

EÖTVÖS LORÁND TUDOMÁNYEGYETEM
TERMÉSZETTUDOMÁNYI KAR

Mogyorósi Bálint

**NEM FELTÉTLENÜL NORMÁLT POLINOMOK
HELYETTESÍTÉSI ÉRTÉKEINEK LEGNAGYOBB
KÖZÖS OSZTÓJA**

TDK dolgozat
Matematikus Msc

Témavezető:

dr. Zábrádi Gergely

Algebra és Számelmélet Tanszék



Budapest, 2022

Tartalomjegyzék

1. Bevezetés	3
2. Jelölések	4
3. Saját eredmények	5

1. fejezet

Bevezetés

Frenkel és Zábrádi becsléseket adtak egész együtthatós normált polinomok helyettesítési értékeinek legnagyobb közös osztóira a rezultáns segítségével. Ezt általánosítjuk arra az esetre, amikor a polinomok főegyütthatója nem feltétlenül 1.

2. fejezet

Jelölések

Rögzítsünk le egy p prímet, ekkor legyen az $a \rightarrow$ függvény ami egy $a \in$ hozzárendeli a pímtényezőös felbontásában, rögzített p prímünk kitevőjét.

$f, g \in [x]$:

$$f(x) = c_\gamma \prod_{j=1}^k (x - \gamma_j)$$

$$g(x) = c_\delta \prod_{i=1}^m (x - \delta_i)$$

$$R = c_\gamma^m \cdot c_\delta^k \cdot \prod_{i,j} (\delta_i - \gamma_j)$$

$$D = v(c_\delta)$$

$$G = v(c_\gamma)$$

3. fejezet

Saját eredmények

3.0.1. Lemma. $m \in, I \subseteq \{1, 2, \dots, k\}$ indexhalmaz, és $\forall i \in I$ teljesül, hogy $v(m - \gamma_i) \notin$.
 Legyen $0 \leq t_I < p$ azon $i \in \{1, 2, \dots, k\} \setminus I$ száma amikre teljesül, hogy $v(m - \gamma_i) > 0$.
 Ekkor létezik egy $n \in$, hogy $n \equiv m \pmod{p}$ és

$$v(f(n)) \leq v(c_\gamma) + \sum_{i \in I} v(m - \gamma_i) + t_I$$

.

Bizonyítás.

$$I^+ = \{i \in \{1, 2, \dots, k\} \setminus I \mid v(n - \gamma_i) > 0\}$$

$$I^- = \{i \in \{1, 2, \dots, k\} \setminus I \mid v(n - \gamma_i) \leq 0\}$$

$$v(f(n)) = v(c_\gamma) + \sum_{i=1}^k v(x - \gamma_i) =$$

$$= v(c_\gamma) + \sum_{i \in I} v(n - \gamma_i) + \sum_{i \in I^+} v(n - \gamma_i) + \sum_{i \in I^-} v(n - \gamma_i)$$

I^- -hoz tartozó tagjainkat elhagyjuk ugyanis ezek negatívak, szeretnénk választani úgy egy $n \in$ hogy ezzel felültudjuk becsülni I^+ -hoz tartozó tagokat. Teljesülni kell, hogy $n \equiv m \pmod{p}$ és ezután úgy választjuk meg n -et $\pmod{p^2}$, hogy $v(n - \gamma_i) \leq 1$ teljesüljön $i \in I^+$ -ra.

$\forall n \in \mathbb{Z}, i \in I$:

$$v(n - \gamma_i) = v((n - m) + (m - \gamma_i)) = \min((n - m), (m - \gamma_i)) \leq v(m - \gamma_i)$$

Az így választott n -nel:

$$\begin{aligned}
v(f(n)) &= v(c_\gamma) + \sum_{i=1}^k v(x - \gamma_i) = \\
&= v(c_\gamma) + \sum_{i \in I} v(x - \gamma_i) + \sum_{i \in I^+} v(x - \gamma_i) + \sum_{i \in I^-} v(x - \gamma_i) \leq \\
&\leq v(c_\gamma) + \sum_{i \in I} v(x - \gamma_i) + \sum_{i \in I^+} 1 \leq v(c_\gamma) + \sum_{i \in I} v(m - \gamma_i) + t_I
\end{aligned}$$

□

3.0.2. Tétel. *Ha $l = 0$ teljesül a lentebbi egyenlőtlenség:*

$$v(c_\gamma)m + v(c_\delta)k + \sum_{i,j:\gamma_j \equiv l \equiv \delta_i} v(\delta_i - \gamma_j) \geq G \cdot m + s(s-1-D) + S$$

Egyébként:

$$v(c_\gamma)m + v(c_\delta)k + \sum_{i,j:\gamma_j \equiv l \equiv \delta_i} v(\delta_i - \gamma_j) \geq G \cdot m + s(s-D)$$

Bizonyítás.

$$\begin{aligned}
a_j &= v(l - \gamma_j), \quad b_i = v(l - \delta_i) \\
v(\delta_i - \gamma_j) &\geq \min(a_j, b_i) \\
D &= v(c_\delta), \quad G = v(c_\gamma)
\end{aligned}$$

Legyen $c_i = D$ ha $i = 1$ és 0 értéket vesz fel egyébként.

$$v(c_\gamma)m + v(c_\delta)k + \sum_{i,j:\gamma_j \equiv l \equiv \delta_i} v(\delta_i - \gamma_j) \geq g \cdot m + \sum_{j=1}^k \sum_{i=1}^m (\min(a_j, b_i) + c_i)$$

$$I_j = \{i \in \{1, 2, \dots, k \mid a_i < \min(1, b_j), a_i \notin \}\}$$

Alkalmazzuk az előző lemmát $I = I_j$ -re:

$$s \leq \sum_{j \in I_j} a_j + t_j + v(c_\gamma)$$

$j \notin I_j, a_j \geq \min(1, b_i)$:

$$\sum_{j=1}^k (\min(a_i, b_j) + c_i) \geq D + \sum_{j \in I} a_j + t_I \cdot \min(1, b_i) \geq$$

$$\geq (D + \sum_{j \in I} a_j + t_I) \cdot \min(1, b_i) \geq s \cdot \min(1, b_i)$$

Megint alkalmazzuk az első lemmát $I = \{i \in 1, 2, \dots, n \mid 0 < b_i < 1\}$

$$s \leq \sum_{i \in I} b_i + t_I + D \leq \sum_{j=1}^k \min(1, b_j) + D$$

Feltesszük hogy $S, n = 0$ esetén vevődik fel és b_k a legnagyobb gyökünk, ha nem akkor átindexeljük úgy hogy b_k legyen a legnagyobb ezt megtehetjük hisz a polinomjaink gyűrűje kommutatív:

$$\sum_{i=1}^m (\min(a_i, b_k) + c_i) = \sum_{i=1}^m a_i + D = v(f(0)) \geq S$$

Valamint

$$\begin{aligned} 1 + \sum_{j=1}^{k-1} \min(1, b_j) &\geq \sum_{j=1}^k \min(1, b_j) \geq s - D \\ G \cdot m + D \cdot k + \sum_{i,j} v(\delta_i - \gamma_j) &\geq \sum_{j=1}^k \sum_{i=1}^m (\min(a_i, b_j) + c_i) + G \cdot m \\ &\geq G \cdot m + \sum_{j=1}^{k-1} s \cdot \min(1, b_j) + \sum_{i=1}^m (\min(a_i, b_j) + c_i) \geq \\ &\geq G \cdot m + s \cdot \left(\sum_{j=1}^{k-1} \min(1, b_j) \right) + S \geq G \cdot m + s(s - 1 - D) + S \end{aligned}$$

□

3.0.3. Tétel. Legyen $s \leq p$ és p^s osztja g -t és f -et minden n -re.

$$S = \max_{n \in v} (\gcd(f(n), g(n)))$$

Ekkor:

$$v(R) \geq -D \cdot p \cdot s + G \cdot m \cdot p + p \cdot s^2 - s + S$$

Bizonyítás.

Adjuk össze az előző tétel becsléseit:

$$V(R) \geq (p-1) \cdot (G \cdot m + s(s-D)) + G \cdot m + s(s-1-D) + S = -D \cdot p \cdot s + G \cdot m \cdot p + p \cdot s^2 - s + S$$

□

3.0.4. Állítás. *A következő konstrukcióra a becslésünk egyenlőséggel telejsül, így éles.*

$$s = s' + D, S = S' + D$$

$$f(x) = G \cdot x(x - 2p)^{s-1} \prod_{j=1}^{\frac{p-1}{2}} (x - j)^{2s} \cdot (x - p^{G \cdot m} - \frac{p+1}{2})$$

$$g(x) = D \cdot (x - p^{S'-s'+1-D})(x - p)^{s'-1-D} \prod_{j=1}^{\frac{p-1}{2}} (x - j - p)^{s'-D} (x - \frac{p+1}{2})^{p-1}$$

Bizonyítás.

Tegyük fel hogy minden kitevő nem negatív.

$$\begin{aligned} v(r) &= v(c_\gamma^{deg(g)} \prod_{x:f(x)=0} g(x)) = \\ &= mG + v(g(0)g(2p)^{s-1} \prod_{j=1}^{\frac{p-1}{2}} g(j)^{2s} g(p^{G \cdot m} + \frac{p+1}{2})^{p-1}) = \\ &= m \cdot G + (S' + D - D) + (s - 1)(s' + D - D) + 2s \cdot \frac{p-1}{2}(s' + D - D) + (p-1) \cdot (G \cdot m) \\ &= m \cdot G + S - D + (s - 1)(s - D) + s(p-1)(s - D) + (p-1)(G \cdot m - D \cdot s) = \\ &= G \cdot m + S - D + s^2 + D - s - sD + Ds - Dps - s^2 + ps^2 + (p-1)G \cdot m = \\ &= pG \cdot m + S - s - Dps + ps^2 \end{aligned}$$

□

Felhasznált irodalom

- [1] Frenkel P. E., Pelikán J., On the Greatest Common Divisor of the Value of Two Polynomials, *The American Mathematical Monthly* 124(5) (May 2017), 446–450.
- [2] D. Gomez, J. Gutierrez, Á. Ibeas, D. Sevilla, Common factors of resultants modulo p , *Bull. Aust. Math. Soc.* 79 (2009), 299–302.
- [3] S. Janson, Resultant and discriminant of polynomials, <https://www.semanticscholar.org>, 2010
- [4] Keller G., Olson F. R., Counting polynomial functions (mod pn), *Duke Math. J.* 35 (1968), 835–838.
- [5] Kempner A. J., Polynomials and their residue systems, *Amer. Math. Soc. Trans.* 22 (1921), 240–288.
- [6] D. I. Khomovsky, On the relationship between the number of solutions of congruence systems and the resultant of two polynomials, *INTEGERS – Electronic Journal of Combinatorial Number Theory* 16, A41
- [7] Péter E. Frenkel and Gergely Zábrádi, Estimating the greatest common divisor of the value of two polynomials, *International Journal of Number Theory* 14(9) (2018), 2543–2554