Magasabb hatvány Diofantikus halmazok

Batta Gergő Péter

Debreceni Egyetem

Számelmélet szeminárium
2023. május 5.

Definíció és példák

Diofantikus halmaz

Legyen $k \geq 2$ rögzített egész szám. Páronként különböző nem nulla racionális számok egy $\{a_1, a_2, ..., a_n\}$ halmazát k -adik hatvány racionális Diofantikus n-esnek mondjuk, ha bármely $1 \leq i < j \leq n$ esetén

$$a_i a_j + 1 = r_{ij}^k$$

valamely r_{ij} racionális számok mellett.

Példák

- Egész: $(2, \{1, 3, 8\}); (3, \{2, 171, 25326\})$
- Racionális: $(2, \{2, -1/2, 3/2\}); (3, \{2, -1/2, -14\})$

Eddigi eredmények $k = 2$ esetben

Egész értékű

- Fermat (XVII. század):
  példa négyesre
- Euler (XVIII. század):
  négyesek paraméteres családja
- Dujella (2004):
  nem létezik hatos és legfeljebb véges sok ötös létezik
- He, Togbe, Ziegler (2019):
  nem létezik Diofantikus ötös

Racionális értékű

- Diofantosz (III. század):
  példa négyesre
- Euler (XVIII. század):
  példa ötösre
- Gibbs (1999):
  példa hatosra
- Dujella, Mikic, Kazalicki, Szikszai (2017):
  végtelen sok Diofantikus hatos létezik

Eddigi eredmények $k \geq 3$ esetben

Egész értékű

- Bugeaud, Dujella (2003): abszolút felső korlátot adtak k függvényében a halmazok méretére, elszórt példák hármasokra
  $(3; \{2, 171, 26326\})$
  $(4, \{1352, 9539880, 9768370\})$

Racionális értékű

- Ismert példák hármasokra

Párok által indukált görbe

Legyen $\{a, b\}$ k-adik hatvány Diofantikus pár. Ekkor bármely $y \neq 0$ bővítésre teljesül, hogy

$$ay + 1 = x_1^k \qquad\qquad by + 1 = x_2^k.$$

Definiáljuk a

$$C_{a,b} : (ay + 1)(by + 1) = x^k$$

affin algebrai görbét, melyet az $\{a, b\}$ pár által indukált görbének fogunk nevezni. Ekkor a görbén a következő nyilvánvaló pontok szerepelnek

$$P = (1, 0), \qquad A = \left(0, -\frac{1}{a}\right), \qquad B = \left(0, -\frac{1}{b}\right).$$

Görbe transzformáció páratlan k esetén

Az

$$X = abx \text{ , és az } Y = (ab)^{(k+1)/2}y + \frac{(ab)^{(k-1)/2}(a+b)}{2}$$

biracionális változótranszformációk az alábbi, aritmetikailag kedvezőbb alakra vezetnek

$$C'_{a,b}: \ Y^2 = X^k + \left(\frac{(ab)^{(k-1)/2}(a-b)}{2}\right)^2.$$

Ekkor a P, A, B pontok transzformáltjai rendre:

$$P' = \left(ab, \frac{(ab)^{(k-1)/2}(a+b)}{2}\right),$$

$$A' = \left(0, \frac{(ab)^{(k-1)/2}(a-b)}{2}\right), \qquad B' = \left(0, -\frac{(ab)^{(k-1)/2}(a-b)}{2}\right).$$

Görbe transzformáció páros k esetén

A

$$X = abx \text{ , és az } Y = (ab)^{k/2+1}y + \frac{(ab)^{k/2}(a+b)}{2}$$

biracionális változótranszformációk az alábbi, aritmetikailag kedvezőbb alakra vezetnek

$$C'_{a,b}: \ Y^2 = abX^k + \left(\frac{(ab)^{k/2}(a-b)}{2}\right)^2.$$

Ekkor a P, A, B pontok transzformáltjai rendre:

$$P' = \left(ab, \frac{(ab)^{k/2}(a+b)}{2}\right),$$

$$A' = \left(0, \frac{(ab)^{k/2}(a-b)}{2}\right), \qquad B' = \left(0, -\frac{(ab)^{k/2}(a-b)}{2}\right).$$

Görbe alapvető tulajdonsága

Állítás

A $C_{a,b}$ görbe nem szinguláris.

Legyen $F(x,y) = (ay+1)(by+1) - x^k$. A szinguláris pontokat $C_{a,b}$-n az alábbi egyenletrendszer határozza meg:

$$\begin{cases} F(x,y) = 0 \\ \frac{\partial}{\partial x} F(x,y) = 0 \\ \frac{\partial}{\partial y} F(x,y) = 0 \end{cases}$$

Indirekt tegyük fel, hogy van megoldása az egyenletnek. Ekkor a második egyenletből $kx^{k-1} = 0$, így $x = 0$ adódik. Ekkor

$$F(0,y) = (ay+1)(by+1) = 0,$$

ebből következik, hogy $y = -1/a$ vagy $y = -1/b$. Ezt a harmadik egyenletbe helyettesítve kapjuk, hogy $a\left(-\frac{b}{a}+1\right) = 0$, melyből $a = b$ adódna.

Görbe alapvető tulajdonsága

Génusz szerint osztályozva, megállapítható, hogy:

- $k = 2$ esetben Pell-kúpszelet,

$$C'_{a,b}: \ Y^2 = abX2 + \left(\frac{(ab)(a-b)}{2}\right)^2 \ \rightarrow \ C''_{a,b}: X^2 - abY^2 = 4,$$

- $k = 3$ esetben elliptikus görbe,

$$C'_{a,b}: Y^2 = X^3 + \left(\frac{ab(a-b)}{2}\right)^2$$

- $k = 4$ esetben elliptikus görbe,

$$C'_{a,b}: \ Y^2 = abX^4 + \left(\frac{(ab)^2(a-b)}{2}\right)^2 \rightarrow C''_{a,b}: Y^2 = X^3 - 2(ab)^3(a-b)$$

- $k \geq 5$ esetben hiperelliptikus görbe.

$k = 3$ eset

Ebben az esetben a görbénk az alábbi

$$C'_{a,b}: \ Y^2 = X^3 + \left(\frac{(ab)(a-b)}{2}\right)^2$$

Weierstrass alakot ölti, amelyet a következő biracionális transzformációkkal értünk el

$$X = abx, \qquad Y = (ab)^2 y + \frac{(ab)(a+b)}{2}.$$

Ekkor a triviális pontok a transzformált görbén a következőek:

$$P' = \left(ab, \frac{(ab)(a+b)}{2}\right),$$

$$A' = \left(0, \frac{(ab)(a-b)}{2}\right), \qquad B' = \left(0, -\frac{(ab)(a-b)}{2}\right).$$

$C_{a,b}$ tulajdonságai

Lemma 1 (Fueter - 1930)

Legyen

$$E: \ y^2 = x^3 + B$$

elliptikus görbe, $B \in \mathbb{Z}$ és $B = B_0^6 B_1$, ahol B_1 hatodik hatvány mentes. A T torziós részcsoportja $E(\mathbb{Q})$-nak ekkor a következő:

$$T = \begin{cases} \mathbb{Z}/6\mathbb{Z} & \text{ha } \ B_1 = 1 \\ \mathbb{Z}/3\mathbb{Z} & \text{ha } \ B_1 = -432 \text{ vagy } B_1 \neq 1 \text{ négyzetszám} \\ \mathbb{Z}/2\mathbb{Z} & \text{ha } \ B_1 \neq 1 \text{ köbszám} \\ \{\mathcal{O}\} & \text{egyébként} \end{cases}$$

Következmény

$C'_{a,b}(\mathbb{Q})$ torziós részcsoportja $\mathbb{Z}/6\mathbb{Z}$ vagy $\mathbb{Z}/3\mathbb{Z}$.

$C_{a,b}$ tulajdonságai

Lemma 2 (B., Szikszai)

Legyen $\{a, b\}$ harmadik hatvány Diofantikus pár. Ekkor a $P = (1, 0)$ rendje végtelen a $C_{a,b}(\mathbb{Q})$ csoportban kivéve, ha $a = -b, 2b$, vagy $\frac{b}{2}$.

Alkalmazva a $Lemma1$ következményét elegendő csupán a $3P$-t és a $6P$-t vizsgálni. Mindkét esetben a számlálót 0-vá téve a feladat egy reciprok polinom racionális gyökeinek a keresésére redukálódik ahol a változónk $\frac{a}{b}$. Például $3P$ esetén

$$a^6 - 3a^5b + 6a^4b^2 - 7a^3b^3 + 6a^2b^4 - 3ab^5 + b^6 = 0$$

Ekkor a kapott egyenletek racionális megoldási az $\frac{1}{2}, -1$ és 2.

Kimaradó esetek

Lemma 3 (B., Szikszai)

Az $\{-1, 1\}$ és $\{-3, 3\}$ az összes lehetséges harmadik hatvány racionális Diofantikus pár, ahol $a = -b$. Továbbá nem létezik olyan harmadik hatvány Diofantikus pár, ahol $a = 2b$ vagy $\frac{b}{2}$.

Tegyük fel, hogy $\{a, b\}$ harmadik hatvány Diofantikus pár, ahol $a = 2b$ vagy $\frac{b}{2}$. A szimmetria miatt, az általánosság sérelme nélkül feltehető, hogy $a = 2b$. Ekkor az $E_{b,2b}$ 0 rangú görbe, azaz elegendő a torziópontokat vizsgálni, melyeket a Lutz-Nagell tétel segítségével könnyen meghatározhatunk. Ezek alapján nem létezik a feltételeket kielégítő $\{a, b\}$ pár.

Az $E_{-b,b}$ görbe szintén 0 rangú, így hasonló eljárást alkalmazhatunk, de ebben az esetben vannak megfelelő tórziópontokból származó párok, a $\{-1, 1\}$ és a $\{-3, 3\}$.

3-leszállás

Definíció: 3-leszállás

Definiáljuk az $\alpha : C_{a,b}(\mathbb{Q}) \to \mathbb{Q}^*/\mathbb{Q}^{*3}$ leképezést a következőképpen:

$$\alpha(R) = \begin{cases} 1 & \text{ha } R = \mathcal{O} \\ (ab)^2(a-b)^2 & \text{ha } R = A \\ y - \frac{ab(a-b)}{2} & \text{ha } R = (x,y) \neq A \end{cases}$$

Megjegyezzük, hogy hasonlóan B-vel is definiálható a 3-leszállás.

Lemma (Cohen - 2007)

Az α leképezés csoport homomorfizmus, és $3C'_{a,b}(\mathbb{Q}) \subset ker\alpha$.

Tétel

Tétel (B., Szikszai)

Legyen $\{a, b\}$ harmadik hatvány racionális Diofantikus pár. Ha $P \neq T \in C_{a,b}(\mathbb{Q})$ úgy, hogy $T - P \in 3C_{a,b}(\mathbb{Q})$, akkor $c = y(T)$ kiterjeszti az $\{a, b\}$ párt harmadik hatvány racionális Diofantikus hármassá.

Bizonyítás

Ha $\alpha(T') = \alpha(P')$, akkor definíció szerint

$$\alpha(P') = y(P') - \frac{ab(a-b)}{2} = \frac{ab(a+b)}{2} - \frac{ab(a-b)}{2} = ab^2.$$

Legyen r racionális szám, ekkor teljesül, hogy

$$y(T') = 2ab^2r^3 + \frac{ab(a-b)}{2}.$$

Alkalmazva az inverz biracionális transzformációt kapjuk, hogy

$$y(T) = \frac{ab^2r^3 + \frac{ab(a-b)}{2} - \frac{ab(a+b)}{2}}{a^2b^2} = \frac{r^3-1}{a}$$

melyből adódik az állítás.

Bővítés hármasokká

Az előző tétel következménye, hogy végtelen sok harmadik hatvány Diofantikus hármas létezik. Precízebben:

Következmény (B., Szikszai)

Legyen $\{a, b\}$ harmadik hatvány Diofantikus pár, ekkor az $y((3m+1)P)$ bővítése a párnak feltéve, hogy $a \notin \left\{-b, 2b, \frac{b}{2}\right\}$, ahol $m \in \mathbb{Z} \setminus \{0\}$.

Példaként bővítsünk a $y(-2P)$-vel, ekkor

$$\left\{a,\ b,\ -9\frac{(a^2-ab+b^2)}{(a^3+3a^2b+3ab^2+b^3)}\right\}$$

harmadik hatvány Diofantikus hármas.

A feltételekről

Vegyük észre, hogy $T-P \in 3C_{a,b}(\mathbb{Q})$ elégséges, de nem szükséges feltétel. Tekintsük például a

$$\{2, 171, 25326\}$$

hármast. Ekkor az $S = (6031, 25326) \in C_{2,171}(\mathbb{Q})$ úgy, hogy $S - P \notin 3C_{2,171}(\mathbb{Q})$.

Következtetésképpen P-nek más többszöröse is bővítés lehet.

Lemma 4 (B., Szikszai)

Legyen $r = t^3, t \in \mathbb{Q}, t \neq 0, \pm 1, \{a, b\} = \left\{r, -\frac{1}{r}\right\}$ és $T \in E_{a,b}$. Ekkor $\{y(T), y(-T))\}$ harmadik hatvány Diofantikus pár.

Bizonyítás

Tekintsük az

$$E'_{a,b}:\ y^2 = x^3 + \left(\frac{t^3 + \frac{1}{t^3}}{2}\right)^2$$

görbét. Legyen $T' \in E'_{a,b}$. Ekkor rendezéssel adódik, hogy

$$-x(T')^3 = -y(T')^2 + \left(\frac{t^3 + \frac{1}{t^3}}{2}\right)^2 = -y(T')^2 + \frac{t^6 + 2 + \frac{1}{t^6}}{4} =$$

$$-y(T')^2 + 1 + \frac{t^6 - 2 + \frac{1}{t^6}}{4} = -y(T')^2 + \left(\frac{t^3 - \frac{1}{t^3}}{2}\right)^2 + 1 =$$

$$\left(y(T') + \frac{t^3 - \frac{1}{t^3}}{2}\right)\left(-y(T') + \frac{t^3 - \frac{1}{t^3}}{2}\right) + 1 = y(T)y(-T) + 1.$$

Bővítés négyesekké

Az $y(2P)$ és az $y(-2P)$ kibővítik az $\{t^3, -1/t^3\}$ párt négyessé.

Tétel (B., Szikszai)

Legyen $r = t^3$ valamely racionális t esetén. Ekkor

$$\{r, -1/r, (r^8 + 5 \cdot r^6 + 15 \cdot r^4 + 5 \cdot r^2 + 1)/(r^7 - 3 \cdot r^5 + 3 \cdot r^3 - r), \\ - 9 \cdot (r^5 + r^3 + r)/(r^6 - 3 \cdot r^4 + 3 \cdot r^2 - 1)\}$$

harmadik hatvány racionális Diofantikus négyes.

Bizonyítás:
Egyszerű számítással igazolható.

Bővítés négyesekké

Lemma 5 (B., Szikszai)

Legyen $r = t^3, t \in \mathbb{Q}, t \neq 0, \pm 1, \{a, b\} = \left\{r, -\frac{1}{r}\right\}$ és $T \in E_{a,b}$. Ha $\{a, b, y(T))\}$ harmadik hatvány Diofantikus pármas, akkor $\{a, b, y(-T))\}$ szintén harmadik hatvány Diofantikus hármas.

Következmény (B., Szikszai)

Legyen $r = t^3, t \in \mathbb{Q}, t \neq 0, \pm 1, \{a, b\} = \left\{r, -\frac{1}{r}\right\}$. Ekkor minden $m \in \mathbb{Z} \setminus \{0\}$ esetén az $\{a, b, y((3m+1)P), y(-(3m+1)P)\}$ harmadik hatvány Diofantikus négyes.

Bővítés négyesekké

Alkalmazva a biracionális transzformációkat adódik, hogy

$$y(-T) = -y(T) + t^3 - \frac{1}{t^3}$$

Ekkor

$$y(-T) - t^3 = -y(T) - \frac{1}{t^3}$$

$$y(-T)t^3 - t^6 = -[y(T)t^3 + 1]$$

$$y(-T)t^3 - t^6 = -r^3$$

$$y(-T)(-\frac{1}{t^3}) + 1 = \frac{r^3}{t^6}.$$

Azaz $\{y(-T), -\frac{1}{t^3}\}$ harmadik hatvány Diofantikus pár. Hasonlóan bizonyítható $\{y(-T), t^3\}$ párra is.

Hivatkozások I

Thomas L. Heath.

Diophantus of Alexandria: A study in the history of Greek algebra.
Dover Publications, Inc., New York, second edition, 1964.
With a supplement containing an account of Fermat's theorems and problems connected with Diophantine analysis and some solutions of Diophantine problems by Euler.

Philip Gibbs.

Some rational Diophantine sextuples.
Glas. Mat. Ser. III, 41(61)(2):195–203, 2006.

Michael Stoll.

Diagonal genus 5 curves, elliptic curves over $\mathbb{Q}(t)$, and rational Diophantine quintuples.
Acta Arith., 190(3):239–261, 2019.

Hivatkozások II

Leonhard Euler.

Elements of algebra.

Springer-Verlag, New York, 1984.

Translated from the German by John Hewlett, Reprint of the 1840 edition, With an introduction by C. Truesdell.

Andrej Dujella, Matija Kazalicki, Miljen Mikić, and Márton Szikszai.

There are infinitely many rational Diophantine sextuples.

Int. Math. Res. Not. IMRN, (2):490–508, 2017.

Hivatkozások III

E. Brassinne.

Précis des œuvres mathématiques de P. Fermat et de l'Arithmétique de Diophante.

Éditions Jacques Gabay, Sceaux, 1989.

Reprint of the 1853 edition.

Yann Bugeaud and Andrej Dujella.

On a problem of Diophantus for higher powers.

Math. Proc. Cambridge Philos. Soc., 135(1):1–10, 2003.

Franz Lemmermeyer.

Higher descent on pell conics iii. the first 2-descent, 2003.

Hivatkozások IV

Rudolf Fueter.

Ueber kubische diophantische gleichungen.

Commentarii mathematici Helvetici, 2:69–90, 1930.

Andrej Dujella.

There are only finitely many Diophantine quintuples.

J. Reine Angew. Math., 566:183–214, 2004.

Bo He, Alain Togbé, and Volker Ziegler.

There is no Diophantine quintuple.

Trans. Amer. Math. Soc., 371(9):6665–6709, 2019.

Andrej Dujell.

Diophantine m-tuples webpage, Accesed 2022.

Hivatkozások V

P. Fermat.

Observations sur diophante, oeuvres de fermat.

P. Tannery, C. Henry, eds., 1:303, 1891.

Andrej Dujella.

Diophantine m-tuples and elliptic curves.

Journal de théorie des nombres de Bordeaux, 13(1):111–124, 2001.

Henri Cohen.

Number theory. Vol. I. Tools and Diophantine equations, volume 239 of *Graduate Texts in Mathematics*.

Springer, New York, 2007.

Hivatkozások VI


Leonhard Euler.
Opuscula analytica i.
1783.

Köszönöm a figyelmet!