Racionális együtthatós polinomok Newton-poligonja

1. Definíció. *Legyen $p \in \mathbb{Z}$ egy rögzített prímszám. Egy $0 \neq a \in \mathbb{Q}$ racinális szám p-adikus értékelése alatt az a prímtényezős felbontásában p kitevőjét értjük. Másszóval ha $a = p^\alpha \frac{u}{v}$ ahol $(p, u) = (p, v) = 1$ és $\alpha \in \mathbb{Z}$, akkor a p-adikus értékelése $v_p(a) := \alpha$. (Vegyük észre, hogy minden $0 \neq a \in \mathbb{Q}$ ilyen alakba írható.) Továbbá legyen $v_p(0) := \infty$.*

Például $v_2(15/4) = -2$ és $v_3(15/4) = 1$.

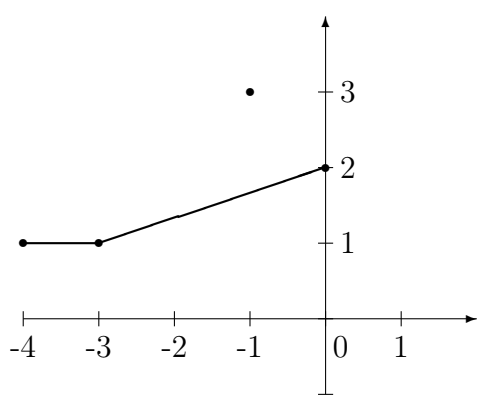
2. Lemma. *$v_p(ab) = v_p(a) + v_p(b)$; $v_p(a + b) \geq \min(v_p(a), v_p(b))$ és egyenlőség van, ha $v_p(a) \neq v_p(b)$.*

Bizonyítás. Ha $a = p^\alpha \frac{u_1}{v_1}$ és $b = p^\beta \frac{u_2}{v_2}$, akkor $ab = p^{\alpha+\beta} \frac{u_1 u_2}{v_1 v_2}$. Továbbá ha $\alpha \leq \beta$, akkor $a + b = p^\alpha \frac{u_1 v_2 + p^{\beta-\alpha} u_2 v_1}{v_1 v_2}$, ahol $p \nmid v_1 v_2$ és $\beta > \alpha$ esetén $p \nmid u_1 v_2 + p^{\beta-\alpha} u_2 v_1$. □

3. Definíció. *Legyen $f(x) = \sum_{i=0}^n a_i x^i \in \mathbb{Z}[x]$ egy egész együtthatós n-edfokú polinom és tegyük fel, hogy $a_n \neq 0 \neq a_0$. Az f polinom (p-hez tartozó) Newton-poligonja a síkon a $\{(-i, v_p(a_i)) \mid i = 0, \ldots, n\} \subset \mathbb{Z}^2 \subset \mathbb{R}^2$ rácspontok alsó konvex burka, mint a $(-n, v_p(a_n))$ és a $(0, v_p(a_0))$ pontokat összekötő töröttvonal. (Azaz a konvex burok alsó határvonala.) Ha valamely i-re $a_i = 0$ és így $v_p(a_i) = \infty$, akkor ezt a pontot figyelmen kívül hagyjuk. A Newton-poligon meredeksége az $S(f) := \{s_n, \ldots, s_1\}$ multihalmaz (egy szám többször is szerepelhet), ahol s_i nem más, mint a töröttvonal meredeksége a függőleges $x = -i$ és $x = -i + 1$ egyenesek között.*

4. Megjegyzés. *A Newton-poligont olyan polinomokra is értelmezhetjük, melyeknek konstans tagja 0. Ekkor ha j a legkisebb index, melyre $a_j \neq 0$, akkor a Newton-poligon töröttvonala csak $(-j, v_p(a_j))$-ig tart, és meredekségeinek multihalmazát kiegészíthetjük j darab ∞-nel. Így az $S(f)$ multihalmaz minden esetben $\deg(f)$ elemű.*

Például ha $p = 2$, akkor a $2x^4 + 2x^3 + 8x + 4$ Newton-poligonja az alábbi töröttvonal:



A meredekség ebben az esetben: $\{0, 1/3, 1/3, 1/3\}$.

5. Állítás. *A Newton-poligon csúcsai rácspontok, meredekségeire teljesül $s_n \leq s_{n-1} \leq \cdots \leq s_1 \in \mathbb{Q}$.*

Bizonyítás. Véges sok pont konvex burkának csúcsai a véges sok pont közül kerülnek ki, a Newton-poligon esetében ezek rácspontok. A meredekségekre vonatkozó egyenlőtlenség a konvexitás következménye. □

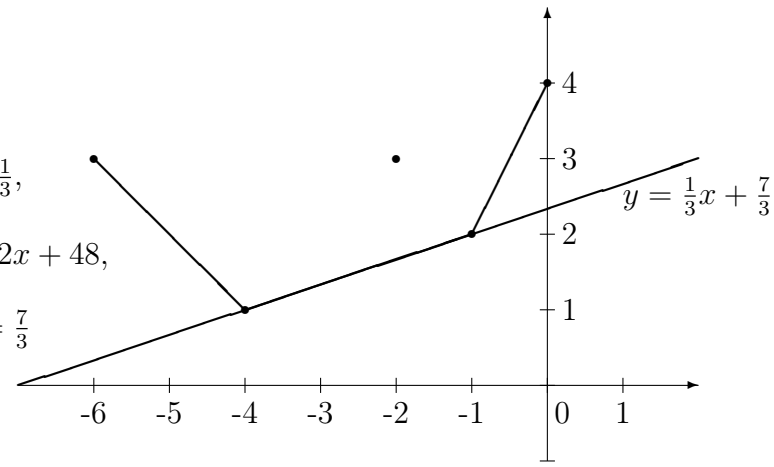
6. Tétel. *Legyenek $f(x), g(x) \in \mathbb{Q}[x]$ polinomok, melyekre $f(0) \neq 0 \neq g(0)$. Ekkor a Newton-poligon meredekségeire teljesül: $S(fg) = S(f) \cup S(g)$ (mint multihalmazok).*

Bizonyítás. Legyen $f(x) = \sum_{i=0}^{n} a_i x^i$ és $g(x) = \sum_{j=0}^{k} b_j x^j$. Elég belátni, hogy fix $s \in \mathbb{Q}$-ra s multiplicitása $S(fg)$-ben megegyezik az $S(f)$-beli és az $S(g)$-beli multiplicitások összegével. Ehhez kiszámoljuk $f(x)$ és s ismeretében s multiplicitását $S(f)$-ben. Vegyük az $y = sx + c$ egyenletű egyenest. Ennek meredeksége épp s. Legyen $c = c_f \in \mathbb{Q}$ az a konstans, melyre az $y = sx + c_f$ egyenes érinti f Newton-poligonját. Másszóval $c_f := \min_{0 \le i \le n}(v_p(a_i) - s(-i))$. Legyen továbbá $M = M_f$ (illetve $m = m_f$) az a maximális (illetve minimális) i index, melyre a c_f-et definiáló minimum felvétetik. Másszóval $M_f := \max(i \mid v_p(a_i) + si = c_f)$, ill. $m_f := \min(i \mid v_p(a_i) + si = c_f)$. Vegyük észre, hogy ekkor s multiplicitása az $S(f)$ multihalmazban nem más, mint $M_f - m_f$.

Az ábrán $p = 2$, $s = \frac{1}{3}$,

$f(x) = 8x^6 + 2x^4 - 8x^2 + 12x + 48$,

$M_f = 4$, $m_f = 1$, $c_f = \frac{7}{3}$



7. Lemma. $c_{fg} = c_f + c_g$, $M_{fg} = M_f + M_g$, $m_{fg} = m_f + m_g$.

Bizonyítás. A polinomok szorzásának definíciójából $fg(x) = \sum_{r=0}^{n+k} \left(\sum_{i=0}^{r} a_i b_{r-i}\right) x^r$. A 2-es Lemma miatt

$$v_p\Big(\sum_{i=0}^{r} a_i b_{r-i}\Big) + rs \overset{(1)}{\ge} \min_{0 \le i \le r} (v_p(a_i) + v_p(b_{r-i})) + rs =$$

$$= \min_{0 \le i \le r} (v_p(a_i) + si + v_p(b_{r-i}) + s(r-i)) \overset{(2)}{\ge}$$

$$\ge \min_{0 \le i \le n} (v_p(a_i) + si) + \min_{0 \le j \le k} (v_p(b_j) + sj) = c_f + c_g \ .$$

A fenti egyenlet bal oldalán minimumot véve (r fut 0-tól $n+k$-ig) azt kapjuk, hogy $c_{fg} \ge c_f + c_g$. Továbbá vegyük észre, hogy $i > M_f$ vagy $i < m_f$ esetén $v_p(a_i) + si > c_f$. Hasonlóképp ha $r - i > M_g$ vagy ha $r - i < m_g$, akkor $v_p(b_{r-i}) + s(r-i) > c_g$. Tehát ha $r > M_f + M_g$ vagy ha $r < m_f + m_g$, akkor (2)-esnél mindenképp szigorú egyenlőtlenség van. Viszont ha $r = M_f + M_g$ (vagy ha $r = m_f + m_g$), akkor $i = M_f$, $j = r - i = M_g$-nél a (2)-es mindkét oldalán felvétetik a minimum, és ezek egyenlők. Sőt, ez esetben a 2-es Lemma utolsó állítása szerint (1)-esnél is egyenlőség áll fenn, hiszen ekkor a $\sum_{i=0}^{r} a_i b_{r-i}$ összegben az összeadandók között v_p minimuma csak egyetlen helyen vétetik fel (mégpedig $i = M_f$-re). □

A tétel nyilvánvalóan következik a fenti lemmából. □

8. Megjegyzés. *A fenti tétel bizonyítására úgy is gondolhatunk, hogy adott $s \in \mathbb{Q}$ esetén az x változó p-adikus értékelését $v_p(x) := s$-nek definiáljuk, így minden $f(x) \in \mathbb{Q}[x]$ polinomnak is értelmezhetjük a p-adikus értékelését a $v_p(a_n x^n + \cdots + a_0) := \min_k(v_p(a_k x^k)) = \min_k(v_p(a_k) + ks)$ formulával. Továbbá ha a p-adikus abszolútértéket $|\alpha|_p := p^{-v_p(\alpha)}$ képlettel definiáljuk, akkor így (minden $s \in \mathbb{Q}$ számra) bevezethetjük az $f(x)$ polinom p-adikus s-edrendű* Gauss-normáját, *mégpedig $\|f(x)\|_{p,s} := p^{-v_p(f(x))}$ (itt most jelöltük az s-től való függést is, de valójában már $v_p(f(x))$ is függ s-től). Ezen a „nyelven" a bizonyításban azt látjuk be, hogy a $\|\cdot\|_{p,s}$ norma multiplikatív, azaz $\|f(x)g(x)\|_{p,s} = \|f(x)\|_{p,s}\|g(x)\|_{p,s}$. A Gauss-normák*

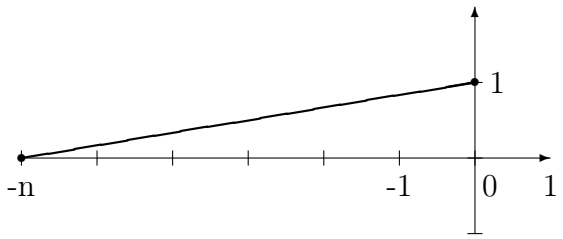
(és a Newton-poligon) fontos szerepet játszanak a p-adikus analízisben. Könnyű meggondolni, hogy ez valóban egy norma lesz, hiszen a háromszögegyenlőtlenség (sőt, az ultrametrikus egyenlőtlenség, miszerint $\|a+b\| \leq \max(\|a\|, \|b\|)$*) is teljesül a 2-es Lemma miatt.*

9. Következmény. *Ha* $f(x) \in \mathbb{Q}[x]$*,* p *prím, és* f *p-hez tartozó Newton-poligonja egy darab szakasz, melyen a két végén kívül nincs más rácspont, akkor* f *irreducibilis.*

Bizonyítás. Ez esetben f Newton-poligonját nem lehet két rácstöröttvonal valódi uniójára bontani. □

10. Következmény (Schönemann-Eisenstein)**.** *Ha* $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$ *polinomra* $p \nmid a_n$*,* $p \mid a_i$ *(*$0 \leq i < n$*) és* $p^2 \nmid a_0$*, akkor* f *irreducibilis* $\mathbb{Q}$ *fölött.*

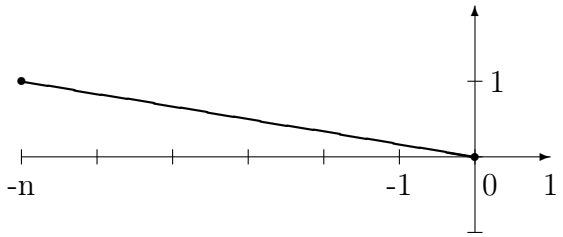
Bizonyítás. Ez esetben a Newton-poligon nem más, mint a $(-n, 0)$ és a $(0, 1)$ pontokat összekötő



szakasz, melynek belsejében nincs rácspont. □

11. Következmény (Schönemann-Eisenstein tükörképe)**.** *Ha* $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$ *polinomra* $p \nmid a_0$*,* $p \mid a_i$ *(*$0 < i \leq n$*) és* $p^2 \nmid a_n$*, akkor* f *irreducibilis* $\mathbb{Q}$ *fölött.*

Bizonyítás. Hasonlóan a hagyományos Schönemann-Eisenstein kritériumhoz, a Newton-poligon most a $(-n, 1)$ és a $(0, 0)$ pontokat összekötő



szakasz, melynek belsejében szintén nincs rácspont. □

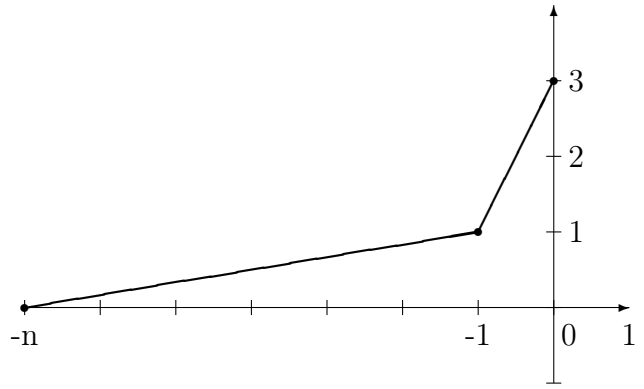
12. Megjegyzés. *Vegyük észre, hogy elsőfokú polinom Newton-poligonjának meredeksége nem más, mint a(z egyetlen) gyökének p-adikus értékelése. Tehát a 6. Tétel szerint joggal várhatnánk, hogy egy tetszőleges* f *polinom gyökeinek p-adikus értékeléseinek multihalmaza* $S(f)$ *legyen. Ez tényleg így is van, de ahhoz, hogy ennek az állításnak értelmet adjunk, több elméletre lenne szükségünk, ami túlmutat az elsőéves előadás anyagán. Azt kellene értelmeznünk például, hogy mit jelent az, hogy p-nek épp a* $3/4$*-ik hatványa oszt egy komplex számot (vagy csak egy olyan komplex számot, mely gyöke egy racionális együtthatós polinomnak – az ilyen számokat* algebrai *számoknak hívják).*

13. Következmény (Racionális gyökteszt)**.** *Ha a* $0 \neq r/s$ *(*$(r, s) = 1$*) racionális szám gyöke az* $f(x) = a_n x^n + \cdots + a_0$ *polinomnak, ahol* $a_n \neq 0 \neq a_0$*, akkor* $r \mid a_0$ *és* $s \mid a_n$*.*

Bizonyítás. Azt kell belátnunk, hogy tetszőleges p prímre $v_p(a_n) \geq v_p(s)$ és $v_p(a_0) \geq v_p(r)$. Vegyük észre, hogy ha r/s gyöke f-nek, akkor f Newton-poligonjában van $v_p(r/s)$ meredekségű szakasz. Mivel f egész együtthatós, ezért $v_p(a_i) \geq 0$ minden $i = 0, 1, \ldots, n$-re, tehát ha $v_p(r/s) > 0$, akkor a Newton-poligon jobboldali végpontja, azaz a $(0, v_p(a_0))$ rácspont y koordinátája legalább $v_p(r/s)$, hiszen egy $v_p(r/s)$ meredekségű, felső félsíkban levő rácsszakasz jobb oldali végpontja legalább ilyen magasan van. Hasonlóképp ha $v_p(r/s) < 0$, akkor $v_p(a_n) \geq -v_p(r/s) = v_p(s)$. □

14. Megjegyzés. *Ahogy a fenti megjegyzésben is láttuk, a Newton-poligon segítségével a racionális gyöktesztnél jóval erősebb állítás jön ki, ami segít a racionális gyökök megtalálásában. Ugyanis ha van egy r/s gyöke az $f(x)$ polinomnak és p egy tetszőleges prím, akkor f-nek a p prím szerinti Newton-poligonjában kell lennie $v_p(r/s)$-meredekségű – speciálisan egész meredekségű! – szakasznak.*

Például ahhoz, hogy belássuk, hogy az $x^n + 3x + 27$ polinomnak nincs egész gyöke ($n > 3$), elegendő megvizsgálni, hogy a ± 9 gyöke-e, hiszen a 3-hoz tartozó Newton-poligon egyetlen egész meredeksége a 2, azaz $v_3(r/s) = 2$ minden r/s racionális gyökre, hiszen a fenti polinom Newton-poligonja:



15. Következmény (Gauß-lemma)**.** *Primitív polinomok szorzata primitív.*

Bizonyítás. Itt elég belátni, hogy ha egy adott p prímszám nem osztja se f se g együtthatóinak legnagyobb közös osztóját, akkor p nem osztja fg együtthatóinak legnagyobb közös osztóját sem. Másként fogalmazva ez azt jelenti, hogy ha f-nek és g-nek is van p-vel nem osztható együtthatója, akkor fg-nek is van. A feltétel azt jelenti, hogy $s = 0$-ra $c_f = c_g = 0$. Ekkor viszont $c_{fg} = c_f + c_g = 0$, azaz fg-nek is van p-vel nem osztható együtthatója. $\square$

Joggal merül fel a kérdés, hogy Newtont miért érdekelték az irreducibilis racionális polinomok. A válasz az, hogy *nem érdekelték*, a Newton-poligonokat teljesen más (de mint látjuk mindjárt meglehetősen hasonló) kontextusban találta ki. Vegyünk egy $f(x, y)$ kétváltozós polinomot (kényelmi szempontból leginkább $\mathbb{C}$ felett), és próbáljuk meg az $f(x, y) = 0$ egyenletet y-ban megoldani (x függvényeként). Tehát az $f(x, y) = 0$ egyenletre tekinthetünk úgy, mint y-beli polinomegyenletre, melynek együtthatói $\mathbb{C}[x]$-beli polinomok. Ha $g(x) \in \mathbb{C}[x]$, akkor legyen g x-adikus értékelése az a legnagyobb kitevő, ahányadik hatványa x-nek osztja g-t. Másszóval $v_x(g(x))$ nem más, mint g-ben az $x = 0$ gyök multiplicitása. Készítsük el (v_p helyett v_x-szel) az $f(x, y)$ Newton-poligonját. A fenti megjegyzés szerint azt várjuk, hogy az $y_j(x)$ ($j = 1, \ldots, \deg_y(f(x, y))$) megoldások (mint függvények) x-adikus értékeléseinek multihalmaza nem más, mint a meredekségek $S(f)$ multihalmaza. Ha most $y_j(x)$-et megpróbáljuk x szerint hatványsorba fejteni, azt kapjuk, hogy az első tagnak cx^{s_j}-nek kellene lennie (alkalmas $0 \neq c \in \mathbb{C}$-vel), hiszen x-nek épp az s_j-edik hatványa fogja osztani $y_j(x)$-et. Viszont s_j nem feltétlenül egész, csak annyit tudunk róla, hogy racionális (a Newton-poligon csúcsai továbbra is rácspontok). Tehát abban reménykedhetünk csak, hogy x racionális kitevőjű hatványai fognak szerepelni a kapott hatványsorban. Ezt mindig meg is lehet tenni: minden j-re $y_j(x)$ előáll x racionális kitevős hatványainak végtelen lineáris kombinációjaként, sőt, ezekben a racionális kitevőkben a nevezők korlátos halmazt alkotnak (azaz van "közös" nevező). Tehát $y_j(x) \in \mathbb{C}((x^{1/n}))$ egy formális Laurent-sor $x^{1/n}$-ben, ahol n a kitevők közös nevezője. Sőt, ezt akkor is meg lehet tenni, ha $f(x, y)$-ban y hatványainak együtthatói nem feltétlen polinomok, hanem csak $\mathbb{C}((x))$-beliek. Speciálisan igaz az alábbi tétel, amit nem bizonyítunk:

16. Tétel (Puiseux)**.** *A $\bigcup_{n=1}^{\infty} \mathbb{C}((x^{1/n}))$ test algebrailag zárt.*