

Magasabb hatvány Diofantikus halmazok

TDK dolgozat

Szerző:

Batta Gergő Péter

Debreceni Egyetem, Alkalmazott matematikus MSc, II. évfolyam

Belső konzulens:

Dr. Bérczes Attila Jenő, Debreceni Egyetem, egyetemi tanár

Külső konzulens:

Dr. Szikszai Márton

Debrecen

2022.

Tartalomjegyzék

1. Bevezetés	1
2. k-adik hatvány Diofantikus halmazok	4
2.1. Racionális Diofantikus hármasok	4
2.2. Indukált görbék	7
3. Második hatvány Diofantikus halmazok	11
3.1. Indukált görbe $k = 2$ esetben	11
3.2. Bővítések	13
4. Harmadik hatvány Diofantikus halmazok	15
4.1. Indukált görbe $k = 3$ esetben és a 3-leszállás	15
4.2. Hármasok konstrukciója	15
4.3. Négyesek konstrukciója	18
Hivatkozások	20

1. Bevezetés

1.1. Definíció. Legyen $k \geq 2$ rögzített egész szám. Páronként különböző nem nulla racionális számok egy $\{a_1, a_2, \dots, a_n\}$ 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 választása mellett.

Két természetes probléma fogalmazható meg. Mennyi eleme lehet egy Diofantikus halmaznak, továbbá adott elemszám esetén mi állítható az ilyen tulajdonságú halmazok számosságáról? A kérdések kiterjedt, régre nyúló, ma is aktív szakirodalommal rendelkeznek.

Az $n = 2$ eset triviális. Legyenek $a \neq 0$ és $r^k \neq 1$ racionális számok. Ekkor

$$\left\{ a, \frac{r^k - 1}{a} \right\}$$

egy k -adik hatvány racionális Diofantikus pár. Amennyiben a és r egész számok úgy, hogy a osztója $(r^k - 1)$ -nek, akkor a pár is egész értékű. Az irodalomban klasszikus esetnek éppen a $k = 2$ hatvány és az egész értékű Diofantikus halmazok számítanak, így ezekről ejtünk elsőként szót.

Az

$$\left\{ \frac{1}{16}, \frac{33}{16}, \frac{17}{4}, \frac{105}{16} \right\} \quad \text{és} \quad \{1, 3, 8, 120\}$$

négyeseket Diophantos [13] és Fermat[1] munkáiban találhatjuk. Utóbbi megfeleltethető az Euler [8] által konstruált

$$\{a, b, a + b + 2r, 4r(r + a)(r + b)\}$$

végtelen család egy elemének, az $(a, b) = (1, 3)$ választás mellett, ahol $\{a, b\}$ egy Diofantikus pár, továbbá $r^2 = ab + 1$. Sokáig megoldatlan sejtés volt, miszerint nem létezik

ötelemű Diofantikus halmaz csupa egész számokból. Hosszú időn át a legerősebb eredmény Dujella [6] nevéhez köthető, miszerint legfeljebb véges sok ilyen halmaz létezik és ezekre effektív felső korlát adható. 2019-ben He, Togbe, illetve Ziegler [12] közös kutatásának köszönhetően került végül igazolásra a sejtés.

Továbbra is a $k = 2$ választással tekintjük most az általános racionális esetet. Euler [9] adta az első példát Diofantikus ötösre, a

$$\left\{ 1, 3, 8, 120, \frac{777480}{8288641} \right\}$$

halmaz éppen Fermat négyesének egy bővítése. Stoll [15] igazolta, hogy a fenti racionális tört az egyetlen lehetséges bővítés. Az első példa Diofantikus hatosra a

$$\left\{ \frac{11}{192}, \frac{35}{192}, \frac{155}{27}, \frac{512}{27}, \frac{1235}{48}, \frac{180873}{16} \right\}$$

volt, mely Gibbs [11] nevéhez köthető.

2017-ben Dujella, Mikic, Kazalicki, Szikszai [7] belátták, hogy végtelen sok Diofantikus hatos létezik, hetesre azonban még egyetlen példát sem ismerünk, továbbá nem ismert abszolút felső korlát sem a második hatvány racionális Diofantikus halmazok elemszámára.

Vegyük most az általánosabb hatványkitevőket górcső alá. A klasszikus esettel ellentétben a $k \geq 3$ választással nincs dokumentált négyes, de már hármasok végtelen családja sem lelhető fel a szakirodalomban. A mi kontextusunkban a legrelevánsabb eredmények Bugeaud és Dujella [2] nevéhez köthetők, akik egyrészt abszolút felső korlátot adtak a lehetséges egész értékű Diofantikus halmazok méretére, másrészt néhány egyszerű példát is mutattak hármasokra $k = 3$ és $k = 4$ esetekben, nevezetese a $\{2, 171, 25326\}$ és a $\{1352, 9539880, 9768370\}$ halmazokat.

Jelen dolgozatban figyelmünket eleinte a racionális Diofantikus halmazoknak szenteljük, kezdetben általános, majd specializált hatványkitevők választása mellett.

A második fejezetben a kitevőtől függetlenül naiv numerikus leszámlálással kapott példákat mutatunk be, melyekben paraméteres családok mintáit ismerhetjük fel. Ezt követően definiáljuk az úgynevezett Diofantikus párok által indukált görbét, továbbá azok néhány alapvető tulajdonságát ismertetjük.

A harmadik fejezetben a klasszikus $k = 2$ esetet tekintjük. Célunk az indukált görbéken alapuló geometriai módszerek használata már ismert eredmény igazolására. Bi-

zonyításainkban elsősorban Lemmermeyer [14] Pell-kúpszeletek aritmetikájával kapcsolatos vizsgálataira támaszkodunk.

Az utolsó fejezetben a $k = 3$ esetet részletezzük. Definiáljuk a 3-leszállás homomorfizmust és ennek segítségével elégséges feltételt adunk bővítések konstrukciójára. Megmutatjuk, hogy néhány kivétellel tetszőleges harmadik hatvány Diofantikus pár végtelen módon bővíthető hármassá. Végezetül ismertetünk egy naiv kereséssel kapott paraméteres harmadik hatvány Diofantikus négyes családot is.

2. k -adik hatvány Diofantikus halmazok

Ebben a fejezetben az általános hatványkitevő vizsgálatát helyezzük fókuszba. Numerikus kereséssel példákat mutatunk racionális Diofantikus hármásokra, melyek több egyszerű parameterikus családból származnak. Ezt követően definiáljuk az úgynevezett Diofantikus párok által indukált görbéket, majd ismertetjük azok néhány alapvető tulajdonságát.

2.1. Racionális Diofantikus hármások

Egy előre rögzített abszolút magasságig¹, tetszőleges k esetén generálhatjuk az összes k -adik hatvány Diofantikus párt. Ezeket a párokat bővíthetjük egy újabb

$$c = \frac{r^k - 1}{a}$$

elemmel, ahol $r \in \mathbb{Q}$. Az egyetlen ellenőrizendő tulajdonság, hogy a $bc + 1$ kifejezés valamilyen r' racionális szám k -adik hatványa legyen.

A fenti keresés számos eredményt ad már egészen kicsi abszolút magasság esetén is, például a

$$\left\{-\frac{1}{2}, \frac{3}{2}, 2\right\}, \left\{-\frac{1}{2}, \frac{7}{2}, 4\right\}, \left\{-\frac{1}{4}, \frac{15}{4}, 4\right\}, \left\{-\frac{1}{4}, \frac{31}{8}, 8\right\}$$

k -adik hatvány Diofantikus halmazokat, ahol $k = 2, 3, 4$, illetve 5. Amennyiben k páros a következő paraméterezést fedezhetjük fel:

$$\{a, b, c\} = \left\{-\frac{1}{2^{\frac{k}{2}}}, \frac{2^k - 1}{2^{\frac{k}{2}}}, 2^{\frac{k}{2}}\right\}. \quad (1)$$

Amennyiben k páratlan, úgy

$$\{a, b, c\} = \left\{-\frac{1}{2^{\frac{k-1}{2}}}, \frac{2^k - 1}{2^{\frac{k+1}{2}}}, 2^{\frac{k+1}{2}}\right\}. \quad (2)$$

¹Legyen $r = \frac{p}{q} \in \mathbb{Q}$ ahol $\gcd(p, q) = 1$. Ekkor r abszolút magasságán $H(r) = \max\{|p|, |q|\}$ kifejezést értjük.

Mindkét esetben:

$$ab + 1 = \left\{ \frac{1}{2} \right\}^k \quad \text{és} \quad bc + 1 = 2^k$$

míg

$$ac + 1 = \begin{cases} 0 & \text{ha } k \equiv 0 \pmod{2} \\ -1 & \text{ha } k \equiv 1 \pmod{2}. \end{cases}$$

Ha a kitevő páratlan, úgy további minták azonosíthatóak be. Először vizsgáljuk a

$$\left\{ 8, \frac{7}{8}, -\frac{9}{8} \right\}, \left\{ 32, \frac{31}{32}, -\frac{33}{32} \right\}, \left\{ 128, \frac{127}{128}, -\frac{129}{128} \right\} \quad (3)$$

hármasokat, majd a

$$\left\{ 7, 9, -\frac{1}{8} \right\}, \left\{ 31, 33, -\frac{1}{32} \right\}, \left\{ 127, 129, -\frac{1}{128} \right\} \quad (4)$$

hármasokat, ahol k rendre 3, 5, illetve 7. A következő paraméterezéseket használhatjuk.

A (3) esetben

$$\{a, b, c\} = \left\{ 2^k, \frac{2^k - 1}{2^k}, \frac{-2^k - 1}{2^k} \right\}. \quad (5)$$

Ekkor

$$ab + 1 = 2^k, \quad ac + 1 = (-2)^k \quad \text{és} \quad bc + 1 = -\frac{1}{2^{2k}}.$$

A (4) esetben

$$\{a, b, c\} = \left\{ 2^k - 1, 2^k + 1, -\frac{1}{2^k} \right\}. \quad (6)$$

Ekkor

$$ab + 1 = 2^{2k}, \quad ac + 1 = \frac{1}{2^k} \quad \text{és} \quad bc + 1 = -\frac{1}{2^k}.$$

Vegyük észre, hogy a fentiekben a következő állítás igazolását végeztük el.

2.1. Állítás. *Bármely k esetén létezik k -adik hatvány racionális Diofantikus hármas.*

Vegyük észre, hogy az előző konstrukciók könnyűszerrel általánosíthatók. Ha k páros az (1) esetben, akkor tetszőleges $r \neq 0, \pm 1$ racionális hatványalapot helyettesítve

$$\{a, b, c\} = \left\{ -\frac{1}{r^{\frac{k}{2}}}, \frac{r^k - 1}{r^{\frac{k}{2}}}, r^{\frac{k}{2}} \right\}. \quad (7)$$

Ekkor

$$ab + 1 = \left(\frac{1}{r} \right)^k, \quad ac + 1 = 0 \quad \text{és} \quad bc + 1 = r^k.$$

Ha k páratlan az (5) és a (6) esetekben, úgy szintén egyszerű helyettesítést végezhetünk. Előbbire

$$\{a, b, c\} = \left\{ r^k, \frac{r^k - 1}{r^k}, \frac{-r^k - 1}{r^k} \right\},$$

ebben az esetben

$$ab + 1 = r^k, \quad ac + 1 = (-r)^k \quad \text{és} \quad bc + 1 = -\frac{1}{r^{2k}},$$

míg utóbbira

$$\{a, b, c\} = \left\{ r^k - 1, r^k + 1, -\frac{1}{r^k} \right\}.$$

Ekkor

$$ab + 1 = r^{2k}, \quad ac + 1 = \frac{1}{r^k} \quad \text{és} \quad bc + 1 = -\frac{1}{r^k}.$$

A (2) ilyen módon történő általánosítása egy kicsit bonyolultabb. Ha tetszőleges r -et helyettesítve a formulába azt kapjuk, hogy

$$ac + 1 = -\frac{1}{r^{\frac{k-1}{2}}} r^{\frac{k+1}{2}} + 1 = -r + 1$$

A probléma feloldásához legyen $r = 1 - s^k$ valamilyen racionális $s \neq 0, 1$ esetén, így

$$\{a, b, c\} = \left\{ -\frac{1}{r^{\frac{k-1}{2}}}, \frac{r^k - 1}{r^{\frac{k+1}{2}}}, r^{\frac{k+1}{2}} \right\}$$

k -adik hatvány racionális Diofantikus halmaz lesz, hiszen

$$ab + 1 = \left(\frac{1}{r}\right)^k, \quad ac + 1 = s^k, \quad bc + 1 = r^k.$$

Ezek alapján a következőt állíthatjuk.

2.2. Tétel. *Bármely k esetén végtelen sok k -adik hatvány racionális Diofantikus hármas létezik.*

2.3. *Megjegyzés.* Ezen paraméterezések nem fedik le az összes hármaszt. Például könnyű számolással adódik, hogy az $\{1, -35/8, 63\}$ halmaz egyik családba sem tartozó harmadik hatvány racionális Diofantikus hármas.

A továbbiakban egy másik megközelítést alkalmazunk.

2.2. Indukált görbék

2.4. Definíció. *Legyen az $\{a, b\}$ k -adik hatvány Diofantikus pár. Ekkor a*

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

affin algebrai görbét az $\{a, b\}$ pár által indukált görbének nevezzük.

Látható, hogy bármely racionális c , amely az $\{a, b\}$ párt hármassá bővíti megfelel a $C_{a,b}$ valamely racionális pontjában² szereplő y koordinátának. Továbbá vegyük észre, hogy amennyiben valamelyik koordinátát 0-nak választjuk, úgy adódik, hogy a $C_{a,b}$ görbén az alábbi racionális pontok szerepelnek:

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

²A $C_{a,b}$ racionálási pontjain a $C_{a,b}(\mathbb{Q}) = \{(x, y) | (ay + 1)(by + 1) = x^k, (x, y) \in \mathbb{Q} \times \mathbb{Q}\}$ halmazt értjük.

A továbbiakban megmutatjuk, hogy ezen görbék biracionális transzformációk segítségével aritmetikailag kedvezőbb alakra hozhatóak. Pontosabban.

2.5. Állítás. *Legyen $C_{a,b}$ az $\{a, b\}$ pár által indukált görbe. Ekkor páratlan k esetén az*

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

biracionális változótranszformációk az alábbi, modellre vezetnek

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

Páros k esetén az

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

transzformációkkal a görbe egyenlete

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

alakra hozható.

Bizonyítás. Az indukált görbe egyenletének tagjait kibontva kapjuk, hogy

$$aby^2 + (a+b)y + 1 = x^k.$$

Ha k páratlan, akkor mindkét oldalt megszorozva $(ab)^k$ -nal és teljes négyzetté alakítva adódik, hogy

$$\left((ab)^{\frac{k+1}{2}}y + \frac{(a+b)(ab)^{\frac{k-1}{2}}}{2} \right)^2 - \left(\frac{a+b}{2} \right)^2 ab^{k-1} + (ab)^k = x^k(ab)^k.$$

Tovább alakítva

$$\left((ab)^{\frac{k+1}{2}} y + \frac{(a+b)(ab)^{\frac{k-1}{2}}}{2} \right)^2 - \left(\frac{a-b}{2} \right)^2 ab^{k-1} = (abx)^k.$$

Ha k páros akkor mindkét oldalt $(ab)^{k+1}$ -nel szorozva és teljes négyzetté alakítva hasonló számítással kapjuk az állítás eredményét. $\square$

A fenti biracionális transzformációk alkalmazásával, a P, A, B pontok páros k esetén az alábbi

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

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

míg páratlan k esetén

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

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

koordináta párokkal írhatók.

Továbbá ezen görbék a következő alapvető tulajdonságokkal rendelkeznek.

2.6. Állítás. $C_{a,b}$ nem szinguláris.

Bizonyítás. Legyen

$$F(x, y) = (ay + 1)(by + 1) - x^k$$

A szinguláris pontokat $C_{a,b}$ -n az alábbi egyenletrendszer határozza meg:

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

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 $a = b$ adódik, ami ellent mond az 1.1 definícióban szereplő páronként különböző feltételnek. $\square$

A görbék osztályozását a geometriai génuszuk³ szerint végezzük. Ezek alapján adódik, hogy a görbe

- $k = 2$ esetben Pell-kúpszelet,
- $k = 3, 4$ esetben elliptikus görbe,
- $k \geq 5$ esetben hiperelliptikus görbe.

A dolgozat további részeiben a $k = 2$ és a $k = 3$ esetekre fogunk összpontosítani.

³A dolgozatnak nem tárgya a geometriai és/vagy aritmetikai génusz precíz definiálása, de esetünkben a nem szinguláris görbék kapcsán elegendő a génusz-fokszám formula használata. Eszerint a görbe projektív modelljét tekintve az adódó polinom fokszámát d -vel jelölve, a génusz éppen $\frac{(d-1)(d-2)}{2}$.

3. Második hatvány Diofantikus halmazok

Ebben a fejezetben célunk már ismert eredmények újszerű geometriai megközelítésből történő vizsgálata. Elsősorban Lemmermeyer [14] Pell-kúpszeletekkel kapcsolatos, valamint Dujella [4, 5], a klasszikus $k = 2$ esetben végzett összefoglaló munkáira támaszkodunk.

3.1. Indukált görbe $k = 2$ esetben

A $k = 2$ esetnél az indukált görbe a

$$C_{a,b} : (ay + 1)(by + 1) = x^2$$

modellel írható le, melyet az alábbi, aritmetikailag szerencsésebb, alakban írhatunk

$$C'_{a,b} : X^2 - dY^2 = 4,$$

ahol

$$Y = \left(\frac{4x}{a-b} \right), \quad X = \left(aby + \frac{a+b}{2} \right) \left(\frac{4}{a-b} \right) \quad \text{és} \quad d = ab,$$

és d négyzementes egész.⁴ A standard pontok a transzformált görbén a következők:

$$P' = \left(2\frac{a+b}{a-b}, \frac{4}{a-b} \right), \quad A' = (2, 0), \quad B' = (-2, 0).$$

Definiáljuk a C racionális pontjain értelmezett összeadást a következőképpen. Legyen $N = (2, 0)$ neutrális elem. A $P + Q = R$ esetén legyen R a görbe második metszéspontja a PQ egyenes N -en áthaladó eltoltjával.

3.1. Állítás. *Legyen $P = (r, s)$ és $Q = (t, u) \in C(\mathbb{Z})$. Ekkor*

$$P + Q = \begin{cases} \left(2\frac{r^2+ds^2}{r^2-ds}, 4\frac{rs}{r^2-ds^2} \right) & \text{ha } P = Q \\ \left(2\frac{\Delta(s-u)^2+(r-t)^2}{\Delta(s-u)^2-(r-t)^2}, 4\frac{(r-t)(s-u)}{\Delta(s-u)^2-(r-t)^2} \right) & \text{ha } P \neq Q \end{cases}$$

⁴Az x és y változócsere az eddigi szakirodalomba történő elhelyezkedés jegyében hajtottuk végre.

3.2. *Megjegyzés.* [14] első esetében a $P + Q = (r^2 - 2, rs)$ kifejezés szerepel. Vegyük észre, hogy ez a formula nem elégíti ki az $x^2 - dy^2 = 4$ egyenletet. A bizonyítás során apró számolási hibát találtunk, ezért magunk vezetjük le a bizonyítás ezen részét.

Bizonyítás. Legyen $P = (r, s)$, $Q = (t, u)$ és $N = (2, 0)$. Az N -en átmenő egyenes egyenlete $Y = m(X - 2)$. Ha $P = Q$, a PQ egyenes meredeksége a P beli érintő meredeksége, melyet deriválással kaphatunk meg.

$$2x - 2dy y' = 0$$

Ebből y' kifejezve adódik, hogy

$$m = y' = \frac{x}{dy} = \frac{r}{ds}.$$

Az egyenes és görbe metszéspontját a következő egyenletből kaphatjuk meg:

$$(X - 2)[X + 2 - dm^2(X - 2)] = 0.$$

Ha $X = 2$ az N pont adódik, a másik metszéspontot az

$$X = 2 \frac{dm^2 + 1}{dm^2 - 1}$$

$m = \frac{r}{ds}$ kifejezést helyettesítve kapjuk, hogy

$$X = 2 \frac{r^2 + ds^2}{r^2 - ds^2}$$

Ezt behelyettesítve kapjuk, hogy

$$Y = \frac{4rs}{r^2 - ds^2}.$$

□

3.3. Tétel ([14] Proposition 1.2). *A 3.1-ben definiált összeadás zárt az egész pontokra nézve.*

3.2. Bővítések

Dujella [4] egy $\{a, b, c\}$ Diofantikus hármashból kiindulva az

$$E_{a,b} : (ay + 1)(by + 1)(cy + 1) = x^2$$

elliptikus görbét vizsgálta. Teljesül a következő állítás.

3.4. Állítás ([5] Proposition 1.). *Legyen $\{a, b\}$ második hatvány értékű Diofantikus pár. Ekkor egy $S \in E_{a,b}(\mathbb{Q})$ pont y -koordinátája pontosan akkor bővítés, ha $S - P \in 2E_{a,b}(\mathbb{Q})$.*

Ennek analógiájaként ígéretes stratégiának tűnik a $(2m + 1)P$ alakú pontokat vizsgálni, ahol $m \in \mathbb{Z} \setminus \{0, -1\}$. Alkalmazva a pont összeadás formulát, legyen

$$c = y(3P) = 8 \frac{a + b}{a^2 - 2ab + b^2}$$

és

$$d = y(5P) = 8 \frac{3a^3 + 13a^2b + 13ab^2 + 3b^3}{a^4 - 4a^3b + 6a^2b^2 - 4ab^3 + b^4}.$$

Ekkor

$$ac + 1 = \frac{9a^2 + 6ab + b^2}{a^2 - 2ab + b^2} = \left(\frac{3a + b}{a - b} \right)^2,$$

$$bc + 1 = \frac{a^2 + 6ab + 9b^2}{a^2 - 2ab + b^2} = \left(\frac{a + 3b}{a - b} \right)^2,$$

$$ad + 1 = \frac{25a^4 + 100a^3b + 110a^2b^2 + 20ab^3 + b^4}{a^4 - 4a^3b + 6a^2b^2 - 4ab^3 + b^4} = \left(\frac{5a^2 + 10ab + b^2}{(a - b)^2} \right)^2,$$

$$bd + 1 = \frac{a^4 + 20a^3b + 110a^2b^2 + 100ab^3 + 25b^4}{a^4 - 4a^3b + 6a^2b^2 - 4ab^3 + b^4} = \left(\frac{a^2 + 10ab + 5b^2}{(a - b)^2} \right)^2.$$

A négyessé való bővítéshez szükséges lenne, hogy

$$cd + 1 = \frac{a^6 - 6a^5b + 15a^4b^2 - 20a^3b^3 + 15a^2b^4 - 6ab^5 + b^6 + 192a^4 + 1024a^3b + 1664a^2b^2 + 1024ab^3 + 192b^4}{(a-b)^6}$$

teljes négyzet legyen, ami sajnos nem teljesül szükségszerűen. A másik érdekes kérdés, hogy mikor garantálható az egészértékűség? Ebben a konstrukcióban, ehhez már a P egészértékűségét is biztosítani kell, azaz teljesülnie kell az

$$\left. \begin{array}{l} (a-b)|4 \\ (a-b)|2(a+b) \end{array} \right\}$$

relációknak. Ezen túlmenően az inverz transzformációk, azaz az

$$x = \frac{Y(a-b)}{4} \quad y = \frac{a-b}{4ab}X - \frac{a+b}{2ab} = \frac{1}{4} \frac{(a-b)X - 2a - 2b}{ab}$$

eredményéül kapott értékeknek szintén egészeknek kell lenniük. Egy megoldása a feltételrendszernek az $\{a, b\} = \{t-1, t+1\}$, valamely $t \in \mathbb{Z}$ esetén. Ezzel a választással egy klasszikus eredményt kapunk nevezetesen az $y(3P) = 4t, y(5P) = 16t^3 - 4t$, melyek nem csak bővítései az $\{a, b\}$ párnak, hanem teljesül, hogy $y(3P)y(5P) + 1 = (8t^2 - 1)^2$ azaz egy második hatvány Diofantikus négyeshez jutottunk.

4. Harmadik hatvány Diofantikus halmazok

Ebben a fejezetben a $k = 3$ esettel fogunk foglalkozni. A $k = 2$ klasszikus eset analógiájaként, definiáljuk a 3-leszállást és segítségével elégséges feltételt adunk a bővítésekre. Megmutatjuk, hogy ezen feltétel nem szükséges. Az utolsó szekcióban harmadik hatvány Diofantikus négyesek egy családját mutatjuk be.

4.1. Indukált görbe $k = 3$ esetben és a 3-leszállás

A 2.5 állítás specializálásával kapjuk, hogy az indukált görbe

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

alakra hozható. A triviális pontok a görbén a következők:

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

Egyszerű számítással kapjuk, hogy az A' és a B' rendje 3.

A fejezetben Cohen [3] explicit leírását a használjuk a 3-leszállásnak. Definiáljuk a 3-leszállás leképezést $\alpha : C'_{a,b}(\mathbb{Q}) \rightarrow \mathbb{Q}^*/\mathbb{Q}^{*3}$

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

4.1. Tétel (Cohen [3]). *Az α leképezés csoporthomomorfizmus, továbbá $\ker \alpha \supset 3C'_{a,b}(\mathbb{Q})$*

4.2. Hármások konstrukciója

A $k = 2$ esetben a megfelelő bővítéseket az [5]-ben szereplő 2-leszállás klasszifikálja. Informálisan fogalmazva, a megfelelő kiterjesztések és a triviális választás megegyeznek modulo négyzetek a leképezés mentén. Figyeljük meg, hogy a 3-leszállás lényegében ugyanezt teszi, de modulo köbszámok. Ezek alapján a következő eredményt kapjuk.

4.2. Tétel. 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. □

4.3. Megjegyzés. Az előző bizonyításban csupán az $ay(T) + 1 = r^3$ részt igazoltuk, a $by(T) + 1 = r'^k$ belátásához a 3-leszállás definíciójában B pontot kell használni, melyből következik az állítás.

4.4. Lemma. Legyen $\{a, b\}$ harmadik hatvány racionális Diofantikus pár. Ekkor a $P = (1, 0)$ rendje végtelen a $C_{a,b}$ -n, amennyiben $a \neq -b, 2b$ vagy $\frac{b}{2}$.

A bizonyításhoz szükségünk lesz Fueter [10] következő, a Mordell görbék torziójára vonatkozó eredményére.

4.5. Lemma (Fueter [10]). 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 következőképpen adható meg:

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

4.6. Következmény. *A torziós részcsoportja a $C_{a,b}(\mathbb{Q})$ -nak csak $\mathbb{Z}/6\mathbb{Z}$ vagy $\mathbb{Z}/3\mathbb{Z}$ lehet.*

Bizonyítás. Tekintsük az $\{a, b\}$ pár által indukált görbét. Legyen $a = \frac{a_1}{a_2}, b = \frac{b_1}{b_2}$ úgy, hogy $\gcd(a_1, a_2) = \gcd(b_1, b_2) = 1$. Ekkor az indukált görbét a következő

$$Y'^2 = X'^3 + B,$$

alakra transzformálhatjuk, ahol $B = a_1^2 b_1^2 (a_1 b_2 - b_1 a_2)^2 a_2^2 b_2^2$. Ekkor, a 4.5 lemma jelölését használva, $B_1 = 1$ vagy $B_1 \neq 1$ négyzet. $\square$

4.4 lemma bizonyítása. Alkalmazzuk a 4.5 lemmát és a 4.6 következményt. Ekkor ellenőrizzük az mP' pontokat, ahol $m \in \{3, 6\}$. Ezek alapján P rendje végtelen, kivéve ha $a = -b, 2b$ vagy $\frac{b}{2}$. $\square$

4.7. Lemma. *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 $\frac{b}{2}$.*

Bizonyítás. 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 a pár a következő görbét származtatja

$$E_{b,2b} : 2b^2 + 1 = x^3.$$

Az $E_{b,2b}$ 0 rangú görbe, azaz elegendő a torzióspontokat vizsgálni, melyeket a Lutz-Nagell tétel segítségével könnyen meghatározhatunk. Ezek alapján nem létezik a feltételeket kielégítő $\{a, b\}$ pár.

A $\{-b, b\}$ alakú párok a következő görbét származtatják

$$E_{-b,b} : -b^2 + 1 = x^3.$$

A görbe szintén 0 rangú, így hasonló eljárást alkalmazhatunk, de ebben az esetben vannak megfelelő torzióspontokból származó párok, a $\{-1, 1\}$ és a $\{-3, 3\}$. $\square$

Hasonlóan a klasszikus esethez a végtelen rendű pont többszörösének felhasználásával standard módon bővíthetünk hármasokká. Itt elegendő egy racionális T nem torziós pont a $C_{a,b}$ -n, ekkor a $(3m)T + P$ pontok, bármelyike $m \in \mathbb{Z} \setminus \{0\}$, megfelelő kiterjesztést ad az y koordinátájában. Kézenfekvő választásként használjuk a P végtelen rendű pontot. Ezek alapján a következő tételt fogalmazhatjuk meg.

4.8. Tétel. *Bármely $\{a, b\}$ harmadik hatvány racionális Diofantikus pár végtelen módon bővíthető hármasokká, amennyiben nem $\{-1, 1\}$ vagy $\{-3, 3\}$. Ezen kivételek nem bővíthetők hármassá.*

Bizonyítás. Az állítás első része közvetlen következménye a 4.2 tételnek. A második részéhez vizsgáljuk a $\{-1, 1\}$ és a $\{-3, 3\}$ által indukált görbéket.

$$C_{-1,1} : (-y + 1)(y + 1) = x^3 \quad \text{és} \quad C_{-3,3} : (-3y + 1)(3y + 1) = x^3.$$

Mindkét esetben a görbe rangja 0, és a torziós részcsoporthoz izomorf $\mathbb{Z}/3\mathbb{Z}$ -vel, így a triviálisokon kívül nincsenek racionális pontok a görbén, melyből az állításunk következik. $\square$

4.9. Példa. *Példaként bővítsük az $\{a, b\}$ párt az $y(-2P)$ -vel, ekkor a következő Diofantikus hármasst kapjuk:*

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

4.3. Négyesek konstrukciója

Alapvető gondolatként merül fel, hogy vajon egy pár különböző bővítései segítségével négyest kapunk-e? Sajnos már a legegyszerűbb esetekben is a magasság "felrobban". Szemléltetésképpen, ha az $\{a, b\}$ párt az $c = y(-2P)$ és az $d = y(4P)$ -vel bővítjük akkor

$$cd + 1 = \frac{r_1}{r_2}$$

ahol

$$\begin{aligned} r_1 = & a^{18} - 36a^{17}b + 423a^{16}b^2 - 1452a^{15}b^3 - 2718a^{14}b^4 + 8136a^{13}b^5 + 5118a^{12}b^6 - 19908a^{11}b^7 - 2952a^{10}b^8 + \\ & 26264a^9b^9 - 2952a^8b^{10} - 19908a^7b^{11} + 5118a^6b^{12} + 8136a^5b^{13} - 2718a^4b^{14} - 1452a^3b^{15} + 423a^2b^{16} - 36ab^{17} + \\ & b^{18} - 567a^{16} + 4536a^{15}b - 22599a^{14}b^2 + 78813a^{13}b^3 - 266733a^{12}b^4 + 782217a^{11}b^5 - 1710801a^{10}b^6 + \\ & 2721519a^9b^7 - 3173337a^8b^8 + 2721519a^7b^9 - 1710801a^6b^{10} + 782217a^5b^{11} - 266733a^4b^{12} + 78813a^3b^{13} - \\ & 22599a^2b^{14} + 4536ab^{15} - 567b^{16} \end{aligned}$$

és

$$r_2 = (a^4 - 14a^3b + 24a^2b^2 - 14ab^3 + b^4)^3(a + b)^6.$$

Más bővítések alkalmazásával magasabb fokú kifejezésekhez jutunk, ezért a továbbhaladáshoz némi heurisztikára lesz szükségünk. Vegyük észre, hogy a 4.2 tételben szereplő $T - P \in 3C_{a,b}(\mathbb{Q}) \subset \ker \alpha$ szükséges, de nem elégséges feltétel. Például a

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

esetben az $S = (6031, 25326) \in C_{2,171}(\mathbb{Q})$ bővítése a $\{2, 171\}$ párnak, de az $S - P$ nem háromszoros pont. Ezek alapján lehetséges, hogy P más többszörösei is bővítésként szolgálhatnak. Kiindulásként a korábban bemutatott hármas családok egyik legegyszerűbb racionális párjából indultunk ki, az $\{a, b\} = \{t, -\frac{1}{t}\}$ halmazból, ahol $t = r^3$ valamely $r \in \mathbb{Q}$ esetén, majd vettük a $y(mP)$ számokat, ahol $m \in \mathbb{Z}$. Az eredményt a következő tételben mutatjuk be.

4.10. Tétel. *Legyen $t = r^3, r \in \mathbb{Q}, r \neq 0, \pm 1$. Ekkor*

$$\left\{ t, -\frac{1}{t}, \frac{-9 \cdot (t^{15} + t^9 + t^3)}{(t^{18} - 3 \cdot t^{12} + 3 \cdot t^6 - 1)}, \frac{t^{24} + 5 \cdot t^{18} + 15 \cdot t^{12} + 5 \cdot t^6 + 1}{(t^{21} - 3 \cdot t^{15} + 3 \cdot t^9 - t^3)} \right\}$$

harmadik hatvány racionális Diofantikus négyes.

Bizonyítás. A halmaz harmadik eleme az $y(-2P)$, mely a 4.2 Tétel miatt bővítés, ezért elegendő csupán az utolsó tagot vizsgálni.

$$\begin{aligned} ad + 1 &= \frac{r^{24} + 6r^{18} + 12r^{12} + 8 \cdot r^6}{r^{18} - 3r^{12} + 3r^6 - 1} = \left(\frac{r^8 + 2r^2}{r^6 - 1} \right)^3 \\ bd + 1 &= -\frac{8r^{18} + 12r^{12} + 6r^6 + 1}{r^{24} - 3r^{18} + 3r^{12} - r^6} = \left(\frac{2r^6 + 1}{r^8 - r^2} \right)^3 \\ cd + 1 &= -\frac{8r^{36} + 60r^{30} + 174r^{24} + 245r^{18} + 174r^{12} + 60r^6 + 8}{r^{36} - 6r^{30} + 15r^{24} - 20r^{18} + 15r^{12} - 6r^6 + 1} = \\ &= \left(\frac{(2r^6 + 1)(r^6 + 2)}{(r^2 + r + 1)^2(r^2 - r + 1)^2(r + 1)^2(r - 1)^2} \right)^3 \end{aligned}$$

□

Hivatkozások

- [1] 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.
- [2] Yann Bugeaud and Andrej Dujella. On a problem of Diophantus for higher powers. *Math. Proc. Cambridge Philos. Soc.*, 135(1):1–10, 2003.
- [3] Henri Cohen. *Number theory. Vol. I. Tools and Diophantine equations*, volume 239 of *Graduate Texts in Mathematics*. Springer, New York, 2007.
- [4] Andrej Dujell. Diophantine m -tuples webpage, Accessed 2022.
- [5] Andrej Dujella. Diophantine m -tuples and elliptic curves. *Journal de théorie des nombres de Bordeaux*, 13(1):111–124, 2001.
- [6] Andrej Dujella. There are only finitely many Diophantine quintuples. *J. Reine Angew. Math.*, 566:183–214, 2004.
- [7] 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.
- [8] Leonhard Euler. *Opuscula analytica* i. 1783.
- [9] 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.
- [10] Rudolf Fueter. Ueber kubische diophantische gleichungen. *Commentarii mathematici Helvetici*, 2:69–90, 1930.
- [11] Philip Gibbs. Some rational Diophantine sextuples. *Glas. Mat. Ser. III*, 41(61)(2):195–203, 2006.
- [12] Bo He, Alain Togbé, and Volker Ziegler. There is no Diophantine quintuple. *Trans. Amer. Math. Soc.*, 371(9):6665–6709, 2019.
- [13] 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.
- [14] Franz Lemmermeyer. Higher descent on pell conics iii. the first 2-descent, 2003.

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