és legyen $I = \{i \mid A_i \neq 0\}$. Minden $i \in I$ esetén végezzük el az $A_i = a_i p^{\alpha_i}$ felbontást, ahol $p \nmid a_i$. Ekkor $\alpha_i = \nu_p(A_i)$ és $f = \sum_{i \in I} a_i p^{\alpha_i} x^i$.

Hasonlóan járunk el a g és h polinomokra: $g = \sum_{j \in J} b_j p^{\beta_j} x^j$ és $h = \sum_{k \in K} c_k p^{\gamma_k} x^k$, ahol $J = \{j \mid B_j \neq 0\}$ és $K = \{k \mid C_k \neq 0\}$. Mivel f előáll g és h szorzataként, ezért $\deg f = n = \deg g + \deg h$.

Legyen $P_\ell P_{\ell+1}$ az f polinom Newton-poligonjának egy oldala, és legyenek P_ℓ koordinátái (i_-, α_{i_-}), valamint $P_{\ell+1}$ koordinátái (i_+, α_{i_+}). Ekkor az oldal meredeksége:

$$M = \frac{\alpha_{i_+} - \alpha_{i_-}}{i_+ - i_-}.$$

A $P_\ell P_{\ell+1}$ oldal az $\alpha = Mi + F$ egyenletű egyenesen van, ahol $F = \alpha_{i_+} - Mi_+ = \alpha_{i_-} - Mi_-$. Vegyük észre, hogy a konvexitás miatt minden (i, α_i) pont ezen az egyenesen, vagy fölötte helyezkedik el, tehát minden $i \in I$ esetén $\alpha_i - Mi \geq F$, ahol az egyenlőtlenség szigorú $i < i_-$ és $i > i_+$ esetén.

2.3. Definíció. Nevezzük minden $i \in \mathbb{N}_0$, $A \in \mathbb{Z}$ esetén a $\nu_p(A) - Mi$ számot az Ax^i monom súlyának, jelölése: $w(Ax^i)$.

2.4. Megjegyzés. A fentiekből az f polinom monomjai súlyára a következőt kapjuk:

$$\begin{aligned} w(a_i p^{\alpha_i} x^i) &> F, \quad \text{ha } i < i_-; \\ w(a_i p^{\alpha_i} x^i) &= F, \quad \text{ha } i_- \leq i \leq i_+; \\ w(a_i p^{\alpha_i} x^i) &> F, \quad \text{ha } i > i_+. \end{aligned}$$

Tehát az f-beli monomok súlyainak minimuma F, továbbá az i_- és i_+ számok egyértelműen meghatározottak, mint x legkisebb illetve legnagyobb kitevője, mely esetén a monom súlya minimális.

2.5. Lemma. *Legyen $B, C \in \mathbb{Z}$ és $j, k \in \mathbb{N}_0$. Ekkor*

1. $w(Bx^j \cdot Cx^k) = w(Bx^j) + w(Cx^k)$;
2. $w(Bx^j + Cx^j) \geq \min(w(Bx^j), w(Cx^j))$; *és*
3. *ha* $w(Bx^j) \neq w(Cx^j)$, *akkor* $w(Bx^j + Cx^j) = \min(w(Bx^j), w(Cx^j))$.

Bizonyítás.

1. Vizsgáljuk először az egyenlőség bal oldalát:

   $$w(Bx^j \cdot Cx^k) = w(BCx^j x^k) = w(BC \cdot x^{j+k}).$$

   A súly definíciója alapján a bal oldal $w(Bx^j \cdot Cx^k) = \nu_p(BC) - M(j+k)$. Felhasználva az 1.1. Lemma 1. pontját, átalakítás után kapjuk, hogy $\nu_p(BC) - M(j+k) = \nu_p(B) - Mj + \nu_p(C) - Mk$. Ez a súly definíciója alapján éppen $w(Bx^j) + w(Cx^k)$, ami a jobb oldalon szerepel.

2. A súly definícióját alkalmazva $\min(w(Bx^j), w(Cx^j)) = \min(\nu_p(B)-Mj, \nu_p(C)-Mj) = \min(\nu_p(B), \nu_p(C)) - Mj$. A bizonyítandó egyenlőtlenség bal oldalát alakítva kapjuk, hogy $w(Bx^j + Cx^j) = w((B+C)x^j)$. A súly definíciója alapján $w((B+C)x^j) = \nu_p(B+C) - Mj$. Az 1.1. Lemma 2. állítása szerint $\nu_p(B+C) \geq \min(\nu_p(B), \nu_p(C))$, ezzel az egyenlőtlenséget beláttuk.

3. A $w(Bx^j) \neq w(Cx^j)$ feltétel a súly definíciója alapján $\nu_p(B) - Mj \neq \nu_p(C) - Mj$ alakra hozható, amiből $\nu_p(B) \neq \nu_p(C)$ adódik. A bizonyítandó egyenlőség bal oldalát átalakítva kapjuk, hogy $w(Bx^j + Cx^j) = \nu_p(B+C) - Mj$. Mivel $\nu_p(B) \neq \nu_p(C)$, ezért az 1.1. Lemma 3. pontját alkalmazva kapjuk, hogy $\nu_p(B+C) = \min(\nu_p(B), \nu_p(C))$. Így $w(Bx^j+Cx^j) = \min(\nu_p(B), \nu_p(C))-Mj = \min(\nu_p(B) - Mj, \nu_p(C) - Mj)$, ami a súly definíciója alapján nem más, mint $\min(w(Bx^j), w(Cx^j))$.

$\square$

Visszatérve a tétel bizonyítására, tekintsük a g polinomra a

$$G = \min_{j \in J}(w(B_j x^j)) = \min_{j \in J}(\beta_j - Mj)$$

értéket és legyen j_- és j_+ az x legkisebb és legnagyobb kitevője, melyre

$$G = \beta_{j_-} - Mj_- = \beta_{j_+} - Mj_+. \tag{2.1}$$

Hasonlóan, legyen a h polinomra

$$H = \min_{k \in K}(w(C_k x^k)) = \min_{k \in K}(\gamma_k - Mk),$$

és legyen k_- és k_+ az x legkisebb és legnagyobb kitevője, melyre

$$H = \gamma_{k_-} - Mk_- = \gamma_{k_+} - Mk_+. \tag{2.2}$$

Vizsgáljuk a $j_- + k_-$ kitevőjű tagot az $f = g \cdot h$ egyenlőségben. A polinomok szorzásának szabályából tudjuk, hogy:

$$A_{j_-+k_-} x^{j_-+k_-} = \sum_{j+k=j_-+k_-} B_j x^j \cdot C_k x^k. \tag{2.3}$$

1. Ha $j = j_-$ és $k = k_-$, akkor $w(B_j x^j) = G$ és $w(C_k x^k) = H$, tehát a 2.5. Lemma 1. pontja alapján $w(B_j x^j \cdot C_k x^k) = G + H$.

2. Ha $j > j_-$, akkor $k < k_-$, tehát $w(B_j x^j) \geq G$ és $w(C_k x^k) > H$, tehát a 2.5. Lemma 1. pontja alapján $w(B_j x^j \cdot C_k x^k) > G + H$.

3. Hasonlóan, ha $j < j_-$, akkor $k > k_-$, tehát $w(B_j x^j) > G$ és $w(C_k x^k) \geq H$, tehát a 2.5. Lemma 1. pontja alapján $w(B_j x^j \cdot C_k x^k) > G + H$.

A (2.3) egyenlőség jobb oldalát kettébontva:

$$\sum_{j+k=j_-+k_-} B_j x^j \cdot C_k x^k = \sum_{\substack{j+k=j_-+k_- \\ (j,k)\neq(j_-,k_-)}} B_j x^j \cdot C_k x^k + B_{j_-} x^{j_-} \cdot C_{k_-} x^{k_-}.$$

Jelölje S a fenti egyenlőség jobb oldalán álló szummát. Ekkor a 2.5. Lemma 2. pontja alapján

$$w(S) \geq \min\{w(B_j x^j \cdot C_k x^k) \mid j+k = j_- + k_-, (j,k) \neq (j_- + k_-)\} > G + H.$$

Tehát $w(S) > G + H$ és $w(B_{j_-} x^{j_-} C_{k_-} x^{k_-}) = G + H$, ezért a 2.5. Lemma 3. pontja miatt

$$w(A_{j_- + k_-} x^{j_- + k_-}) = w\left(\sum_{j+k=j_-+k_-} B_j x^j \cdot C_k x^k \right) = \min(w(S), G+H) = G + H.$$

A bizonyítás következő részében megmutatjuk, hogy $F = G + H$ és $i_- = j_- + k_-$. Ehhez vizsgáljuk az $A_i x^i$ monomot tetszőleges $i \in I$ esetén:

$$A_i x^i = \sum_{j+k=i} B_j x^j \cdot C_k x^k.$$

Amennyiben $i < j_- + k_-$, akkor $j < j_-$ vagy $k < k_-$. Az első esetben $w(B_j x^j) > G$ és $w(C_k x^k) \geq H$, így a 2.5. Lemma 1. pontja szerint $w(A_i x^i) > G + H$. A második esetben $w(B_j x^j) \geq G$ és $w(C_k x^k) > H$, ezért a 2.5 lemma 1. pontja miatt $w(A_i x^i) > G + H$. Ha $i > j_- + k_-$, akkor $w(B_j x^j) \geq G$ és $w(C_k x^k) \geq H$, ezért a 2.5. Lemma 1. pontja alapján $w(A_i x^i) \geq G + H$.

Összefoglalva:

$$\begin{aligned} i < j_- + k_- \quad &\Longrightarrow \quad w(A_i x^i) > G + H; \\ i = j_- + k_- \quad &\Longrightarrow \quad w(A_i x^i) = G + H; \\ i > j_- + k_- \quad &\Longrightarrow \quad w(A_i x^i) \geq G + H. \end{aligned}$$

Tehát $\min\{w(A_i x^i) \mid i \in I\} = G + H$, továbbá

$$j_- + k_- = \min\{i \mid w(A_i x^i) = G + H\}.$$

Másrészt, a 2.4. Megjegyzés szerint $\min\{w(A_i x^i) \mid i \in I\} = F$, valamint

$$i_- = \min\{i \mid w(A_i x^i) = F\}.$$

Ezekből következik, hogy $F = G + H$ és $i_- = j_- + k_-$. Az $i_+ = j_+ + k_+$ egyenlőséget hasonlóan bizonyíthatjuk.

Mivel $i_- = j_- + k_-$ és $i_+ = j_+ + k_+$, ezért

$$i_+ - i_- = (j_+ - j_-) + (k_+ - k_-). \tag{2.4}$$

Ha $j_+ - j_-$ és $k_+ - k_-$ is pozitív, akkor g Newton-poligonjában van egy (j_-, β_{j_-}) és (j_+, β_{j_+}) végpontú oldal, illetve h Newton-poligonjában található (k_-, γ_{k_-}) és (k_+, γ_{k_+}) végpontokkal megadható oldal. Ez a két oldal éppen M meredekségű, hiszen (2.1) és (2.2) miatt

$$\frac{\beta_{j_+} - \beta_{j_-}}{j_+ - j_-} = M = \frac{\gamma_{k_+} - \gamma_{k_-}}{k_+ - k_-}.$$

A (2.4) egyenlőségből következik, hogy az M meredekségű oldalak v-hosszainak összege a g és a h polinomok Newton-poligonjában megegyezik az f Newton-poligonjában található M meredekségű oldal, azaz $P_\ell P_{\ell+1}$ v-hosszával.

Ha $j_+ - j_-$ és $k_+ - k_-$ valamelyike nulla, akkor csak g vagy h Newton-poligonjában található M meredekségű oldal, melynek v-hossza megegyezik $P_\ell P_{\ell+1}$ v-hosszával.

Beláttuk, hogy f Newton-poligonjának minden oldala vagy szerepel g vagy h Newton-poligonjában, vagy előáll g és h Newton-poligonja egy-egy oldalának összeillesztésével, azaz f Newton-poligonja „felépíthető" a g és h Newton-poligonját alkotó oldalakból.

Nyilvánvalóan az f polinom Newton-poligonjában az oldalak v-hosszainak összege éppen $\deg f$, hasonlóan a g polinom Newton-poligonjában az oldalak v-hosszainak összege $\deg g$, továbbá a h polinom Newton-poligonjában az oldalak v-hosszainak összege $\deg h$. Mivel $\deg f = \deg g + \deg h$, ezért g és h Newton-poligonjának minden oldalát felhasználtuk f Newton-poligonjának fenti felépítésében. $\square$

Vegyük észre, hogy amennyiben egy polinom Newton-poligonja csak egy oldalból áll, melyen nem található rácspont, akkor a 2.2. Tétel miatt a polinom irreducibilis.

3. Irreducibilitási kritériumok

Ebben a részben különböző irreducibilitási kritériumokat fogunk kimondani, melyeket Dumas tételével könnyedén be tudunk bizonyítani. A könnyebb felírás érdekében bevezetjük a pontos osztó fogalmát.

3.1. Definíció. Tetszőleges p prímszám és a egész szám esetén azt mondjuk, hogy p^k pontos osztója a-nak, ha $\nu_p(a) = k$.
Jelölés: $p^k \parallel a$.

Az egyik legelső irreducibilitási kritérium a Schönemann–Eisenstein-féle kritérium. Schönemann egy 1846-os cikkében szerepel ez a tétel [14], Eisenstein pár évvel később, függetlenül Schönemanntól, 1850-ben publikálta [5]. A kritérium történetéről bővebb leírás található Cox cikkében [2].

3.2. Tétel (Schönemann–Eisenstein-tétel). *Legyen $f = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$. Ha létezik olyan p prímszám, melyre*

$$p \parallel a_0,\ p \mid a_1, \ldots,\ p \mid a_{n-1},\ p \nmid a_n,$$

akkor f irreducibilis a racionális számok teste felett.

Bizonyítás. Ebben a speciális esetben az f polinom p-hez tartozó Newton-poligonja egyetlen oldalból áll $(0, 1)$ és $(n, 0)$ végpontokkal, melyen nem található rácspont, tehát a 2.2. Tételből következik, hogy f irreducibilis. □

Az előző tételnek egy általánosabb formája a következő tétel.

3.3. Tétel. *Legyen $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ és $1 \leq k \leq n - 1$. Ha létezik olyan p prímszám, amelyre*

$$p \parallel a_0,\ p \mid a_1, \ldots, p \mid a_k,\ p \nmid a_{k+1},$$

akkor f-nek van olyan irreducibilis osztója, melynek foka legalább $k + 1$.

Bizonyítás. A megadott oszthatósági feltételek miatt az f polinom Newton-poligonjában biztosan szerepel a $(0, 1)$ és $(k + 1, 0)$ végpontokkal megadott oldal, melyen nincs másik rácspont. Ekkor a 2.2. Tétel szerint f irreducibilis felbontásában valamelyik tényező Newton-poligonjának tartalmaznia kell ezt az oldalt, vagyis ennek a tényezőnek a foka legalább $k + 1$. □

Vegyük észre, hogy a $k = n-1$ eset éppen a Schönemann–Eisenstein-kritériumot adja. A tételt a $k = n - 2$ esetben alkalmazva kapjuk az alábbi irreducibilitási kritériumot, mely megtalálható Perron cikkében [12].

3.4. Következmény. *Legyen $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$. Ha f-nek nincs racionális gyöke, és létezik olyan p prímszám, amelyre*

$$p \parallel a_0,\ p \mid a_1, \ldots, p \mid a_{n-2},\ p \nmid a_{n-1},$$

akkor f irreducibilis.

Bizonyítás. A feltételek szerint f Newton-poligonja két oldalból áll, a bal szélső oldal végpontjai $(0, 1)$ és $(n-1, 0)$, míg a másik oldal végpontjai $(n-1, 0)$ és $(n, \nu_p(a_n))$. Mivel a bal szélső oldalon nem található rácspont, így ha f nem irreducibilis, akkor csak egy $(n-1)$-ed fokú és egy elsőfokú polinom szorzatára bontható. Azonban f-nek nincs racionális gyöke, ezért nem lehet elsőfokú osztója. Következésképp f irreducibilis. $\square$

Alkalmazásként oldjuk meg az 1993-as Nemzetközi Matematikai Diákolimpia első feladatát. Ehhez Rolle tételét is használni fogjuk, melynek segítségével ellenőrizhető, hogy egy egész együtthatós polinomnak van-e racionális gyöke.

3.5. Tétel (Rolle tétele). *Legyen $f = a_n x^n + \ldots + a_1 x + a_0$ egy tetszőleges egész együtthatós polinom. Ha $\frac{s}{t}$ egy egyszerűsíthetetlen tört alakjában felírt racionális szám, akkor*

$$f\left(\frac{s}{t}\right) = 0 \implies t \mid a_n, \ s \mid a_0.$$

3.6. Megjegyzés. Vegyük észre, hogy $a_n = 1$ esetén az f polinom racionális gyökei mindig egész számok.

3.7. Példa. Bizonyítsuk be, hogy $n > 1$ esetén az $x^n + 5x^{n-1} + 3$ polinom irreducibilis.

Vegyük észre, hogy $p = 3$ esetén teljesülnek a 3.4. Következmény oszthatósági feltételei, hiszen $3 \parallel 3$ és $3 \nmid 5$. A 3.5. Tétel szerint, ha f-nek van racionális gyöke, akkor a gyöke egy olyan egész szám, mely osztja f konstans tagját, ami esetünkben 3. Tehát ha f-nek van racionális gyöke, akkor az csak $\pm 1, \pm 3$ lehet. Könnyen ellenőrizhető, hogy ezek egyike sem gyöke f-nek, ezért a 3.4. Következmény összes feltétele teljesül, vagyis f irreducibilis.

A következő kritérium Netto 1896-os cikkében szerepel [10].

3.8. Tétel. *Legyen $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ és $k < \frac{n}{2}$. Ha létezik olyan p prímszám, amelyre*

$$p^2 \parallel a_0, \ p^2 \mid a_1, \ldots, p^2 \mid a_k, \ p \mid a_{k+1}, \ \ldots, p \mid a_{n-1}, \ p \nmid a_n,$$

akkor f-nek nincs olyan osztója, melynek foka legfeljebb k.

Bizonyítás. Az f polinom Newton-poligonja legfeljebb két oldalból állhat, hiszen $\nu_p(a_0) = 2$ és $\nu_p(a_n) = 0$. Ha egy oldalból áll, akkor annak az oldalnak a két végpontja a $(0, 2)$ és az $(n, 0)$ pont. Amennyiben f foka páratlan, nincs rácspont az oldalon, tehát f irreducibilis. Ha f foka páros, akkor az $(\frac{n}{2}, 1)$ rácspont az oldalra esik, tehát f csak két $\frac{n}{2}$-ed fokú polinom szorzatára bomolhat (ha nem irreducibilis), viszont $k < \frac{n}{2}$.

Amennyiben f Newton-poligonja két oldalból áll, akkor három csúcsa van: $(0, 2)$, $(a, 1)$ és $(n, 0)$. A $p^2 \mid a_1, \ldots, p^2 \mid a_k$ feltételekből következik, hogy $a \geq k+1$. Továbbá $a \leq \frac{n}{2}$, mert ellenkező esetben a második oldal meredeksége kisebb lenne mint az első oldalé, ami a konvexitás miatt nem lehetséges. Tehát a Newton-poligon két oldalának v-hossza $a \geq k+1$ és $n - a \geq \frac{n}{2} > k$, így a 2.2. Tétel alapján f bármely osztójának foka nagyobb, mint k. $\square$

Az $n = 2k+1$ speciális esetből adódik az alábbi kritérium, ez szerepel Netto [10] és Oleinikov cikkében is [11].

3.9. Következmény. *Legyen* $f = a_{2k+1}x^{2k+1} + \cdots + a_1x + a_0 \in \mathbb{Z}[x]$. *Ha létezik olyan* p *prímszám, amelyre*

$$p^2 \parallel a_0,\ p^2 \mid a_1, \ldots, p^2 \mid a_k,\ p \mid a_{k+1},\ \ldots, p \mid a_{2k},\ p \nmid a_{2k+1},$$

akkor f *irreducibilis.*

Bizonyítás. Alkalmazzuk a 3.8. Tételt $n = 2k + 1$ esetén. Ekkor $k = \frac{n-1}{2} < \frac{n}{2}$, továbbá az oszthatósági feltételek is teljesülnek, vagyis f-nek nincs olyan osztója, melynek foka legfeljebb k. Azonban, ha f felbomlana két polinom szorzatára, akkor a kisebb fokszámú tényező foka legfeljebb k lenne, tehát f irreducibilis. □

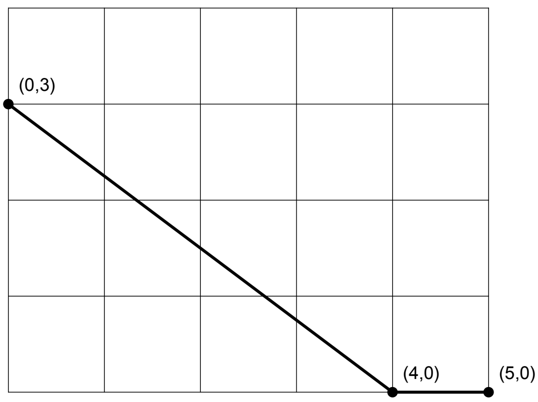
Königsberger [9] a következő kritériumot adta ötödfokú polinomokra, amelyben már két prím szerepel.

3.10. Tétel. *Legyen* $f = a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 \in \mathbb{Z}[x]$. *Ha léteznek olyan különböző* p *és* q *prímszámok, amelyekre*

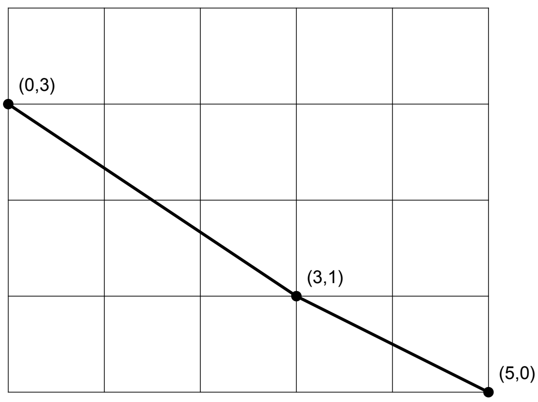
$$\begin{gathered} p^3 \parallel a_0,\ p^3 \mid a_1,\ p^2 \mid a_2,\ p \mid a_3,\ p \nmid a_4,\ p \nmid a_5, \\ q^3 \parallel a_0,\ q^3 \mid a_1,\ q^2 \mid a_2,\ q \parallel a_3,\ , q \mid a_4,\ q \nmid a_5, \end{gathered}$$

akkor f *irreducibilis.*

Bizonyítás. Az f polinom bármilyen $a_0,\ a_1, \ldots,\ a_5$ együtthatói esetén a megadott oszthatósági feltételek szerint a p-hez és q-hoz tartozó Newton-poligon a következő (az ábrázolt pontokon kívül más pont nem szerepelhet Newton-poligonban):



4. ábra. p-hez tartozó Newton-poligon



5. ábra. q-hoz tartozó Newton-poligon

A 4. ábra alapján az f polinom, ha felbomlik, csak egy első és egy negyedfokú polinom szorzatára bomolhat. Ellenben az 5. ábra szerint az f polinom csak egy másod- és egy harmadfokú polinom szorzatára bontható. Következésképp f irreducibilis. □

4. Egy összetettebb példa

Ebben a részben egy összetettebb példát vizsgálunk, mely Filaseta egyik 2005-ös előadásában szerepelt [7].

4.1. Példa. Vizsgáljuk irreducibilitási szempontból az

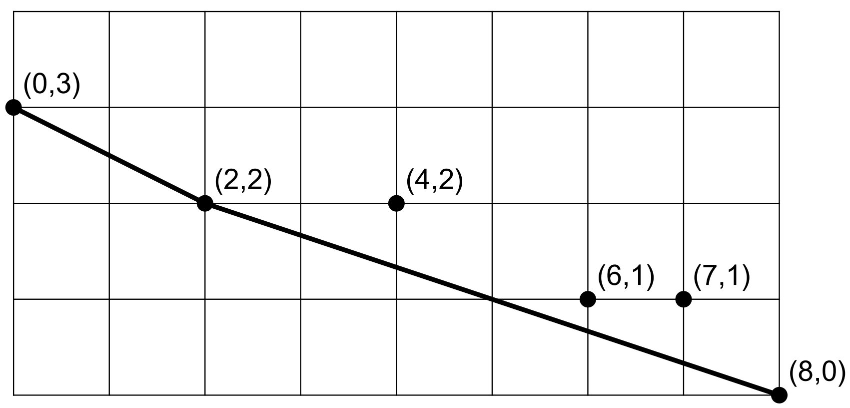
$$f = 81000 + 2700x^2 + 150x^4 + 15x^6 + 20x^7 + 42x^8$$

polinomot.

Tekintsük az f polinom $p = 5$–höz tartozó Newton-poligonját. Ehhez bontsuk fel f minden együtthatóját a korábban látott módon:

$$f = 5^3 \cdot 648 + 5^2 \cdot 108x^2 + 5^2 \cdot 6x^4 + 5^1 \cdot 3x^6 + 5^1 \cdot 4x^7 + 5^0 \cdot 42x^8.$$

Így az alábbi Newton-poligont kapjuk:



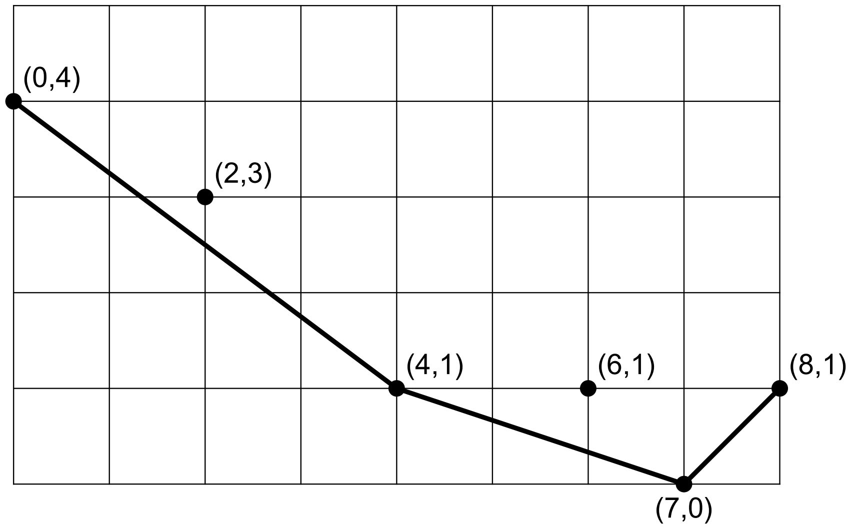
6. ábra. $p = 5$–höz tartozó Newton-poligon

Vizsgáljuk meg, hogy ha f felbontható polinomok szorzatára, az osztóknak milyen fokszámai lehetnek. A Newton-poligonban egy 2 és egy 6 v-hosszú oldal szerepel, de a hosszabb oldalon található rácspont, így az felbomolhat két 3 v-hosszú oldalra. Tehát egy tetszőleges $f = g \cdot h$ nemtriviális felbontásnál g és h Newton-poligonjában együttesen $2, 3, 3$ v-hosszúságú oldalak szerepelnek. Így a $(k, l) := (\deg g, \deg h)$ fokszámpárra két lehetőség van: $(k, l) = (2, 3 + 3) = (2, 6)$ és $(k, l) = (3, 2 + 3) = (3, 5)$. (Az általánosság megszorítása nélkül feltettük, hogy $k \leq l$.)

Hasonlóan járjunk el $p = 3$ esetén is, ekkor az együtthatók megfelelő felbontása a következő:

$$f = 3^4 \cdot 1000 + 3^3 \cdot 100x^2 + 3^1 \cdot 50x^4 + 3^1 \cdot 5x^6 + 3^0 \cdot 20x^7 + 3^1 \cdot 14x^8,$$

melyhez a következő Newton-poligon tartozik:



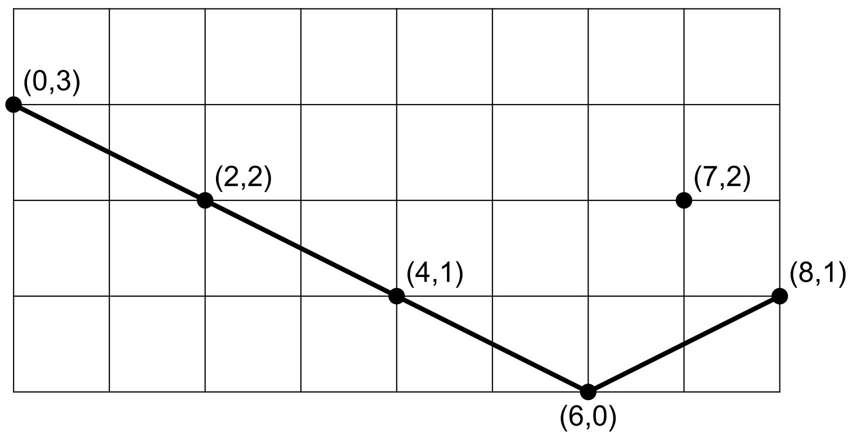
7. ábra. $p = 3$–hoz tartozó Newton-poligon

Itt az oldalak v-hosszai: $1, 3, 4$, tehát a fentiekhez hasonlóan a (k, l) fokszámpárra az $(1, 3+4) = (1, 7)$, $(3, 1+4) = (3, 5)$ és $(4, 1+3) = (4, 4)$ lehetőségek adódnak.

Vizsgáljuk a $p = 2$–höz tartozó Newton-poligont. Ekkor az együtthatók felbontása

$$f = 2^3 \cdot 10125 + 2^2 \cdot 675x^2 + 2^1 \cdot 75x^4 + 2^0 \cdot 15x^6 + 2^2 \cdot 5x^7 + 2^1 \cdot 21x^8,$$

mely alapján a $p = 2$–höz tartozó Newton-poligon a következő:



8. ábra. $p = 2$–höz tartozó Newton-poligon

Ebben az esetben egy 6 és egy 2 v-hosszúságú oldalt kapunk, azonban a 6 v-hosszúságú oldalt a rácspontok három 2 v-hosszúságú szakaszra bontják. Ennek alapján a lehetséges (k, l) párok $(2, 2+2+2) = (2, 6)$ és $(2+2, 2+2) = (4, 4)$.

Tehát a $p = 5, 3, 2$ prímekhez tartozó Newton-poligonokat vizsgálva a (k, l) fokszámpárra az alábbi lehetőségeket kaptuk:

$p = 5$:		$(2, 6)$	$(3, 5)$	
$p = 3$:	$(1, 7)$		$(3, 5)$	$(4, 4)$
$p = 2$:		$(2, 6)$		$(4, 4)$

Mivel nem található olyan felbontás, amely mind a három prímszám esetén kielégíti a fokszámokra vonatkozó feltételt, így f nem bontható fel, tehát irreducibilis.

5. Schur tétele

Ebben a fejezetben Schur egy szép tételét ismertetjük. A bizonyításhoz három lemmát használunk fel, melyek közül az elsőt be is látjuk.

5.1. Lemma. *Legyenek k, l egészek úgy, hogy $k > l \geq 0$ és legyen $g = \sum_{j=0}^{n} b_j x^j \in \mathbb{Z}[x]$. Tegyük fel, hogy létezik olyan p prím, melyre $p \nmid b_n$, és $p \mid b_j$ minden $j \in \{0, 1, \ldots, n-l-1\}$ esetén, továbbá a g polinom p-hez tartozó Newton-poligonjában a bal szélső oldal meredeksége nagyobb mint $-\frac{1}{k}$. Ekkor g-nek nincs olyan $u \in \mathbb{Z}[x]$ osztója, melyre $l + 1 \leq \deg u \leq k$, sőt ugyanez érvényes az $f = \sum_{j=0}^{n} a_j b_j x^j$ polinomra is tetszőleges $a_0, a_1, \ldots, a_n \in \mathbb{Z}$ esetén, amennyiben $p \nmid a_0$ és $p \nmid a_n$.*

Bizonyítás. Először indirekt módon belátjuk az állítást a g polinomra. Tegyük fel, hogy létezik a g polinomnak olyan osztója, melynek a foka $l+1$ és k közé esik, legyen ez az osztó u. Vizsgáljuk a g polinom p-hez tartozó Newton-poligonját.

Mivel a Newton-poligon oldalainak meredeksége a konvexitás miatt balról jobbra nő, ezért minden oldal meredeksége nagyobb, mint $-\frac{1}{k}$. Továbbá $p \nmid b_n$ miatt a poligon jobb szélső pontja $(n, 0)$ az első tengelyen van, ezért minden oldal meredeksége nempozitív, azaz az oldalak meredekségei $-\frac{1}{k}$ és 0 között vannak. A jobb szélső oldal meredeksége lehet 0 is, ha létezik olyan b_j ($j \in \{n-l, n-l+1, \ldots, n-1\}$), melyre $p \nmid b_j$.

Tekintsünk egy tetszőleges negatív meredekségű oldalt. Legyen ennek az oldalnak a két végpontja (a, b) és (c, d). Mivel az oldal meredeksége negatív, ezért $d - b < 0$. Másrészt, az oldalak rácspontokat kötnek össze, tehát $d - b \in \mathbb{Z}$. Következésképp $d - b \leq -1$. Az (a, b) és (c, d) pontokon áthaladó egyenes meredeksége éppen $\frac{d-b}{c-a}$, továbbá a $d - b \leq -1$ egyenlőtlenséget felhasználva: $\frac{d-b}{c-a} \leq \frac{-1}{c-a}$. A lemma feltétele alapján ennek az oldalnak a meredeksége nagyobb mint $-\frac{1}{k}$, ezért $-\frac{1}{c-a} > -\frac{1}{k}$, melyből $c - a > k$ adódik, tehát az oldal v-hossza nagyobb mint k. Vagyis negatív meredekségű oldal nem szerepelhet u Newton-poligonjában, hiszen $\deg u \leq k$.

Az előzőekből következik, hogy u Newton-poligonjában csak 0 meredekségű oldal szerepelhet, viszont a $p \mid b_j$ ($j = 0, 1, \ldots, n-l-1$) feltétel miatt g Newton-poligonjában a 0 meredekségű (jobb szélső) oldal v-hossza legfeljebb l lehet, tehát $\deg u \leq l$, ami ellentmond az $l + 1 \leq \deg u$ feltételnek.

Térjünk át az f polinom vizsgálatára. Figyeljük meg mi történik g Newton-poligonjával, ha minden együtthatóját megszorozzuk egy egész számmal. Vegyük észre, hogy ha $p \mid a_j$, akkor $\nu_p(a_j b_j) > \nu_p(b_j)$, valamint ha $p \nmid a_j$, akkor $\nu_p(a_j b_j) = \nu_p(b_j)$. Tehát minden j-re $\nu_p(a_j b_j) \geq \nu_p(b_j)$, azaz a g-ről f-re való áttérés során a pontok csak „felfelé” mozdulhatnak el. Mivel $p \nmid a_0$, a poligon bal szélső pontja helyben marad, ezért a bal szélső oldal meredeksége nem csökkenhet. Tehát f Newton-poligonjára is igaz, hogy a bal szélső oldal meredeksége nagyobb, mint $-\frac{1}{k}$. Másrészt $p \nmid a_n$ miatt $p \nmid a_n b_n$, továbbá minden $j \in \{0, 1, \ldots, n-l-1\}$ esetén $p \mid a_j b_j$. Ez azt jelenti, hogy f Newton-poligonjában a 0 meredekségű (jobb szélső) oldal (ha van ilyen) v-hossza továbbra is legfeljebb l lehet. Tehát a korábbi gondolatmenet f-re is alkalmazható. $\square$

A következő lemmát Schur bizonyította be a [15] cikkben, de korábban már Sylvester is igazolta [16]. Ez a lemma fog segíteni Schur tételének bizonyításában megfelelő p prímszámot találni, amelyhez tartozó Newton-poligont fogjuk vizsgálni.

5.2. Lemma. *Legyenek m és k pozitív egész számok úgy, hogy $m \geq k$. Ekkor létezik olyan $p \geq k+1$ prím, amelyre p osztja az $m+1, m+2, \ldots, m+k$ számok valamelyikét.*

Figyeljük meg, hogy a fenti lemma $m = k$ esetén azt mutatja, hogy tetszőleges k pozitív egészre van olyan p prím, amelyre $k + 1 \leq p \leq 2k$. Tehát ez a lemma Csebisev tételének egy általánosítása.

A következő formulát Legendre adta tetszőleges n természetes szám és p prímszám esetén a $\nu_p(n!)$ kitevő kiszámítására.

5.3. Lemma. *Tetszőleges $n \in \mathbb{N}$ és p prím esetén*

$$\nu_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \ldots = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor .$$

5.4. Megjegyzés. Vegyük észre, hogy a fenti formálisan végtelen összeg véges, hiszen létezik olyan r nemnegatív egész szám, melyre $p^r \leq n < p^{r+1}$. Ekkor $\frac{n}{p^i} < 1$, tehát $\left\lfloor \frac{n}{p^i} \right\rfloor = 0$ minden $i > r$ esetén. Vagyis:

$$\nu_p(n!) = \sum_{i=1}^{r} \left\lfloor \frac{n}{p^i} \right\rfloor .$$

A fenti három lemma segítségével be tudjuk bizonyítani Schur tételét, amely irreducibilis polinomok egy végtelen családját adja. A tétel Filaseta-féle bizonyítását ismertetjük [6].

5.5. Tétel (Schur tétele). *Legyen n egy pozitív egész szám, továbbá $a_0, a_1, \ldots, a_n$ tetszőleges egészek, úgy hogy $|a_0| = 1$ és $|a_n| = 1$. Ekkor*

$$a_n \frac{x^n}{n!} + a_{n-1} \frac{x^{n-1}}{(n-1)!} + \ldots + a_1 x + a_0$$

irreducibilis a racionális számok teste felett.

Bizonyítás. Mivel a tételben szereplő $a_n \frac{x^n}{n!} + a_{n-1} \frac{x^{n-1}}{(n-1)!} + \ldots + a_1 x + a_0$ polinom nem egész együtthatós, vizsgáljuk $n!$-szorosát, hiszen egy konstanssal való szorzás nem változtat a racionális számtest feletti irreducibilitáson. Tehát tekintsük a $g = \sum_{j=0}^{n} \frac{n!}{j!} x^j$ és az $f = \sum_{j=0}^{n} a_j \frac{n!}{j!} x^j$ polinomokat, továbbá legyen $b_j = \frac{n!}{j!}$.

Tegyük fel, hogy f nem irreducibilis és legyen k a legkisebb fokú nemtriviális osztójának foka. Ekkor $k \leq \frac{1}{2}n$, tehát $n - k \geq k$. Az 5.2. Lemmát $m = n - k$-ra alkalmazva kapjuk, hogy létezik olyan $p \geq k + 1$ prím, amelyre $p \mid n - l$ valamely $l \in \{0, 1, \ldots, k - 1\}$ esetén. Megmutatjuk, hogy az így megkapott k és l egészek esetén az 5.1. Lemma feltételei teljesülnek a g polinom b_j együtthatóira. Ha $j \in \{0, 1, \ldots, n - l - 1\}$, akkor $n - l$ szerepel a $b_j = \frac{n!}{j!} = n \cdot (n-1) \cdot \ldots \cdot (j+1)$ szorzatban, ezért $p \mid b_j$. Továbbá mivel $b_n = \frac{n!}{n!} = 1$, ezért $p \nmid b_n$.

Vizsgáljuk a g polinom p-hez tartozó Newton-poligonját. Mutassuk meg, hogy g Newton-poligonjában a bal szélső oldal meredeksége nagyobb, mint $-\frac{1}{k}$. A konvexitás miatt ennek az oldalnak a meredeksége a legkisebb, tehát éppen

$$\min_{1 \leq j \leq n} \left(\frac{\nu_p(b_j) - \nu_p(b_0)}{j - 0} \right) = \min_{1 \leq j \leq n} \left(\frac{\nu_p(n!/j!) - \nu_p(n!)}{j} \right).$$

Legyen r az a nemnegatív egész szám, melyre $p^r \leq n < p^{r+1}$. Ekkor bármely $j \in \{1, 2, \ldots, n\}$ esetén az 1.1. Lemma 1. állítását és az 5.3. Lemmát használva kapjuk, hogy

$$\nu_p(n!) - \nu_p(n!/j!) = \nu_p(j!) = \left\lfloor \frac{j}{p} \right\rfloor + \left\lfloor \frac{j}{p^2} \right\rfloor + \ldots + \left\lfloor \frac{j}{p^r} \right\rfloor \leq j \cdot \left(\frac{1}{p} + \ldots + \frac{1}{p^r} \right).$$

Összegezzük a jobb oldalon álló mértani sorozatot, majd becsüljük felülről:

$$j \cdot \left(\frac{1}{p} + \ldots + \frac{1}{p^r} \right) = j \cdot \frac{p^r - 1}{p^r(p-1)} = j \cdot \frac{p^r - 1}{p^r} \cdot \frac{1}{p-1} < \frac{j}{p-1}.$$

Ezt a becslést felhasználva kapjuk, hogy

$$\frac{\nu_p(n!/j!) - \nu_p(n!)}{j} > -\frac{\frac{j}{p-1}}{j} = -\frac{1}{p-1}.$$

Tehát minden $j \in \{1, 2, \ldots, n\}$ esetén $\frac{\nu_p(n!/j!) - \nu_p(n!)}{j} > -\frac{1}{k}$, hiszen $p \geq k+1$. Ezzel beláttuk, hogy a bal szélső oldal meredeksége nagyobb mint $-\frac{1}{k}$, így teljesülnek az 5.1. Lemma feltételei. Tehát f-nek nincs olyan u osztója, melyre $l+1 \leq \deg u \leq k$, ami ellentmond annak, hogy k az f polinom legkisebb fokú osztójának foka. □

Schur tételéből következik, hogy az e^x, $\sin x$, $\cos x$ függvények Taylor-polinomjai irreducibilisek, csakúgy mint az alábbi formulákkal definiált *Laguerre-polinomok:*

$$L_n = \frac{e^x}{n!} \frac{d^n}{dx^n} \left(e^{-x} x^n \right) = \sum_{k=0}^{n} (-1)^k \cdot \binom{n}{k} \cdot \frac{x^k}{k!}.$$

5.6. Következmény. *Tetszőleges n természetes szám esetén az alábbi polinomok irreducibilisek:*

$$\begin{aligned}
&1 + x + \frac{x^2}{2!} + \ldots + \frac{x^n}{n!} \\
&x - \frac{x^3}{3!} + \frac{x^5}{5!} + \ldots + (-1)^n \cdot \frac{x^{2n+1}}{(2n+1)!} \\
&1 - \frac{x^2}{2!} + \frac{x^4}{4!} + \ldots + (-1)^n \cdot \frac{x^{2n}}{(2n)!} \\
L_n = \ &1 - nx + \binom{n}{2} \cdot \frac{x^2}{2!} + \ldots + (-1)^n \cdot \frac{x^n}{n!}
\end{aligned}$$

Hivatkozások

[1] C. Christensen, *Newton's Method for Resolving Affected Equations,* College Math. J. **27** (1996), 330–340.

[2] D. A. Cox, *Why Eisenstein proved the Eisenstein criterion and why Schönemann discovered it first,* Amer. Math. Monthly **118** (2011), no. 1, 3–21.

[3] H. L. Dorwart, *Irreducibility of Polynomials,* Amer. Math. Monthly **42** (1935), no. 6, 369–381.

[4] G. Dumas, *Sur quelques cas d'irréducibilité des polynomes à coefficients rationnels,* J. Math. Pures Appl. 6éme Série **2** (1906), 191–258.

[5] G. Eisenstein, *Über die Irreductibilität und einige andere Eigenschaften der Gleichung, von welcher die Theilung der ganzen Lemniscate abhängt,* J. Reine Angew. Math. **39** (1850), 160–179.

[6] M. Filaseta, *The irreducibility of all but finitely many Bessel polynomials,* Acta Math. **174** (1995), no. 2, 383–397.

[7] M. Filaseta, *Different uses of Diophantine analysis in the theory of irreducibility,* Diophantine Equations Conference at the Tata Institute of Fundamental Research in Honor of T. N. Shorey's 60th birthday, Mumbai, India, 2005.

[8] L. Kronecker, *Grundzüge einer arithmetischen Theorie der algebraischen Grössen,* J. Reine Angew. Math. **92** (1882), 1–122.

[9] L. Königsberger, *Ueber die Entwicklungsform algebraischer Functionen und die Irreducibilität algebraischer Gleichungen,* J. Reine Angew. Math. **121** (1900), 320–359.

[10] E. Netto, *Ueber die Irreductibilität ganzzahliger ganzer Functionen,* Math. Ann. **48** (1896), no. 1-2, 81–88.

[11] V. A. Oleinikov, *Irreducibility and Irrationality,* Kvant Selecta: Algebra and Analysis II, Mathematical World **15**, 95–103. American Mathematical Society, 1999.

[12] O. Perron, *Über eine Anwendung der Idealtheorie auf die Frage nach der Irreduzibilität algebraischer Gleichungen,* Math. Ann. **60** (1905), no. 3, 448–458.

[13] V. V. Prasolov, *Polynomials,* Algorithms and Computation in Mathematics **11**, Springer-Verlag, 2004.

[14] L. Schönemann, *Von denjenigen Moduln, welche Potenzen von Primzahlen sind,* J. Reine Angew. Math. **32** (1846), 93–105.

[15] I. Schur, *Einige Sätze über Primzahlen mit Anwendungen auf Irreduzibilitätsfragen I,* Sitzungsber. Preuss. Akad. Wiss., Phys.-Math. Kl. **14** (1929), 125-136.

[16] J. J. Sylvester, *On arithmetical series,* Messenger of Math., **21** (1892), 1-19, 87-120.

Nyilatkozat

Alulírott Sarró Mihály kijelentem, hogy a szakdolgozatban foglaltak a saját munkám eredményei, és csak a hivatkozott forrásokat (szakirodalom, eszközök, stb.) használtam fel. Tudomásul veszem, hogy szakdolgozatomat a Szegedi Tudományegyetem könyvtárában a kölcsönözhető könyvek között helyezik el, és az interneten is nyilvánosságra hozhatják.

....

Szeged, 2015. május 16.