dc_871_14

Polinomiális-exponenciális diofantikus egyenletek és egyenletrendszerek

MTA doktori rövid értekezés

Szalay László

Sopron, 2014

dc_871_14

Tartalomjegyzék

dc_871_14

Bevezetés

A *De Numeris Harmonicis* című, 1343-ban írt könyvében Levi ben Gershon bizonyítást adott arra, hogy csak az

$$(1,2), \quad (2,3), \quad (3,4), \quad (8,9)$$

harmonikus számokból álló párok tagjainak különbsége pontosan 1. A probléma Philippe de Vitry francia zeneszerzőtől származik, aki a 2^k3^ℓ alakú, ún. harmonikus számok iránt érdeklődött zeneelméleti nézőpontból.

Valószínűleg ez volt az első exponenciális (tágabb értelemben polinomiális-exponenciális) diofantikus egyenlet, amelynek története és megoldása bizonyítottan ismert. A későbbiekben a témához tartozó legnevesebb tételek egyike Nagell nevéhez fűződik (1948), aki belátta Ramanujan azon sejtését, miszerint az X^2+7 polinom pozitív egész helyeken felvett helyettesítési értékei csak az 1, 3, 5, 11 és 181 helyeken lesznek 2 hatványai.

A két megadott időpont között többnyire elszórt állítások jelentek meg polinomiális-exponenciális egyenletekkel kapcsolatban, melyeket Legendre, Lebesque, Catalan, Ramanujan neve fémjelez. Aztán Bakernek és más kutatóknak az algebrai számok logaritmusai lineáris formáira vonatkozó eredményei, továbbá az Altér tétel valamint az egységegyenletek elmélete új lökést adtak a diofantikus egyenletek hatékony vizsgálatának. Mára kiterjedt és szerteágazó irodalma van a polinomiális-exponenciális diofantikus egyenleteknek, jelen értekezés a szerző ezirányú kutatásait foglalja össze.

A disszertáció első fejezetének elején megadjuk azt az általános polinomiális-exponenciális diofantikus egyenlettípust, melyből az első és második fejezetekben tárgyalt problémák mindegyike származtatható. Elsőként a $2^n \pm 2^m \pm 2^\ell = x^2$ egyenletet elemezzük, majd a következő részben az $(a^n-1)(b^n-1) = x^2$ egyenlettel foglalkozunk. Az első fejezet harmadik problémaköre a másodrendű lineáris rekurziókban előforduló bizonyos polinomiális értékek vizsgálata, például speciális alakú binomiális együtthatóké.

A második fejezet kiindulópontja két, a klasszikus diofantikus szám m-esekhez kapcsolódó rokon feladatosztály. A diofantikus m-es olyan $\{a_1, \ldots, a_m\}$ egészekből álló halmaz, melyre bármely $1 \le i < j \le m$ esetén $a_ia_j + 1$ négyzetszám. Fel lehet vetni, hogy mi történik ha a négyzetszámok helyére egy adott lineáris rekurzív sorozat tagjait tesszük, vagy valamely rögzített $p_1, p_2, \ldots p_r$ prímek esetén a $p_1^{\tau_1}p_2^{\tau_2}\cdots p_r^{\tau_r}$ formájú ún. S-egységeket. Mindkét származtatott esetben – akárcsak a motivációt jelentő alapesetben – egy $m(m-1)/2$ egyenletből álló diofantikus egyenletrendszert vizsgálunk. Kiderült, hogy a bináris rekurzióknál az $m = 3$ érték a „kritikus", míg az S-egységeknél $r = 2$ mellett $m = 4$ (míg az eredeti problémánál $m = 5$ volt).

Az értekezésben elemzett diofantikus egyenletek és egyenletrendszerek esetén bemutatjuk azok szűkebb történetét és előzményeit, valamint az eredmények hatását és következményeit is. Tehát hangsúlyt fektettünk arra, hogy a saját eredményeket beágyazzuk az egyre bővülő szakirodalomba.

A vizsgálatok során az elemi számelméleti ismereteken túl felhasználtuk a kvadratikus maradékok elméletét, az algebrai számelméletet, a Pell egyenletek megoldásaira vonatkozó ismereteket, lineáris rekurzív sorozatokat, diofantikus approximációra vonatkozó eredményeket, lánctörteket, a Baker-módszert, az Altér tételt, az egységegyenletek elméletét. A dolgozat törzsében – a disszertáció jellegének megfelelően – a bizonyításokat nem részletezzük, de több esetben vázoljuk a fő gondolatmenetet, és bemutatjuk az előbb felsorolt módszerek alkalmazási környezetét.

A kapott eredmények jellege egyrészt végességi illetve végtelenségi tételekben nyilvánul meg, másrészt sok esetben sikerült teljes egészében megadni a vizsgált probléma összes (véges vagy végtelen sok) megoldását vagy bizonyítani a megoldhatatlanságát. Az értekezésben megjelenített saját tételeket bekereteztük, hogy jól láthatóan elkülönüljenek mások munkáitól.

A disszertációban leírt eredmények alapvetően a következő tíz publikációban jelentek meg: [83], [81], [27], [34], [84], [19], [58], [30], [85], [86].

1. fejezet

Polinomiális-exponenciális diofantikus egyenletek

Tekintsük az általános

$$u_1\xi_1^{n_1} + u_2\xi_2^{n_2} + \cdots + u_k\xi_k^{n_k} = p(x_1, x_2, \ldots, x_t) \tag{1}$$

diofantikus egyenletet, ahol u_i, ξ_i $(i = 1, 2, ..., k)$ rögzített egészek, $p(X_1, X_2, \ldots, X_t)$ egy adott egészegyütthatós polinom és a megoldásokat az $x_1, x_2, \ldots, x_t$ egészekben és az $n_1, n_2, ..., n_k$ nem negatív egészekben keressük. Az ismeretleneket figyelembe véve (1) bal oldala exponenciális kifejezés, jobb oldala polinomiális, ezért a fenti diofantikus egyenlet vegyes típusú, melyet polinomiális-exponenciálisnak hívunk.

Az (1) egyenlet több változata, módosítása ismert. A $p(X_1, X_2, \ldots, X_t)$ polinom lehet még egészértékű, vagy racionális együtthatós, vagy a racionális számtest egy algebrai bővítésével kapott $\mathbb{K}$ számtest elemei lehetnek az együtthatói. Hasonlóan (1) bal oldalán az együtthatók és a hatványalapok is lehetnek egy algebrai számtest egészei. A megoldásokat is kereshetjük úgy, hogy $n_1, n_2, ..., n_k \in \mathbb{Z}$ és $x_1, x_2, \ldots, x_t$ a $\mathbb{K}$ algebrai számtest egészei.

A fenti alakban az (1) egyenlet túl általános, ezért a rá vonatkozó eredmények különböző specifikus eseteket vizsgálnak. A p polinom általában egyváltozós, melyet a továbbiakban $p(X)$-szel jelölünk. Ekkor az Altér tételt felhasználva Evertse, Schlickewei és Schmidt [17] a következő általános, végességi tételt bizonyították a $p(X)$ polinomot a konstans 1 polinomnak feltételezve. Legyen $\mathbb{L}$ egy 0 karakterisztikájú test, k egy pozitív természetes szám, továbbá Γ a multiplikatív $(\mathbb{L}^\star)^k$ csoport egy végesen generált részcsoportja. Adott $v_1, v_2, \ldots, v_k \in \mathbb{L}^\star$ esetén jelölje $M_{sz}(v_1, v_2, \ldots, v_k, \Gamma)$ a

$$v_1x_1 + v_2x_2 + \cdots + v_kx_k = 1$$

egyenlet olyan $(x_1, x_2, \ldots, x_k) \in \Gamma$ megoldásainak számát, ahol nincs eltűnő részletösszeg. Ekkor

$$M_{sz}(v_1, v_2, \ldots, v_k, \Gamma) \leq \exp\left((6k)^{3k}(r+1)\right),$$

ahol r-rel Γ rangját jelöljük. Általánosabban, a Kummer elméletet és az S-egységek összegére vonatkozó eredményeket felhasználva Laurent [35] leírta a

$$\sum_{\mu} H_k(\mu) v_{1,k}^{m_1} \dots v_{r,k}^{m_r} = 0, \qquad (k = 1, \dots, s)$$

egyenletrendszer megoldáshalmazának szerkezetét, ahol a $v_{i,k}$ értékek $(i = 1, \dots, r)$ nullától különböző algebrai számok, H_k-k algebrai együtthatós polinomok, és $\mu = (m_1, \dots, m_r)$ racionális ismeretlenek egy vektora. Laurent eredményének kvalitatív változatát nyerte Győry [24] és Evertse [16].

Tegyük most fel, hogy az $n_1 = n_2 = \cdots = n_k$ egyenlőségek teljesülnek, továbbá $\xi_1, \xi_2, \dots, \xi_k$ egy adott polinom összes gyöke, mind egyszeres multiplicitással. Ekkor (1) úgy is felfogható, mint egy lineáris rekurzív sorozat adott polinomiális értékeire vonatkozó egyenlőség.

Amennyiben $2 \leq \xi_1 = \xi_2 = \cdots = \xi_k \in \mathbb{N}$ van előírva, akkor egy adott számrendszeren belüli speciális értékek meghatározását kérdezzük. Ezeknél a problémáknál is általában p egy rögzített egyváltozós polinom.

A doktori értekezés első részében két (1) típusú egyenlet tárgyalására kerül sor, ahol a vizsgált egyenletek összes megoldásának meghatározása volt a cél.

1.1. A $\pm 2^{n_1} \pm 2^{n_2} \pm \cdots \pm 2^{n_k} = x^2$ egyenlet

Tegyük fel, hogy $p(X) = X^2$, továbbá $u_1, u_2, \dots, u_k \in \{\pm 1\}$ és $\xi_1 = \xi_2 = \cdots = \xi_k = 2$. Ekkor (1) a

$$\pm 2^{n_1} \pm 2^{n_2} \pm \cdots \pm 2^{n_k} = x^2 \tag{2}$$

formát ölti. Világos, hogy bizonyos előjel konstellációkra eleve nincs megoldás. Az általánosság megszorítása nélkül feltehető, hogy $n_1 \geq n_2 \geq \cdots \geq n_k$, továbbá, hogy 2^{n_1} együtthatója 1.

A címadó egyenlettel kapcsolatos fő eredeményeket a $k = 3$ esetben értük el, mikor [83]-ban sikerült meghatározni az összes megoldást. Akkor ez áttörést jelentett, mivel korábban hasonló problémáknál csak legfeljebb kéttagú összegekre tudták az összes megoldást meghatározni, vagy egészen speciális helyzetben tudtak elemezni valamely $k \geq 3$ esetet.

A fejezet további részének felépítése a következő. Először áttekintjük [83] előzményeit, utána összefoglaljuk annak eredményeit és a legjelentősebb állítás bizonyításának lényegét, az alkalmazott módszereket. Végül [83] következményeit és hatását elemezzük.

Előzmények

A $2^{n_1} + 1 = x^2$ egyenlet egyetlen $(n_1, x) = (3, 3)$ nem negatív egész megoldása régóta ismert. Lebesque [44] munkájából következik, hogy a $2^{n_1} - 1$ Mersenne-féle szám csak akkor lehet teljes négyzet, ha $n_1 = 0$ vagy 1. (Később Gerono [21] ugyanezt igazolta

magasabb hatványokra.) Világos, hogy ezek az eredmények egyben megadják (2) $k = 2$ esetének, azaz a $2^{n_1} \pm 2^{n_2} = x^2$ egyenletnek az összes megoldását is. Rotkiewicz és Złotokowski [74] a

$$p^{n_1} + p^{n_2} + \cdots + p^{n_k} + 1 = x^2 \tag{3}$$

egyenletet vizsgálták, ahol p páratlan prím, $k > 1$, továbbá $n_1 > n_2 > \cdots > n_k \geq 1$. Az $1+3+3^\nu+3^{\nu+1}+3^{2\nu} = (2+3^\nu)^2$, $(\nu \geq 2)$ megoldáscsalád mellett az alábbi megoldásokat találták, feltéve hogy valamely s pozitív egészre $sn_k \leq n_{k-1}$ és $n_1 \leq 2sn_k$ teljesül.

- $s = 1$ esetén (3) nem megoldható;
- $s = 2$ mellett csak $1 + 7 + 7^2 + 7^3 = 20^2$ teljesül;
- ha $s = 3$, akkor (3)-nak két megoldása van: $1 + 3^2 + 3^8 + 3^9 + 3^{11} = 451^2$ és $1 + 3^3 + 3^{10} + 3^{13} + 3^{14} = 2537^2$;
- $s = 4$ esetén csak $1 + 3^2 + 3^8 + 3^9 + 3^{11} = 451^2$ a megoldás.

de Weger [96], a Baker módszert alkalmazva éles felső korlátot adott az

$$ax + by = z^2 \tag{4}$$

egyenletben az $x, y \in S$ és $z \in \mathbb{Z}^+$ ismeretlenek nagyságára, ahol S az adott $p_1, \ldots, p_s$ prímek által multiplikatíve generált, természetes számokból álló halmaz, $a, b \in \mathbb{Z}$, úgy hogy $p_i \nmid ab$ és az a, b számok $\gcd(a, b)$-vel jelölt legnagyobb közös osztója négyzetmentes. Ezen eredményt egy redukciós eljárással kombinálva, $(p_1, p_2, p_3, p_4) = (2, 3, 5, 7)$-re de Weger meghatározta (4), mindösszesen 388 darab megoldását $a = 1$ és $b = \pm 1$ esetén. Ezek közül a 23. és az 50. sorszámú adja vissza a fejezet elején említett $2^1 - 1 = 1^2$ és $2^3 + 1 = 3^2$ megoldásokat.

Ramanujan sejtését [73], miszerint a

$$2^k - 7 = x^2$$

egyenlet összes pozitív egész megoldása $(k, x) = (3, 1), (4, 3), (5, 5), (7, 11)$ és $(15, 181)$, Nagell [67] bizonyította. Az általánosított

$$2^k + D = x^2$$

Ramanujan-Nagell egyenlettel (ahol k és x az ismeretlenek adott $D \neq 0$ mellett) sokan fogalkoztak, többek között Beukers [5] is. Az ő munkáját felhasználtuk az 1. és 2. tételek bizonyításában. Míg Nagell bizonyítása ad hoc természetű, mivel a 7 prímszám specialitásán múlik, addig Beukers módszere általános, a hipergeometrikus függvények egy, a diofantikus approximációkra vonatkozó alkalmazása.

A $2^N \pm 2^M \pm 2^L = z^2$ egyenlet

Tekintsük most a

$$2^N \pm 2^M \pm 2^L = z^2 \tag{5}$$

egyenletet az N, M, L és z nem negatív egész ismeretlenekben. Jelölésében az indexelést megspórolandó tértünk át új változókra (2)-höz képest. Ezt az egyenletet sikerült teljes mértékben megoldani: [83]-ban explicite meghatároztuk az összes megoldást. Ez volt az első eset, amikor az egyenlet exponenciális részében három azonos alapú tag szerepelt általános körülmények között, azaz N, M és L viszonyára csak a természetes $N \geq M \geq L \geq 0$ feltétel volt előírva a szimmetria feloldására ott, ahol erre szükség volt. Világos, hogy (5) vagy a

$$2^n \pm 2^m \pm 1 = x^2 \tag{6}$$

vagy a

$$2^n \pm 2^m \pm 2 = x^2 \tag{7}$$

egyenletekre vezet. Amíg azonban (7) megoldása egyszerű ha modulo 4 tekintjük, akárcsak a $2^n \pm 2^m - 1 = x^2$ egyenleteket, addig

$$2^n + 2^m + 1 = x^2$$

gyökeinek meghatározása jóval bonyolultabb, és egyebek mellett Beukers [5] mély eredményeinek alkalmazását igényelte. Végül

$$2^n - 2^m + 1 = x^2$$

szintén Beukers [5] egy tételének segítségével lett tisztázva.

A fenti eredményeket röviden úgy összegezhetjük, hogy végtelen sok általánosított Ramanujan-Nagell típusú, azaz $2^k + D = x^2$ egyenletet sikerült megoldani. A (7) egyenletre vonatkozó állításokat itt nem részletezzük bizonyításuk egyszerűsége miatt, viszont (6) esetén az alábbi állításokat nyertük.

1. tétel. *(Szalay, 2002, [83].) Ha a pozitív n, m és x egészek az $n \geq m$ feltétellel kielégítik a*

$$2^n + 2^m + 1 = x^2 \tag{8}$$

egyenletet, akkor

- $(n, m, x) \in \{(2t, t+1, 2^t+1) \mid t \in \mathbb{N},\ t \geq 1\}$, *vagy* (8a)
- $(n, m, x) \in \{(5, 4, 7)\ ,\ (9, 4, 23)\}$. (8b)

A probléma, többek között, azért nehéz, mert az egy paraméterrel leírható végtelen sok (8a)-beli megoldás mellett van két sporadikus megoldás is. Érdekes módon, egy alkalmas transzformáció tulajdonságait figyelembe véve, az eredeti problémából származó, látszólag bonyolultabb egyenletrendszer vizsgálata vezetett a sikerhez.

Érdemes megjegyezni, hogy (8) olyan x páratlan számokat ír le, melyek négyzetének kettes számrendszerbeli alakja pontosan három 1 bitet tartalmaz. A tétel szerint az $x^2 = 101_2^2 = 11001_2$, $x^2 = 1001_2^2 = 1010001_2$, $x^2 = 10001_2^2 = 100100001_2$, ... végtelen sorozaton kívül csupán $x^2 = 111_2^2 = 110001_2$ és $x^2 = 10111_2^2 = 1000010001_2$ rendelkeznek a fenti tulajdonsággal.

2. tétel. *(Szalay, 2002, [83].) Amennyiben az n, m és x pozitív egészekre*

$$2^n - 2^m + 1 = x^2$$

áll fenn, akkor

- $(n, m, x) \in \{(2t, t+1, 2^t - 1) \mid t \in \mathbb{N},\ t \geq 2\}$, *vagy*
- $(n, m, x) \in \{(t, t, 1) \mid t \in \mathbb{N},\ t \geq 1\}$, *vagy*
- $(n, m, x) \in \{(5, 3, 5)\ ,\ (7, 3, 11)\ ,\ (15, 3, 181)\}$.

3. tétel. *(Szalay, 2002, [83].) Ha n, m és x pozitív egészek, $n \geq m$ és*

$$2^n + 2^m - 1 = x^2,$$

akkor $(n, m, x) = (3, 1, 3)$. Továbbá a

$$2^n - 2^m - 1 = x^2$$

egyenlet egyetlen pozitív egész n, m és x megoldását $(n, m, x) = (2, 1, 1)$ adja.

Ahogy már korábban említettük, az utolsó tétel könnyen igazolható, ezzel a továbbiakban nem foglalkozunk.

A 2. tétel következménye Beukers [5] alábbi tételének. Legyen $D \in \mathbb{N}$ páratlan szám. A $2^n - D = x^2$ egyenletnek kettő vagy annál több megoldása van az n és x pozitív egész ismeretlenekben akkor és csak akkor, ha $D = 7,\ 23$ vagy $2^k - 1$ $(k \geq 4)$. Továbbá

- ha $D = 7$ akkor $(n, x) = (3, 1),\ (4, 3),\ (5, 5),\ (7, 11),\ (15, 181)$;

- $D = 23$ esetén $(n, x) = (5, 3),\ (11, 45)$;
- végül a $D = 2^k - 1$ $(k \geq 4)$ feltétel mellett $(n, x) = (k, 1),\ (2k - 2, 2^{k-1} - 1)$.

Ezek után vázoljuk a legnagyobb érdeklődésre számot tartó, 1. tétel igazolását.

1. tétel bizonyításának gondolatmenete

Nevezzük (8a) megoldásait szabályosnak, ezektől eltérő esetekben kivételes megoldásokról beszélünk. A bizonyítás azon alapszik, hogy ha (n, m) egy megoldása (8)-nak, akkor

$$2^{2n-2m} + 2^{n-m+1} + 1 = \left(\frac{x^2 - 1}{2^m}\right)^2$$

alapján a

$$\tau\ :\ (n, m) \longmapsto (2n - 2m, n - m + 1), \quad (n > m)$$

leképezés indukál egy másikat, ami mindenképpen szabályos. A dolgozat újszerűségét alapvetően τ felhasználása jelenti. Belátható, hogy elegendő megmutatni azt, hogy pontosan kétszer fordul elő a

$$(n, m) \neq (n_1, m_1), \quad \tau(n, m) = \tau(n_1, m_1)$$

konstelláció. Az egyik legfontosabb észrevétel az, hogy a τ leképezés tulajdonságai lehetővé teszik, hogy a

$$\begin{aligned} 2^n + 2^m + 1 &= x^2, \\ 2^{n+d} + 2^{m+d} + 1 &= y^2 \end{aligned}$$

egyenletekből álló rendszerként fogjuk fel a problémát az n, m, d, x, y pozitív egész ismeretlenekben, ahol $2 \leq m \leq n$, továbbá a két egyenlet egyike szabályos, a másik kivételes megoldáshoz kapcsolódik. A gondolatmenet komplikáltabb része az, amikor az első egyenlet megoldása kivételes, ami a

$$2^{8k+D} + 2^{4k} + 1 = x^2 \tag{9}$$

egyenlet vizsgálatához vezet, ahol $D \geq 1$ páratlan egész, k pozitív egész. (9) ekvivalens az

$$\frac{x}{2^{\frac{D+8k}{2}}} - 1 = \frac{2^{4k} + 1}{2^{\frac{D+8k}{2}}\left(x + 2^{\frac{D+8k}{2}}\right)}$$

egyenlettel, melyre alkalmazzuk Beukers [5] most következő diofantikus approximációs tételét. Legyen p a 2-nek egy páratlan hatványa. Ekkor bármely x egész számra $|x/p^{0.5} - 1| > 2^{-43.5}/p^{0.9}$ teljesül.

Tehát

$$\frac{2^{-43.5}}{2^{(D+8k)\cdot 0.9}} < \frac{2^{4k} + 1}{2 \cdot 2^{D+8k}},$$

ahonnan $D < 32k + 430$ adódik. Ezt összevetve a D-re elemi úton kapott $D > 56k - 32$ egyenlőtlenséggel, $k \leq 19$ következik. Most Beukers [5] egy másik tételét (9)-re

alkalmazva, és figyelembe véve a k-ra kapott felső korlátot, $D \leq 19$ adódik. Végül számítógéppel ellenőrizve a lehetséges eseteket $(D, k, x) = (1, 1, 23)$ lesz (9) egyetlen megoldása a nehezebb ágon. (Egyszerűbb a helyzet, ha a második egyenlet kivételes.) $\diamondsuit$

Kapcsolódó újabb eredmények

A cikk megjelenését követően Luca [52] meghatározta a $p^a \pm p^b + 1 = x^2$ rokon egyenlet összes megoldását páratlan p prímszámok esetén. A bizonyítás alapvetően a Pell egyenletek elméletén alapszik. A szerző megemlíti, hogy az általánosabb $p^a \pm p^b \pm p^c = x^2$ alakú egyenlet megoldásához szükséges lenne kezelni a $p^a \pm p^b - 1 = x^2$ egyenleteket is, ám míg a két eset közül $p^a - p^b - 1 = x^2$-re vonatkozólag vannak részeredmények, addíg $p^a + p^b - 1 = x^2$ megoldásáról szinte semmi sem ismert. Később Le Maohua meghatározta $p^a - p^b + p^c = x^2$ [37] illetve $p^a - p^b - p^c = x^2$ [38] megoldásait, majd a $2 \mid a$ és $a \geq b \geq c \geq 0$ feltételek mellett megoldotta a $p^a + p^b - p^c = x^2$ egyenletet [39], ám a páratlan a esete még mindig nyitott.

Bennett, Bugeaud and Mignotte [6] azt vizsgálták, hogy a 2-es illetve 3-as számrendszerben mely teljes hatványokban van pontosan három darab 1-es számjegy úgy, hogy a többi számjegy 0. A kérdés ekvivalens az $x^a + x^b + 1 = y^q$ egyenlettel $x \in \{2, 3\}$ esetén ($q \geq 2$). A szerzők az algebrai számok logaritmusainak lineáris formáira vonatkozó Baker módszert használva explicite megadták a megoldások halmazát, majd a négy 1-es számjegy esetét vizsgálva a 2-es számrendszerben, megállapították, hogy a q kitevő legfeljebb 4 lehet. Ugyanebben a cikkben belátták, hogy $6^a + 2^b + 1 = y^q$ csak úgy teljesülhet ha $1 < q \mid 6$. Később Bennett [7] elemezte, hogy 3-as számrendszerben mely négyzetszámoknak illetve magasabb hatványoknak van pontosan három 0-tól különböző számjegye. A fenti szerzők mindannyian említésre méltó alapként tekintenek a (8) egyenletre és annak [83]-ban való megoldására.

Scott és Styre [76] a Pillai egyenlet $(-1)^u a^x + (-1)b^y = c$ alakú általánosításának vizsgálatában, többek között, felhasználja az 1. tétel eredményeit. A [77, 78] tanulmányokban Scott egyszerűbb, elemi bizonyítást ad az 1. tételre, valamint Luca $p^a \pm p^b + 1 = x^2$ egyenletre vonatkozó eredményére.

Arenas-Carmona, Berend és Bergelson megemlítik, hogy vizsgálataikban nagy fontossággal bírnak azok a $P(X)$ polinomok, melyekre a $2^{n_1} \pm 2^{n_2} \pm \cdots \pm 2^{n_k} = p(x)$ egyenlet végtelen sok $(n_1, n_2, \ldots, n_k, x)$ megoldással rendelkezik. Ward [95] megjegyzi, hogy egy problémája megoldásában használni lehetne az 1. tételt, de direkt bizonyítást ad a speciális helyzetre.

További cikkek [51, 99, 54, 18], valamint Guy *Unsolved Problems in Number Theory* című könyve [23] (251. oldal) hasonló exponenciális, vagy polinomiális-exponenciális egyenleteket tárgyalva említi meg az 1. tételt vagy hivatkozik a [83] dolgozatra.

1.2. Az $(a^n-1)(b^n-1)=x^2$ egyenlet

Tegyük ismét fel, hogy az (1) egyenlet polinomja egyváltozós, mégpedig $p(X)=X^2$. Amennyiben (1) bal oldalán a kitevőket egyenlőknek tekintjük (legyen mindegyik n), és feltesszük, hogy $k=4$, $u_1=u_4=1$ és $u_2=u_3=-1$, továbbá hogy $\xi_1=\xi_2\xi_3$, $\xi_4=1$, akkor a $(\xi_2^n-1)(\xi_3^n-1)=x^2$ diofantikus egyenlethez jutunk, melyet a továbbiakban az egyszerűség kedvéért

$$(a^n-1)(b^n-1)=x^2 \tag{10}$$

alakban használunk. A következőkben a (10) típusú egyenletre, illetve módosításaira vonatkozó eredményeket ismertetjük az előzményeivel és következményeivel összhangban. Vegyük észre, hogy ha ab, a, b és 1 egy negyedfokú polinom különböző gyökei, akkor (10) egy adott negyedrendű rekurzív sorozatban (másképpen: két másodrendű sorozat szorzatában) kérdezi a négyzetszámok előfordulását. Ez az értelmezés indokolja a most következő történeti áttekintést.

Előzmények

Lineáris rekurzív sorozatokban előforduló teljes hatványok vizsgálata hosszú múltra tekint vissza, valószínűleg Ogilvy [69] volt az első, aki közölte a Fibonacci sorozatban előforduló négyzetszámok problémáját. Ugyanez a kérdés egy év múlva megjelent a Fibonacci Quarterly hasábjain is, majd még egy évvel később Cohn [11, 12] és Wyler [98] egymástól függetlenül, elemi módszerrel igazolták, hogy a Fibonacci sorozatban csak a 0, 1 és 144 számok teljes négyzetek. A magasabb hatványok megjelenésével sokan foglakoztak, többek között London és Finkelstein [50], Pethő [70, 71], McLaughin [65],..., végül Bugeaud, Mignotte és Siksek [8] igazolta, hogy az előbbieken kívül 8 az egyetlen hatvány a Fibonacci sorozatban. Ők a legmodernebb eszközökkel (moduláris formák, három tagú lineáris formák logaritmusaira vonatkozó legújabb eredmények) kombinálták a korábbi megközelítéseket.

Általános másodrendű, vagy magasabbrendű $\{G_n\}$ rekurziók esetén is felvetődött a

$$G_n=x^q$$

egyenlőség kérdése az $n\geq 0$, x és $q\geq 2$ egészekben. Shorey és Stewart [79] illetve tőlük függetlenül Pethő [70] megmutatta, hogy ha $\{G_n\}$ másodrendű, akkor mindhárom változó felülről effektíve korlátos. Amennyiben magasabbrendű rekurzív sorozatokat tekintünk, akkor fel szokták tenni, hogy a sorozat karakterisztikus polinomjának van domináns gyöke. Shorey és Stewart [79] ebben az esetben igazolta, hogy q nem lehet akármilyen nagy. Ezt az eredményt Nemes és Pethő [68] kiterjesztette a

$$G_n=x^q+A(x)$$

esetre, ahol $A(X)$ egy adott egészegyütthatós polinom. A fenti eredmények elsősorban a Baker módszeren múlnak, és a q kitevőre vonatkozó felső korlátok olyan hatalmasak, hogy közvetlenül nem lehet őket használni az adott egyenlet tényleges megoldására.

Közben sok olyan eredmény született, amely különböző bináris rekurziókban meghatározta adott alakú figurális számok összességét, de magasabbrendű rekurziókban ritkán sikerült hasonló eredményeket elérni. Például McDaniel [64] bizonyos Lehmer sorozatokban és asszociáltjaikban le tudta írni a négyzetszámokat. Az ő vizsgálatai kongruenciákon, különböző Jacobi szimbólumok kiszámolásán és a sorozatok osztthatósági tulajdonságain alapulnak. Mivel (10) bal oldala, mint korábban már említésre került, felfogható úgy is, hogy két bináris rekurzió szorzata, azaz egy negyedrendű rekurzív sorozat, így (10) ezekben keresi a négyzetszámok előfordulását. Tehát a (10) típusú egyenletek felvetése, és megoldása új irányt hozott a kutatásokba. A kérdés azért nem könnyű, mert valamely c-hez relatív prím modulust véve $c^n - 1$ maradékai peridikusan 0-t vesznek fel. Ezt a szituációt tovább nehezítheti, ha (10) megoldható.

Az $(a^n - 1)(b^n - 1) = x^2$ alakú egyenletek

Legyenek $1 < a < b$ rögzített egész számok, és keressük (10), azaz az

$$(a^n - 1)(b^n - 1) = x^2$$

polinomiális-exponenciális diofantikus egyenlet gyökeit az n és x nem negatív egészekben. Az $(a, b) = (2, 3), (2, 5), (2, 6), (a, a^k)$ esetekben sikerült megadni (10) összes megoldását [81, 27]. Ezek a dolgozatok úttörő munkának is tekinthetők, mert érdemben elsőként fogalkoztak az $(a^n - 1)(b^n - 1) = x^2$ egyenlettel. A bizonyításokban a kvadratikus maradékok és primitív gyökök elméletét, valamint mások által már megoldott diofantikus egyenletekre vonatkozó eredményeket használtunk fel. Később általánosítottuk a korábbiak egy részét oly módon, hogy az a és b hatványalapokat nem rögzítettük, hanem bizonyos kongruenciáknak kellett eleget tenniük [34] . Itt főleg a Pell egyenletek megoldásainak tulajdonságait használtuk fel. Ez utóbbi cikk mintegy tíz évvel az első kettő után született, közben többen is érdeklődést mutattak a (10) típusú egyenletek iránt. Ennek köszönhetően a téma szakirodalma megnövekedett, köztük nagyon jelentős és általános eredmények is előfordulnak.

A következő részben megadjuk a [81, 27, 34] dolgozatok fő eredményeit.

4. tétel. *(Szalay, 2000, [81].) Nincs pozitív egészekből álló (n, x) megoldása a*

$$(2^n - 1)(3^n - 1) = x^2 \tag{11}$$

egyenletnek.

A bizonyításban a néggyel osztható kitevők jelentették a legnagyobb problémát. Belátható, hogy ekkor $n = k \cdot 4 \cdot 5^{\alpha-1}$ alakban írható ($1 \leq \alpha \in \mathbb{Z}$), továbbá (11) átalakítható a

$$\frac{2^n - 1}{5^\alpha} \cdot \frac{3^n - 1}{5^\alpha} = x_1^2$$

formára. Ezután a kvadratikus maradékok elméletét használva megmutattuk, hogy

$$\left(\frac{\frac{2^n-1}{5^\alpha}\cdot\frac{3^n-1}{5^\alpha}}{5}\right)=\left(\frac{3k}{5}\right)\left(\frac{k}{5}\right)=\left(\frac{3}{5}\right)=-1,$$

ahol $(\cdot/5)$ a megfelelő Legendre szimbólumot jelöli.

5. tétel. *(Szalay, 2000, [81].) A*

$$(2^n-1)(5^n-1)=x^2$$

egyenlet egyetlen pozitív egész megoldása $(n,x)=(1,2)$.

Az 5. tételnek van egy érdekes átfogalmazása: csak az $(n,x)=(0,1)$ pár elégíti ki a $\sigma(10^n)=x^2$ egyenletet, ahol $\sigma(\cdot)$ az osztók összege számelméleti függvényt jelenti.

A tétel igazolása a 4. tételéhez hasonló.

6. tétel. *(Hajdu – Szalay, 2000, [27].) A*

$$(2^n-1)(6^n-1)=x^2$$

diofantikus egyenletnek nincs pozitív egész (n,x) *megoldása.*

Az $(a,b)=(2,6)$ esetben a korábbiaktól eltérő más elemi fogásokra is szükség volt. Csak páros kitevő mellett érdekes az állítás. Az $n=4k+2$ esetben a megoldhatatlanság bizonyításához beláttuk, hogy $n=6w$ alakú kell hogy legyen valamely páratlan w-re, majd találtunk két olyan természetes számot – a 17-et és a 97-et –, hogy a

$$((2^6)^w-1)((6^6)^w-1)$$

sorozat egyik tagja sem kvadratikus maradék egyszerre mindkét modulusra. Végül ha $n=4\cdot k\cdot 5^{\alpha-1}$, akkor

$$\left(\frac{\frac{2^n-1}{5^\alpha}\cdot\frac{6^n-1}{5^\alpha}}{5}\right)=-1.$$

7. tétel. *(Hajdu – Szalay, 2000, [27].) Ha az* a, n, k *és* x *pozitív egészek* $(a,k>1,$ $kn>2)$ *kielégítik az*

$$(a^n-1)\left(a^{kn}-1\right)=x^2$$

egyenletet, akkor $(a,n,k,x)=(2,3,2,21)$ *vagy* $(3,1,5,22)$ *vagy* $(7,1,4,120)$.

2000-ben a [81] dolgozatban először csak a $(2^k-1)(2^{kn}-1)=x^2$ egyenletet oldottuk meg, később azonban sikerült ezen eredményt általánosítani [27], az előző tételnek megfelelően. Itt Chao Ko [9] illetve Ljunggren [49] egy-egy tételére alapoztuk a bizonyítást.

8. tétel. *(Lan – Szalay, 2010, [34].) Ha* $a \equiv 2 \pmod 6$ *és* $b \equiv 0 \pmod 3$ *akkor az*

$$(a^n-1)(b^n-1)=x^2$$

diofantikus egyenletnek nincs pozitív egészekből álló (n,x) *megoldása.*

9. tétel. *(Lan – Szalay, 2010, [34].) Tegyük fel, hogy* $b-1=s^2$ *négyzetszám. Ekkor* $a \equiv 2 \pmod{20}$ *és* $b \equiv 5 \pmod{20}$ *mellett az*

$$(a^n-1)(b^n-1)=x^2$$

egyenlet vagy nem oldható meg, vagy egyetlen lehetséges megoldása $(n,x)=(1,st)$, *ahol* $t=\sqrt{a-1} \in \mathbb{N}$.

A 8. tétel általánosítja a 4. és 6. tételeket és Le Maohua egy dolgozatát [40]. Megjegyezzük, hogy a 8. tétel az (a,b) párok mintegy 1/18 részét tudja kezelni, továbbá, hogy végtelen sok (a,b) pár tesz eleget a 9. tételben szereplő feltételeknek.

Az utóbbi két eredmény bizonyításában elsősorban az $u^2-Dv^2=1$ Pell egyenlet megoldásait leíró $u=\{u_n\}$ sorozat számelméleti tulajdonságait használtuk fel.

Kapcsolódó újabb eredmények

A 2000-ben megjelent két cikk nagy érdeklődést keltett. Pethő [72] jelentős fejleménynek értékelte, hogy új kutatási irányt sikerült nyitni a magasabbrendű rekurziókban előforduló teljes hatványok vizsgálata terén. A dolgozatok hatására többen kezdték el vizsgálni a (10) típusú egyenleteket. Fontos eredményeket publikált Cohn [13], a bizonyítások egy részében felhasználta a $v^4=du^2+1$ típusú egyenletekre vonatkozó saját eredményeit. Egyik tétele az $a^k=b^\ell$ feltétel mellett általánosítja a 7. tételt, majd $n=1,2$ és $4k$ mellett adja meg (10) megoldását. Megoldja továbbá a $2 \le a < b \le 12$ esetekre meghatározott egyenleteket. Nemrég Guo [22] továbbfejlesztette Cohn munkáját.

Az egyik legjelentősebb eredmény Luca és Walsh nevéhez fűződik, akik [62]-ben általános végességi tételt nyertek az $u_n v_n = x^q$ egyenletre, ahol $\{u_n\}$ és $\{v_n\}$ adott

bináris rekurziók. Mivel Corvaja és Zannier egy, az Altér tétellel igazolt eredményét használták, így állításuk ineffektív. Belátták továbbá, hogy a (10) egyenleteknek csak véges sok megoldása lehet rögzített alapokra. Emellett [62]-ben megadtak egy olyan eljárást, amellyel az $(a^n-1)(b^n-1)=x^2$ egyenletek általánosan kezelhetők az adott (a,b) párok többségére. Az algoritmusukat $2 \le a < b \le 100$ esetben demonstrálták, és mintegy 70 kivételes esettől eltekintve megoldották az egyenleteket. A kivételek közül később néhányat Li és Tang [46], valamint Li és Jin [47] kezelni tudtak.

2009-ben Le Maohua két cikket [40, 42] is közölt a $(2^n-1)(b^n-1)=x^2$ egyenletről. Megmutatta, hogy ha $b \mid 3$ teljesül, akkor az előbbi egyenletnek nincs megoldása, általánosítva ezzel a 6. tételt. Ugyanezzel a problémával foglalkozott még Li és Tang [45] is.

A (10) egyenlet $b=a+1$ speciális esetét vizsgálta Le Maohua [43], és Liang [48]. Az előbbi munka szükséges feltételt ad arra, hogy a vizsgált egyenletnek legyen megoldása, míg Liang belátta, hogy ha a maradéka 2 vagy 3 modulo 4, akkor az egyenlet nem lesz megoldható.

Több tanulmány [88, 92, 89, 91, 20, 31, 93] foglalkozik azzal, hogy a-ra és b-re olyan osztályokat keressen, melyekre (10) nem oldható meg. Az említett cikkek közül [88] az általánosabb $(a^n-1)(b^m-1)=x^2$ egyenletet tárgyalja, melynek az előzménye az, hogy Walsh [94] a 4. tételt általánosította: megmutatta, hogy a $(2^n-1)(3^m-1)=x^2$ egyenlet sem oldható meg. Szintén a különböző kitevőjű, általánosabb problémát elemzi He [28] is.

1.3. Rekurzív sorozatokban előforduló további polinomiális értékek

Ha (1)-ben a ξ_i $(i=1,...,k)$ értékek egy egészegyütthatós k-adfokú polinom gyökei és az u_i együtthatók alkalmasan választott algebrai számok, továbbá a kitevők megegyeznek, akkor (1) úgy is felfogható, hogy egy k-adrendű lineáris rekurzív egész sorozat $p(X_1, X_2, \ldots, X_t)$ polinomiális értékeit keressük. Esetünkben p legyen egyváltozós, de az így vizsgált $p(X)$-ről kicsit általánosabban feltehető, hogy egészértékű polinom, például $\binom{X}{3}$.

Tételezzük fel, hogy a $\{G_n\}$ bináris rekurziót a G_0, G_1 kezdeti értékek és a

$$G_n = AG_{n-1} + BG_{n-2} \qquad (n \ge 2) \tag{12}$$

képzési szabály határozza meg, ahol $G_0, G_1, A, B \in \mathbb{Z}$ kielégítik a $|G_0| + |G_1| > 0$ és $AB \neq 0$ feltételeket. Legyen továbbá α és β a

$$k(X) = X^2 - AX - B$$

karakterisztikus polinom két gyöke, valamint $k(X)$ diszkriminánsát jelölje $D = A^2+4B$, ahol feltesszük még, hogy $D \neq 0$ (azaz $\alpha \neq \beta$).

A $\{G_n\}$ sorozat asszociált $\{H_n\}$ sorozatára $H_n = AH_{n-1} + BH_{n-2}$, $(n \ge 2)$ teljesül a $H_0 = 2G_1 - AG_0$ és $H_1 = AG_1 + 2BG_0$ kezdeti értékekkel.

Legyen a továbbiakban $|B| = 1$. A [84] dolgozatban beláttuk, hogy a $G_0 = 0$ és $G_1 = 1$ kezdőértékekkel és a (12) relációval megadott rekurzió és asszociáltja rögzített együtthatók mellett csak véges sok $\binom{x}{3}$ típusú polinomiális értéket tartalmazhat. A bizonyítás Mordellnek [66] egy, az elliptikus egyenletekre vonatkozó ineffektív végességi tételén alapszik.

A cikkben megadtunk egy algoritmust is az összes $\binom{x}{3}$ polinomiális érték meghatározására rögzített $\{G\}$ illetve $\{H\}$ esetén, szintén feltételezve a $G_0 = 0$ és $G_1 = 1$ kezdőértékeket. Az eljárást a Fibonacci, Lucas ill. Pell sorozatokkal – melyek n-edik tagját rendre a szokásos F_n, L_n ill. P_n szimbólumokkal jelöljük – demonstráltuk.

10. tétel. *(Szalay, 2002, [84].) A $G_n = \binom{x}{3}$ és $H_n = \binom{x}{3}$ egyenletek mindegyikének csak véges sok megoldása van az $n \geq 0$ és $x \geq 3$ egészekben.*

11. tétel. *(Szalay, 2002, [84].)*

- *Ha $F_n = \binom{x}{3}$, akkor $(n, x) = (1, 3)$ vagy $(2, 3)$.*
- *$L_n = \binom{x}{3}$-ből $(n, x) = (1, 3)$ vagy $(3, 4)$ következik.*
- *A $P_n = \binom{x}{3}$ egyenletet csak $(n, x) = (1, 3)$ elégíti ki.*

Az algoritmus elliptikus egyenletekre vezeti vissza a problémát, melynek megoldására kifejlesztett számítógépes eljárások állnak rendelkezésre.

A [84] dolgozat eredményeinek kiterjesztését [82] tartalmazza, ahol az általánosabb

$$G_n = \frac{1}{d}(ax^3 + 3abx^2 + cx + (bc - 2ab^3))$$

egyenletet tárgyaltuk az $a \neq 0,\ d \neq 0$ feltételekkel, továbbá tetszőleges G_0, G_1 kezdőértékekkel. Az eljárás alkalmazásaként a Fibonacci sorozatban, a Lucas számok sorozatában és a Pell sorozatban megadtuk a $\sum_{i=1}^{x} i^2$ alakban előállítható tagokat. Mindezeken túl, elemi módszert alkalmazva mindhárom előbb említett sorozatban meghatároztuk az összes $\sum_{i=1}^{x} i^3$ formájú számot, továbbá a Fibonacci ill. Lucas sorozatban az $\binom{x}{4}$ típusú kifejezéseket.

Végül megemlítjük, hogy hasonló jellegű problémákkal foglalkozott Kovács [32, 33], Tengely [90], valamint Luca és Szalay [57]. Ez utóbbi dolgozat nem polinomiális, hanem exponenciális alakú kifejezést keresett a Fibonacci sorozatban. Megmutattuk, hogy csak véges sok $p^a \pm p^b + 1$ alakú 1-nél nagyobb Fibonacci szám létezik, ahol p rögzített prím, a, b pozitív egészek és $\max\{a, b\} \geq 2$.

2. fejezet

Polinomiális-exponenciális diofantikus egyenletrendszerek: diofantikus halmazok

Pozitív egész számok (vagy pozitív racionális számok) egy $\{a_1, \ldots, a_m\}$ halmazát diofantikus szám m-esnek nevezzük, ha bármely $1 \leq i < j \leq m$ esetén $a_i a_j + 1$ egész szám négyzete (vagy racionális szám négyzete). Nyilvánvalóan a kérdés $m \geq 3$ mellett érdekes, és egész számokból álló hármast hamar lehet keresni. Az első, érdekes módon racionális számnégyest Diofantosz adta meg:

$$\left\{\frac{1}{16}, \frac{33}{16}, \frac{17}{4}, \frac{105}{16}\right\}.$$

Fermat jegyezte az $\{1, 3, 8, 120\}$ halmazt, valószínűleg elsőként mutatva példát egész számokból álló diofantikus négyesre. Az idők folyamán sokan vizsgálták a kérdést, különböző variánsait, változatait, kiterjesztéseit. A későbbiekben mindig az egész számokra vonatkozó problémát tekintjük. Ma már ismert, hogy végtelen sok egészekből álló diofantikus számnégyes létezik. A témakör legnagyobb érdeklődésre számot tartó sejtése, hogy a $m = 5$ esetén nincsen egészekből álló diofantikus halmaz. Ezzel kapcsolatban a legerősebb eredmény Dujella [15] nevéhez fűződik, aki belátta, hogy $m = 6$ esetén egyáltalán nincs megoldás, míg $m = 5$ mellett legfeljebb véges sok diofantikus halmaz létezik melyek effektíve meghatározhatók.

A következőkben a diofantikus számhalmazok[1] két változatát vizsgáljuk, mindkét esetben új típusú problémákat vetettünk fel, és oldottuk meg részben. Az első esetben a négyzetszámok helyett egy adott másodrendű rekurzív sorozat tagjait tekintjük. Másodszor pedig adott típusú S-egységekkel helyettesítjük a négyzetszámokat. Bizonyos értelemben a négyzetszámoknál $m = 5$ volt a „kritikus érték", a bináris rekurziókra $m = 3$, a két prímszám által generált S-egységekre pedig $m = 4$ lesz a középpontban.

[1] A diofantikus halmaz fogalmát más értelemben is használják. Az értekezésben mindvégig a klasszikus diofantikus szám m-esek különböző variánsainak eleget tevő szám m-eseket értjük alatta.

Megemlítjük még, hogy egy eredményében és megoldási technikájában is különböző jellegű dolgozatot publikáltunk ([4]), ahol a klasszikus probléma négyzetszámait négyzetmentes számokra cseréltük fel. Beláttuk, hogy a természetes számoknak van olyan H végtelen részhalmaza, hogy tetszőleges, de véges sok H-beli számot véve azok szorzata eggyel megnövelve négyzetmentes lesz. Ugyanebben a dolgozatban megbecsültük H-nak $\mathbb{N}$-re vonatkozó aszimptotikus sűrűségét is. Egy brute force keresési algoritmus segítségével példát adtunk olyan 1229 elemű $H' \subset H$ halmazra, melynek elemei 10^8-nál kisebbek, és a H-ra előírt tulajdonsággal rendelkeznek. H' első elemei:

$$H' = \{1, 2, 5, 6, 9, 10, 14, 18, 21, 30, 33, 42, 45, 50, 64, 65, 77, 81, 82, 92, 100, \dots\}.$$

A konsruktív bizonyításban, ami a dolgozat egyik erénye, Luca és Shparlinski [56] egymás után következő egészek négyzetmentes magjai hányadosainak approximációjára vonatkozó tételét használtuk. Ezideig prímszámokra vonatkozó hasonló eredményről nincs tudomásunk.

2.1. Bináris rekurziókkal kapcsolatos diofantikus hármasok

Legyenek A és B nullától különböző egész számok, melyekre $D = A^2 + 4B \neq 0$ teljesül, és amelyek az együtthatói lesznek a

$$G_{n+2} = AG_{n+1} + BG_n, \qquad n \geq 0$$

rekurzióval definiált $\{G_n\}$ egész számokból álló sorozatnak ($G_0, G_1 \in \mathbb{Z}$ kezdőelemekkel). Legyen α és β a rekurzióhoz tartozó karakterisztikus $k(X) = X^2 - AX - B$ polinom két különböző gyöke. Ismert, hogy léteznek olyan $\gamma, \delta \in \mathbb{K} = \mathbb{Q}[\alpha]$ komplex számok, melyekre

$$G_n = \gamma\alpha^n + \delta\beta^n$$

teljesül minden n-re ($\gamma = (G_1 - \beta G_0)/(\alpha - \beta)$, $\delta = (G_1 - \alpha G_0)/(\alpha - \beta)$.)

Térjünk most vissza az 1. fejezet elején bevezetett

$$u_1\xi_1^{n_1} + u_2\xi_2^{n_2} + \cdots + u_k\xi_k^{n_k} = p(x_1, x_2, \dots, x_t)$$

egyenletre. Legyen az ennek jobb oldalán álló p polinom $t = 2$ változós, mégpedig

$$p(X_1, X_2) = X_1X_2 + 1.$$

A bal oldalon tekintsünk $k = 2$ tagot, ahol a kitevők közösek ($n_1 = n_2 = n$), a hatványalapok pedig a $k(X)$ karakterisztikus polinom gyökei ($\xi_1 = \alpha$, $\xi_2 = \beta$), továbbá legyen $u_1 = \gamma$, $u_2 = \delta$. Világos, hogy röviden $p(x_1, x_2) = G_n$ formában fogalmazható meg a kapott egyenlet. Ilyen egyenletből tekintsünk most hármat az alábbi módon:

$$\begin{aligned} p(a, b) &= G_x, \\ p(a, c) &= G_y, \\ p(b, c) &= G_z. \end{aligned}$$

Amennyiben ezt egyenletrendszerként fogjuk fel az a, b, c és x, y, z ismeretlenekben, akkor olyan diofantikus a, b, c hármasokat keresünk melyek a rögzített $\{G_n\}$ sorozat tagjait állítják elő. A tapasztalatok azt mutatják, hogy a legismertebb bináris rekurziók (Fibonacci sorozat, Lucas számok sorozata, Balansz számok) nem bővelkednek diofantikus hármasokban. (Nyilvánvalóan diofantikus párból végtelen sok van, például $a = 1$, $b = G_x - 1$ megfelel.) Másrészről viszont $G_n = 2^n + 1$ esetén könnyű észrevenni, hogy különböző $a = 2^{a_1}$, $b = 2^{b_1}$ és $c = 2^{c_1}$ hatványokkal végtelen sok diofantikus hármas adható meg. A megoldások számának sokszínűsége is rávilágít a probléma nehézségére. A fentiek alapján két kérdést teszünk fel.

- Melyek azok a másodrendű sorozatok melyekre végtelen sok diofantikus hármas létezik?
- Hogyan lehet meghatározni az összes diofantikus hármast egy adott sorozatra?

Véges vagy végtelen?

Az első kérdés tanulmányozása előtt egy fogalmat vezetünk be. A $\{G_n\}$ sorozatot nem degeneráltnak nevezzük, ha $\gamma\delta \neq 0$ és α/β nem egységgyök. A továbbiakban a nem degeneráltságon túl feltételezzük még, hogy $D > 0$, ekkor az általánosság megszorítása nélkül feltehetjük azt is, hogy $|\alpha| > |\beta|$.

Tehát a megoldások számosságát firtatva az

$$\begin{aligned} ab + 1 &= G_x, \\ ac + 1 &= G_y, \\ bc + 1 &= G_z \end{aligned} \tag{1}$$

egyenletrendszert vizsgáljuk az $1 \leq a < b < c$ és x, y, z nem negatív egész ismeretlenekben. A [19] cikkben az alábbi eredményre jutottunk.

12. tétel. *(Fuchs – Luca – Szalay, 2008, [19].) Legyen a $\{G_n\}$ bináris rekurzív sorozat nem degenerált és $D > 0$. Tegyük fel, hogy létezik végtelen sok a, b, c, x, y és z nem negatív egész az $1 \leq a < b < c$ feltétellel, melyekre*

$$\begin{aligned} ab + 1 &= G_x, \\ ac + 1 &= G_y, \\ bc + 1 &= G_z \end{aligned}$$

teljesül. Ekkor $\beta, \delta \in \{\pm 1\}$, $\alpha, \gamma \in \mathbb{Z}$.

Továbbá, véges sok a, b, c, x, y, z kivételtől eltekintve $\delta\beta^z = \delta\beta^y = 1$, és az alábbiak közül az egyik szükségszerűen igaz:

- *$\delta\beta^x = 1$, amikor γ vagy $\gamma\alpha$ négyzetszám;*
- *$\delta\beta^x = -1$, amikor $x \in \{0, 1\}$.*

Vegyük észre, hogy a tételben megfogalmazott végtelenségi követelmény megvalósítható, tekintsük erre a kérdésfeltevések előtti $G_n = 2^n + 1$ példát. A $D > 0$ feltétel a bizonyításban erősen ki van használva, mivel ekkor a sorozat karakterisztikus polinomjának van domináns gyöke. A vizsgálat fő eszköze ugyanis az Altér tétel egyik változata, ahol az ilyesfajta problémák kezelésénél egyik legfontosabb kritérium a domináns gyök létezése. Hasonlóan az Altér tételt használta Schlickewei és Schmidt [75] az

$$aG_x + bG_y + cG_z = 0$$

egyenlet megoldásainak elemzésére (a, b és c adott egészek). Az (1) rendszer ekvivalens az előzőhöz jellegében hasonló

$$(ab + 1 - G_x)^2 + (ac + 1 - G_y)^2 + (bc + 1 - G_y)^2 = 0$$

egyenlettel, amely három-három változójában polinomiális illetve exponenciális.

12. tétel bizonyításának gondolatmenete

Végtelen sok megoldást feltételezve, először megállapítjuk, hogy $x < y < z$ következik, tehát $z \to \infty$. Ha z elegendően nagy, akkor eleget tesz a $z < 2y + O(1)$ egyenlőtlenségnek. A továbbiakban különböztessük meg a $\delta\beta^z = 1$ és $\delta\beta^z \neq 1$ eseteket.

Ha $\delta\beta^z = 1$, akkor könnyen belátható, hogy $\beta = \pm 1$, $\delta = \pm 1$, $\alpha \in \mathbb{Z}$ és $\gamma \in \mathbb{Z}$ teljesül, továbbá, hogy $\delta\beta^y = \pm 1$ és $\delta\beta^x = \pm 1$ következik (ha z elég nagy). Mivel $\delta\beta^y = -1$ csak véges sok megoldást adhat, így $\delta\beta^y = 1$. Ekkor $\delta\beta^x = \pm 1$ vezet el a tételben megfogalmazott $\delta\beta^x$-re vonatkozó állításokhoz.

Ha $\delta\beta^z \neq 1$ teljesül, akkor legvégül ellentmondásra jutunk majd a feltételezett végtelen sok megoldással. Lényegében ez az ág jelenti magát a cikket, ahol mély eszközöket (Altér tétel, végesen generált multiplikatív csoportokra vonatkozó egységegyenletek megoldása, Puiseux-sor, algebrai számelméleti megfigyelések, polinomok tulajdonságai) kombinálunk. Az előzőek alapján feltekető, hogy $z > y$. Belátjuk, hogy ha $G_y > 1$, és z elég nagy, akkor létezik alkalmas $\kappa_0 \in (0, 1)$ konstans, hogy

$$\gcd(G_y - 1, G_z - 1) < |\alpha|^{\kappa_0 z}.$$

Ennek az egyenlőtlenségnek $x \to \infty$ a következménye, tehát x, y, z mindegyike a végtelenhez tart. Ekkor Fuchs [18] multirekurzív, domináns gyökkel rendelkező sorozatokra vonatkozó eredményéből következik, hogy

$$(G_x - 1)(G_y - 1)(G_z - 1) = (abc)^2 \tag{2}$$

végtelen sok megoldására abc felírható a $\sqrt{(G_x - 1)(G_y - 1)(G_z - 1)}$ Puiseux-sorában megjelenő egytagú $\alpha^x, \beta^x, \alpha^y, \beta^y, \alpha^z, \beta^z$ kifejezések lineáris kombinációjaként. Következésképpen olyan egységegyenlethez jutunk, ahol a megoldásokat az α és β számok által generált multiplikatív csoportban keressük. Ennek kezelése jelenti a tanulmány legnehezebb és leginkább munkaigényes részét.

Ezután két fő esetet választunk szét. Ha α és β multiplikatíve függetlenek, akkor x, y és z között bizonyos lineáris összefüggések fedezhetők fel, melyeket visszaírva az (1) rendszerbe, ellentmondásra jutunk. Amennyiben α és β multiplikatíve összefüggőek, akkor – többek között a skatulya-elv felhasználásával – belátjuk, hogy (2) összes megoldása véges sok $\mathbb{Z}^3$-beli egyenesen helyezkedik el. Ezen egyenesek egyike nyilvánvalóan végtelen sok megoldást tartalmaz, azaz léteznek olyan v_i, w_i $(i = 1, 2, 3)$ egészek, melyekre végtelen sok pozitív egész t értékre

$$x = v_1 t + w_1, \qquad y = v_2 t + w_2, \qquad z = v_3 t + w_3.$$

áll fenn. A multiplikatív összefüggőség miatt valamely ϱ számra $\alpha = \varrho^i$ és $\beta = \pm\varrho^j$ teljesül (i, j egészek), továbbá az előzőek miatt $G_x - 1$, $G_y - 1$ és $G_z - 1$ mindegyike ϱ^t polinomja lesz, melyek közül bármely kettőnek van közös gyöke, hiszen a három tag közül bármely kettő legnagyobb közös osztója elég nagy. A bizonyítás ezen ága a közös gyökök vizsgálatával ér véget. $\diamondsuit$

Az (1) egyenletrendszer megoldása adott $\{G_n\}$ esetén

A 12. tétel rávilágít arra, hogy a bináris rekurziók általában véges sok diofantikus hármast tartalmaznak. Mint láttuk, a bizonyítás azt vizsgálja, hogy mi a szükséges (ami egyben elégséges is) feltétele végtelen sok hármas létezésének. Jellegéből következően nem ad eljárást, hogyan lehet meghatározni az (1) egyenletrendszer nem kivételes esetekben előforduló véges sok megoldását. A Fibonacci sorozatra [58], majd később a Lucas számok sorozatára [59] megadtunk egy módszert, amely lehetővé tette (1) hatékony elemzését.

Az eljárás fő gondolata az, hogy ha van megoldás, akkor $\gcd(G_y - 1, G_z - 1) > \sqrt{G_z}$, tehát a szóban forgó legnagyobb közös osztó viszonylag nagy. Felhasználva a $\{G_n\}$ sorozat számelméleti és analitikus tulajdonságait, a legnagyobb közös osztó felülről jól becsülhető, és a két becslés összevetéséből ellentmondásra jutunk elegendően nagy z értékek mellett. A Fibonacci sorozatnál a kis és nagy z értékeket elválasztó határ kb. 150-nek adódott. A következő állítást bizonyítottuk.

13. tétel. *(Luca – Szalay, 2008, [58].) Nem léteznek olyan pozitív egész $a < b < c$ számok, melyekre*

$$\begin{aligned} ab + 1 &= F_x, \\ ac + 1 &= F_y, \\ bc + 1 &= F_z \end{aligned} \tag{3}$$

teljesülne, ahol $x < y < z$ pozitív egészek.

A Lucas számok sorozatára vonatkozó analóg állítás az, hogy csak $1 \cdot 2 + 1 = L_2$, $1 \cdot 3 + 1 = L_3$ és $2 \cdot 3 + 1 = L_4$ alkotnak diofantikus hármast. A két tétel bizonyításának gondolatmenete lényegében megegyezik, van azonban köztük egy alapvető különbség. [58]-ban felhasználjuk, hogy $F_n - 1$ felbontható kisebb indexű Fibonacci és Lucas számok szorzatára. $L_n - 1$ esetén hasonló faktorizáció csak páratlan indexű tagokra létezik. A felmerült nehézséget úgy küszöböljük ki, hogy a páros indexű tagokra felhasználjuk az $(L_n - 1) \mid F_{3n}$ tulajdonságot, ami valóban megfelelő, mert a később kiszámolandó legnagyobb közös osztókra elegendő felső becslést adni. A következőkben vázoljuk a 13. tétel bizonyítását.

13. tétel bizonyításának gondolatmenete

Legyen $\chi = \gcd(F_z - 1, F_y - 1)$. Először megmutattuk, hogy $\sqrt{F_z} < c$ (nyilván $c \mid \chi$), valamint $z \leq 2y$. Utána beláttuk, hogy

$$\chi \leq F_{\gcd\left(\frac{z-i}{2}, \frac{y-j}{2}\right)} L_{\gcd\left(\frac{z-i}{2}, \frac{y+j}{2}\right)} L_{\gcd\left(\frac{z+i}{2}, \frac{y-j}{2}\right)} L_{\gcd\left(\frac{z+i}{2}, \frac{y+j}{2}\right)},$$

ahol $i, j \in \{\pm 1, \pm 2\}$ értékei attól függenek, hogy z és y milyen maradékot adnak 4-gyel osztva. Rögzítsük most i-t és j-t, és tegyük fel, hogy

$$\gcd\left(\frac{z + \nu i}{2}, \frac{y + \mu j}{2}\right) = \frac{z + \nu i}{2d_{\nu,\mu}}$$

teljesül valamely $2d_{\nu,\mu}$ pozitív egészre, ahol ν, μ a ± 1 értékeket vehetik fel.

Ha most mindegyik $(z + \nu i)/2d_{\nu,\mu}$ legfeljebb $(z + \nu i)/10$, akkor a Fibonacci és Lucas sorozat tagjaira vonatkozó éles alsó és felső becslést használva,

$$\sqrt{F_z} < c \leq \chi \leq F_{(z+1)/10} L^3_{(z+1)/10}$$

alapján ellentmondásra jutunk. Egyébként valamelyik $d_{\nu,\mu}$ érték éppen 1, 2, 3 vagy 4. A négy eset mindegyikében egy lineáris összefüggést kapunk z és y között, amelyet felhasználva beláttuk, hogy (3) nem oldható meg, ha $z > 150$.

Végül számítógéppel ellenőriztük a $z \leq 150$ eseteket. (Megemlítjük, hogy [58] 2. tételének bizonyításából egy egyszerű eset vizsgálata véletlenül kimaradt, de ez nem érinti a 13. tétel állítását.) $\diamondsuit$

Érdemes megjegyezni, hogy a (3) egyenletrendszernek van két racionális $0 < a < b < c$ megoldása (x, y, z továbbra is nem negatív egészek):

$$(a, b, c; x, y, z) = (2/3, 3, 18; 4, 7, 10)\,,\ (9/2, 22/3, 12; 9, 10, 11)\,,$$

és mindmáig nem ismert, hogy rajtuk kívül van-e még más is.

A [58] és [59] cikkeket követve Alp, Irmak és Szalay [1] megvizsgálták a Balansz számokra vonatkozó diofantikus hármasok kérdését, és a Fibonacci sorozathoz hasonlóan ott sem találtak megoldást. Ezt általánosította a [30] dolgozat, ahol már

nem egy adott sorozatról, hanem sorozatok egy jól meghatározott, végtelen sok sorozattal rendelkező osztályáról tudtuk megmutatni, hogy nincs diofantikus hármasuk. A vizsgált sorozatok közös jellemzője a

$$G_n = AG_{n-1} - G_{n-2}$$

rekurzív formula, ahol $A \neq 2$ pozitív egész, a kezdőelemek pedig $G_0 = 0$ és $G_1 = 1$. A bizonyított állítás a következő.

14. tétel. *(Irmak – Szalay, közlésre elfogadva, [30].) Ha $A \neq 2$ egy pozitív egész szám, akkor nem léteznek olyan $1 \leq a < b < c$ egészek, melyekre*

$$\begin{aligned} ab+1 &= G_x, \\ ac+1 &= G_y, \\ bc+1 &= G_z \end{aligned}$$

mindegyike egyszerre teljesülne valamely $1 \leq x < y < z$ egészekre.

A bizonyítás a korábbiakhoz képest két újdonsággal szolgált. Először is, a sorozat tagjaira vonatkozó alsó és felső becslések bonyolultabbak voltak az A paraméter miatt. Emiatt a kis és nagy z értékeket elválasztó korlát túl nagy lett a korábbi módszer alapján, így finomítani kellett a becslést. Másodszor pedig, kis z esetén ($z \leq 138$) a számítógépes vizsgálat is nehezebbé vált, hiszen végtelen sok sorozatról van szó. Ez úgy lett feloldva, hogy egy A változójú $\{G_n(A)\}$ polinomsorozatként fogtuk fel a végtelen sok sorozat összességét, és beláttuk, hogy

$$a = \sqrt{\frac{(G_x(A)-1)\,(G_y(A)-1)}{G_z(A)-1}}$$

csak akkor lehet egész, ha $A \leq 2$. Végül az $A = 1$ esethez tartozó periodikus sorozat vizsgálata könnyű.

Kapcsolódó újabb eredmények

További kutatási irányt kapunk, ha egy adott $\{G_n\}$ sorozatra bevezetjük a $\{G\}$-távolság fogalmát. Egy w valós szám $\{G\}$-távolságán a

$$\|w\|_G = \min\{|w - G_n| : n \geq 0\}$$

kifejezést értjük. Ezzel a terminológiával élve, a Lucas számokra vonatkozó korábbi állítás azt mondja, hogy vannak olyan a, b, c egész számok, melyekre

$$\max\{\|ab\|_L, \|ac\|_L,\ \|bc\|_L\} \leq 1.$$

A fentiek inspirálták az olyan pozitív $a < b < c$ egészek tanulmányozását, melyekre $\|ab\|_G$, $\|ac\|_G$ and $\|bc\|_G$ mindegyike kicsi. Például a Fibonacci sorozatra megmutattuk [60], hogy

$$\max\{\|ab\|_F, \|ac\|_F, \|bc\|_F\} > \exp(0.034\sqrt{\log c}).$$

Ebből következik, hogy ha $\max\{\|ab\|_F, \|ac\|_F, \|bc\|_F\} \leq 2$, akkor $c \leq \exp(415.7)$, és a legnagyobb ilyen c az $(1, 11, 235)$ hármasban fordul elő a 222 megoldás közül. A Balansz számok $\{B_n\}$ sorozatára beláttuk [2], hogy csak $(a, b, c) = (1, 34, 1188)$ ad pontosan 1 $\{B\}$-távolságú ab, ac és bc hármast. Ehhez a Balansz számok eddig még nem vizsgált több tulajdonságát is fel kellett tárni.

További kérdés, hogy milyen becslést lehet adni azon (a, b, c) hármasok számosságára, melyekre az $\|ab\|_G$, $\|ac\|_G$, $\|bc\|_G$ távolságok nem nagyobbak egy előre megadott korlátnál. Vezessük be az

$$s(x) = \#\{(a, b, c) \in \mathbb{Z}^3 : 1 \leq a < b < c,\ \max\{\|ab\|_G, \|ac\|_G, \|bc\|_G\} \leq x\}$$

függvényt, melynek a viselkedését vizsgáltuk a Fibonacci sorozatra. [61]-ben megmutattuk, hogy ha $x \to \infty$ akkor $x^{3/2} \ll s(x) \leq x^{2+o(1)}$, továbbá igazoltuk, hogy $s(0) = 0$, $s(1) = 16$, $s(2) = 49$.

2.2. S-egységekkel kapcsolatos diofantikus négyesek

Legyen S a racionális $p_1, p_2, \ldots, p_r$ prímek egy adott halmaza. S-egységnek nevezünk minden

$$s = p_1^{\tau_1} p_2^{\tau_2} \cdots p_r^{\tau_r}$$

alakú racionális számot, ahol $\tau_i \in \mathbb{Z}$.

Az $\{a_1, \ldots, a_m\}$ pozitív egészekből álló halmazt S-diofantikus szám m-esnek hívjuk, ha

$$a_i a_j + 1 = s_{i,j}$$

S-egység bármely $1 \leq i < j \leq m$ mellett. Részletes vizsgálataink kizárólag az $|S| = 2$ esetre szorítkoznak, és arra keresünk választ, hogy létezik-e ekkor S-diofantikus négyes. Zieglerrel a következő sejtést fogalmaztuk meg.

15. `sejtés.` (*Szalay – Ziegler, 2013, [86].*) *Nincsenek olyan p és q prímek melyekre létezne $\{p, q\}$-diofantikus négyes.*

A sejtést számítógépes vizsgálatokon túl több irányból is megerősítettük úgy, hogy bizonyos speciális osztályokra sikerült bizonyítanunk ([85], [86]). Mielőtt ezek részletezésére rátérnénk, fontos megemlíteni, hogy Győry, Sárközy és Stewart [26] egy sejtése, melyet később Corvaja és Zannier [14], valamint tőlük függetlenül Hernandez és Luca [29] igazoltak, közvetlenül kapcsolódik az S-diofantikus m-esek problematikájához. A sejtés a következőt állította: ha $a < b < c$ pozitív egészekre $c \to \infty$,

akkor $(ab+1)(ac+1)(bc+1)$ legnagyobb prímfaktora is a végtelenhez tart. Eszerint rögzített S (amely nem csak kételemű lehet) esetén csak véges sok S-diofantikus hármas (következésképpen négyes) lehet. Mivel mindkét bizonyítás alapvetően az Altér tétel alkalmazásán múlik, ezért az eredmények ineffektívek, azaz nem adnak alsó korlátot c függvényében a legnagyobb prímtényezőre. (Megjegyezzük, hogy előzőleg Győry és Sárközy [25] bizonyították, hogy a sejtés igaz, ha a, b, c, b/a, c/a és c/b közül legalább egyiknek a maximális prímfaktora korlátos.) A legnagyobb prímfaktor növekedésére Luca [53] a következő becslést adta. Ha S rögzített prímek egy halmaza, akkor léteznek k_1 és k_2, S-től függő konstansok, hogy ha $0 < a < b < c$ és $c > k_1$ akkor

$$[(ac+1)(bc+1)]_{\bar{S}} > \exp\left(\frac{k_2 \log c}{\log\log c}\right)$$

teljesül, ahol $[\cdot]_{\bar{S}}$ az S-mentes részt jelöli.

Számnégyesekből származó

$$s_4 = \prod_{1\le i<j\le 4} (a_i a_j + 1)$$

szorzat esetén pontosabban lehet fogalmazni, ugyanis Stewart és Tijdeman [80] belátták, hogy s_4 legnagyobb prímtényezője legalább $k_3 \log\log \max_i\{a_i\}$, ahol k_3 egy effektíve meghatározható konstans.

Az általunk megfogalmazott sejtést egyrészt végtelen sok, bizonyos technikai feltételeknek eleget tevő p és q prímekre sikerült igazolni [85], másrészt az összes olyan p és q prímszámokra, melyek 4-gyel vett osztási maradéka 3 [86]. A pontos állítások a következők.

16. tétel. *(Szalay – Ziegler, 2013, [85].) Legyen $S = \{p, q\}$, ahol $p < q$ két különböző prím, és tegyük fel, hogy*

$$p^2 \nmid q^{\mathrm{ord}_p(q)} - 1, \qquad q^2 \nmid p^{\mathrm{ord}_q(p)} - 1.$$

Tegyük fel továbbá, hogy valamely $\xi > 1$ valós számra $q < p^\xi$ teljesül.

Ilyen feltételek mellett létezik olyan $C = C(\xi)$ konstans, hogy bármely $p, q > C$ prímek esetén nincs S-diofantikus négyes. A C konstans értékét a

$$C = \Psi(9; 2.142 \cdot 10^{22}\xi^3)$$

egyenlőség határozza meg, ahol $\Psi(k; x)$ az

$$x = \frac{y}{(\log y)^k}$$

egyenlet legnagyobb $y > 0$ valós megoldást jelöli.

Például $\xi = 2$ mellett $C = C(2) = 1.023 \cdot 10^{41}$ adódik.

Belátható, hogy a tétel technikai feltételeit, különös tekintettel a rendekre vonatkozó előírásokra, végtelen sok p és q prím teljesíti. Ebből következik, hogy a tétel értelmében végtelen sok $S = \{p, q\}$ halmazra nincs S-diofantikus négyes. A második állítás az alábbi megfogalmazású.

17. tétel. *(Szalay – Ziegler, 2013, [86].) Ha p és q különböző prímekre $p \equiv q \equiv 3 \pmod 4$ teljesül, akkor nem létezik $\{p, q\}$-diofantikus négyes.*

Megjegyezzük, hogy ha a 17. tételben szereplő páratlan p prím helyett 2-t veszünk és meghagyjuk a q-ra vonatkozó előírást, akkor analóg állítás igaz. Ezt az eredményt publikálás nyújtottuk be [87], ahol még azt is beláttuk, hogy nem létezik diofantikus négyes a $\{p, q\}$ halmazra ha $p = 2$ és $q < 10^9$, illetve függetlenül p és q maradékától modulo 4, $p < q < 10^5$ esetén sincs. Az újdonság a korábbiakhoz képest a lánctörtekkel való approximáció alkalmazása volt.

A következőkben vázoljuk az előbbi két tétel igazolását.

17. tétel bizonyításának gondolatmenete

A $p \equiv q \equiv 3 \pmod 4$ feltételt – a kvadratikus maradékok elméletét alkalmazva – a következő módon használjuk ki. Ha (a, b, c) egy S-diofantikus hármast alkot, azaz valamely nem negatív kitevőkre

$$\begin{aligned} ab + 1 &= p^{\alpha_1} q^{\beta_1}, \\ ac + 1 &= p^{\alpha_2} q^{\beta_2}, \\ bc + 1 &= p^{\alpha_4} q^{\beta_4}, \end{aligned}$$

akkor $\alpha_1, \alpha_2, \alpha_4$ közül legalább az egyik nulla, máskülönben

$$(p^{\alpha_1} q^{\beta_1} - 1)(p^{\alpha_2} q^{\beta_2} - 1)(p^{\alpha_4} q^{\beta_4} - 1) = (abc)^2$$

nem volna kvadratikus maradék modulo p. Hasonlóan $\beta_1, \beta_2, \beta_4$ egyike is nulla. Rátérve az (a, b, c, d) által alkotott feltételezett S-diofantikus négyesre, a

$$\begin{aligned} ab + 1 &= p^{\alpha_1} q^{\beta_1}, & bc + 1 &= p^{\alpha_4} q^{\beta_4}, \\ ac + 1 &= p^{\alpha_2} q^{\beta_2}, & bd + 1 &= p^{\alpha_5} q^{\beta_5}, \\ ad + 1 &= p^{\alpha_3} q^{\beta_3}, & cd + 1 &= p^{\alpha_6} q^{\beta_6} \end{aligned} \tag{4}$$

rendszer négy diofantikus hármast tartalmaz. Az előző megfigyelés értelmében az α_i és β_i kitevők között több 0 is lesz. A lehetséges variánsokat számba véve, közülük több könnyen végiggondolható elemi számelméleti megfontolásokkal. A legkomplikáltabb $\alpha_1 = \alpha_6 = 0$ lehetőség hosszas ellenőrzést igényelt, ahol további alesetek kerültek elő, ezeket [86]-ban egy táblázatban gyűjtöttünk össze. $\diamondsuit$

16. tétel bizonyításának gondolatmenete

A fő nehézséget az okozta, hogyan tudunk szoros összefüggéseket feltárni a (4) egyenletrendszerben szereplő kitevők között. Csak megfelelően nagy p és q prímekre (amelyektől ráadásul két további kritériumot is elvárunk) sikerült ezt megtenni.

Amennyiben létezik $\{p, q\}$-diofantikus négyes, akkor (4) megoldható. Bevezetve az $s_i = p^{\alpha_i} q^{\beta_i}$ jelöléseket ($i = 1, 2, \ldots, 6$), a (4) egyenletrendszerből három S-egységekre vonatkozó egyenletet nyerünk:

$$s_2 s_5 - s_3 s_4 = s_2 + s_5 - s_3 - s_4, \tag{5}$$

$$s_1 s_6 - s_3 s_4 = s_1 + s_6 - s_3 - s_4, \tag{6}$$

$$s_2 s_5 - s_1 s_6 = s_2 + s_5 - s_1 - s_6. \tag{7}$$

Ezek vizsgálata képezi a bizonyítás egyik alappillérét. Bár a harmadik egyenlet nem független az első kettőtől, hiszen azok különbsége, számelméleti szempontból további tulajdonságokat lehet nyerni belőle. A rendszerben szereplő S-egységek kitevőire különböző összefüggések, megszorítások figyelhetők meg, melyeket később a bizonyítás során felhasználunk.

A bizonyítás kezdetén Stewart és Tijdeman [80] ötletét követjük, amikor rendre a

$$\frac{c(bd+1)}{b(cd+1)}, \qquad \frac{(bd+1)(ac+1)}{ab(cd+1)}, \qquad \frac{(ab+1)(cd+1)}{(ac+1)(bd+1)}$$

kifejezések logaritmusainak becslésére alkalmazzuk a Baker-módszert. Míg ők Waldschmidt [97] eredményét használták, mi az újabb és élesebb Matveev-féle [63], valamint két algebrai szám logaritmusainak lineáris formáira vonatkozó Laurent, Mignotte, Nesterenko [36] által kidolgozott tételekkel dolgoztunk. Ezek kombinációinak az lett az eredménye, hogy elegendően nagy p és q mellett d-re a

$$\frac{\log d}{(\log \log d)^4} < 7.969 \cdot 10^{21} (\log p \log q)^3 \tag{8}$$

felső korlátot kapunk $\log p$ és $\log q$ függvényeként.

Ezután (8) segítségével megmutattuk, hogy ha $\alpha_i + \beta_i$ maximuma nagyobb p-nél, akkor p felülről becsülhető a 16. tételben korábban $C(\xi)$-vel jelölt kifejezéssel. Tehát ha $p > C(\xi)$, akkor $\max_i\{\alpha_i + \beta_i\}$ legfeljebb p, és ekkor (5), (6) és (7) bármelyikében p két legkisebb kitevője megegyezik, továbbá a harmadik legkisebb kitevő náluk legfeljebb 1-gyel nagyobb. Hasonló megfigyelés érvényes q kitevőire is.

Az (5) egyenlet kitevőinek elemzése alapján a következő táblázatba foglalt esetek fordulhanak elő.

Eset	α	β
1	$\alpha_2 = \alpha_5 \leq 1$	$\beta_3 = \beta_4 \leq 1$
2	$\alpha_2 = \alpha_5 \leq 1$	$\beta_3 = \beta_4 = \beta_2 - 1$
3	$\alpha_3 = \alpha_4 = \alpha_2 - 1$	$\beta_2 = \beta_5 = \beta_3 - 1$
4	$\alpha_3 = \alpha_4 = \alpha_2 - 1$	$\beta_2 = \beta_5 \leq 1$
5	$\alpha_3 = \alpha_4 \leq 1$	$\beta_2 = \beta_5 = \beta_3 - 1$
6	$\alpha_3 = \alpha_4 \leq 1$	$\beta_2 = \beta_5 = \beta_4 - 1 = 0$
7	$\alpha_3 = \alpha_4 \leq 1$	$\beta_2 = \beta_5 \leq 1$

A bizonyítás az egyes lehetőségek időnként hosszas vizsgálatával folytatódik. Ezután bevonjuk a (6) egyenletet is, így az előző hét esetből négyben ellentmondásra jutunk, a maradék három esetnél pedig további információkat kapunk. Végül (7) figyelembe vételével tudjuk lezárni a még függőben maradt ágakat. $\diamondsuit$

Irodalomjegyzék

[1] Alp, M. – Irmak, N. – Szalay, L., Balancing diophantine triples, Acta Univ. Sapientiae, **4** (2012), 11-19.

[2] Alp, M. – Irmak, N. – Szalay, L., Balancing diophantine triples with distance 1, közlésre elfogadva: Period. Math. Hung.

[3] Arenas-Carmona, L. – Berend, D. – Bergelson, V., Ledrappier's system is almost mixing of all orders, Ergodic Theory Dyn. Syst., **28** (2008), 339-365.

[4] Banks, W. D. – Luca, F. – Szalay L, A variant on the notion of a Diophantine s-tuple, Glasgow Math. J., **51** (2009), 83-93.

[5] Beukers, F., On the generalized Ramanujan-Nagell equation I., Acta Arithm., **38** (1981), 389-410.

[6] Bennett, M. A. – Bugeaud, Y. – Mignotte, M., Perfect powers with few binary digits and related diophantine problems, II., Math. Proc. Cambridge Phil. Soc., **153** (2012), 525-540.

[7] Bennett, M. A., Perfect powers with few ternary digits, Integers, **12** (2012), 1159-1166.

[8] Bugeaud, Y – Mignotte, M. – Siksek, S., Classical and modular approaches to exponential Diophantine equations I. Fibonacci and Lucas perfect powers, Annals Math., **163** (2006), 969-1018.

[9] Chao Ko, On the Diophantine equation $x^2 = y^n + 1$, $xy \neq 0$, Sci. Sinica (Notes), **14** (1965), 457-460.

[10] Chen, Xigeng – Le, Maohua, On the Diophantine equation $(x^m-1)(x^{mn}-1) = y^2$, J. Huaihua Teacher Coll., **20** (2001), 11-12.

[11] Cohn, J. H. E., On square Fibonacci numbers. J. London Math. Soc., **39** (1964), 537-540.

[12] Cohn, J. H. E., Square Fibonacci numbers, etc. Fibonacci Q., **2** (1964), 109-113.

[13] Cohn, J. H. E., The Diophantine equation $(a^n - 1)(b^n - 1) = x^2$, Period. Math. Hung., **44** (2002), 169-175.

[14] Corvaja, P. – Zannier, U., On the greatest prime factor of $(ab + 1)(ac + 1)$, Proc. Amer. Math. Soc., **131** (2003), 1705-1709.

[15] Dujella, A., There are only finitely many Diophantine quintuples, J. Reine Angew. Math., **566** (2004), 183-214.

[16] Evertse, J. H., Points on subvarieties of tori, A panorama of number theory, Cambridge, 2002, p. 214-230.

[17] Evertse, J. H. – Schlickewei, H. P. – Schmidt, W. M., Linear equations in variables which lie in a multiplicative group, Ann. Math., **155** (2002), 807-836.

[18] Fuchs, C., Polynomial-exponential equations involving multi-recurrences, Studia Sci. Math. Hung., **46** (2009), 377-398.

[19] Fuchs, C. – Luca, F. – Szalay, L., Diophantine triples with values in binary recurrences, Ann. Scuola Norm. Sup. Pisa Cl. Sci., **5** Vol. VII (2008), 579-608.

[20] Ge, Jian, On the exponential Diophantine equation $(a^n-1)(b^n-1) = x^2$, J. Xi'an Shioyu Univ. (Nat. Sci.), **27** (2012), 106-107.

[21] Gerono, C. G., Note sur la résolution en nombres entiers et positifs de l' équation $x^m = y^n + 1$, Nouv. Ann. Math. (2), **9** (1870), 469-471; **10** (1871), 204-206.

[22] Guo, Xiaoyan, A note on the diophantine equation $(a^n - 1)(b^n - 1) = x^2$, Period. Math. Hung., **66** (2013), 87-93.

[23] Guy, R. K., Unsolved Problems in Number Theory, Third Edition, Springer Verlag, 2004, (p. 251).

[24] Győry, K., Some recent applications of S-unit equations, Astérisque, **209** (1992), 17-38.

[25] Győry, K. – Sárközy, A., On prime factors of integers of the form $(ab + 1)(bc + 1)(ca + 1)$, Acta Arithm., **79** (1997), 163-171.

[26] Győry, K. – Sárközy, A. – Stewart, C. L., On the number of prime factors of integers of the form $ab + 1$, Acta Arithm., **74** (1996), 365-385.

[27] Hajdu, L. – Szalay, L., On the diophantine equations $(2^n - 1)(6^n - 1) = x^2$ and $(a^n - 1)(a^{kn} - 1) = x^2$, Period. Math. Hung., **40** (2000), 141-145.

[28] He, Guangrong, A note on the exponential Diophantine equation $(a^m-1)(b^n-1) = x^2$, Pure Appl. Math., **27** (2011), 581-585.

[29] Hernandez, S. – Luca, F., On the largest prime factor of $(ab+1)(ac+1)(bc+1)$, Bol. Soc. Mat. Mexicana (3), **9** (2003), 235-244.

[30] Irmak, N., – Szalay, L., Diophantine triples and reduced quadruples with the Lucas sequence of recurrence $u_n = Au_{n-1} - u_{n-2}$, közlésre elfogadva: Glas. Mat.

[31] Jiang, Ziguo – Cao, Xingbing, On the solution to Diophantine equation $[(10k_1 + 2)^n - 1][(10k_2 + 5)^n - 1] = x^2$, J. Aba Teachers Coll., **24** (2007), 124-125.

[32] Kovács, T., Combinatorial numbers in binary recurrences, Period. Math. Hung., **58** (2009), 83-98.

[33] Kovács, T., Combinatorial Diophantine Equations, PhD. thesis, 2011.

[34] Lan, L. – Szalay, L., On the exponential diophantine equation $(a^n-1)(b^n-1) = x^2$, Publ. Math. Debrecen, **77** (2010), 465-470.

[35] Laurent, M., Equations diophantiennes exponetielles, Invent. Math., **78** (1984), 299-327.

[36] Laurent, M. – Mignotte, M. – Nesterenko, Y, Formes linéaires en deux logarithmes et déterminants d'interpolation, J. Number Theory, **55** (1995), 285-321.

[37] Le, Maohua, The exponential diophantine equation $p^a - p^b + p^c = z^2$, J. Shaoyang Univ. (Sciences and Technology), **3** (2006), 1-2.

[38] Le, Maohua, The exponential Diophantine equation $p^a - p^b - p^c = z^2$, J. Foshan Univ., Nat. Sci., **25** (2007), 11-12.

[39] Le, Maohua, The exponential Diophantine equation $p^a + p^b - p^c = z^2$, J. Hubai Univ. Nat., **27** (2009), (oldalszám ismeretlen).

[40] Le, Maohua, A note on the exponential Diophantine equation $(2^n-1)(b^n-1) = x^2$, Publ. Math. Debrecen, **74** (2009), 403-405.

[41] Le, Maohua, The even integer solutions of Diophantine equation $(d^n-1)(b^n-1) = x^2$, J. Wuyi Univ. (Natural Science Edition), **23** (2009), 4-6.

[42] Le, Maohua, On the Diophantine equation $(2^n - 1)((6k)^n - 1) = x^2$, J. Zhoukou Norm. Univ., **26** (2009), 1-2.

[43] Le, Maohua, Conditions for the solubility of the Diophantine equation $(a^n-1)((a+1)^n - 1) = x^2$, J. Zhanjiang Norm. Coll., **31** (2010), (oldalszám ismeretlen).

[44] Lebesque, M., Sur l'impossibilité, en nombres entiers, de l'équation $x^m = y^2 + 1$, Nouv. Ann. Math. (1), **9** (1850), 178-181.

[45] Li, Zhaojun – Tang, Min, On the Diophantine equation $(2^n - 1)(a^n - 1) = x^2$, J. Anhui Norm. Univ., **33** (2010), 515-517.

[46] Li, Zhaojun – Tang Min, A remark on a paper of Luca and Walsh, Integers, **11** (2011), 827-832.

[47] Li, Zhaojun – Jin, Qiaoxiao, On the Diophantine equation $(9^n-1)(19^n-1)=x^2$, J. Sci. Teachers' Coll. Univ., **30** (2010), (oldalszám ismeretlen).

[48] Liang, Ming, On the Diophantine equation $(a^n-1)((a+1)^n-1)=x^2$, J. Math., **32** (2012), 511-514.

[49] Ljunggren, W., Some theorems on indeterminate equations of the form $(x^n-1)/(x-1)=y^q$ (Norvegian), Norsk Mat. Tidsskr., **25** (1943), 17-20.

[50] London, H – Finkelstein R., On Fibonacci and Lucas numbers which are perfect powers, Fibonacci Q., **5** (1969), 476-481.

[51] Luca, F., On the diophantine equation $p^{x_1}-p^{x_2}=q^{y_1}-q^{y_2}$, Indag. Mathem., **14** (2003), 207-222.

[52] Luca, F., The diophantine equation $x^2=p^a\pm p^b+1$, Acta Arithm., **112** (2004), 87-101.

[53] Luca, F., On the greatest common divisor of $u-1$ and $v-1$ with u and v near S-units, Monatsh. Math., **146** (2005), 239-256.

[54] Luca, F., Arithmetic properties of positive integers with fixed digit sum, Rev. Mat. Iberoamer., **22** (2006), 369-412.

[55] Luca, F., Ecuaciones Diofánticas, Caracas, Venezuela, ISBN: 978-980-261-100-3, 2008.

[56] Luca, F. – Shparlinski, I. E., Approximating positive reals by ratios of kernels of consecutive integers, in Diophantine analysis and related fields, Sem. Math. Sci., **35** (Keio Univ., Yokohama, 2006). 141-148.

[57] Luca, F. – Szalay, L., Fibonacci numbers of the form $p^a\pm p^b+1$, Fibonacci Q., **45** (2007), 98-103.

[58] Luca, F. – Szalay, L., Fibonacci diophantine triples, Glas. Mat., **43 (63)** (2008), 253-264.

[59] Luca, F. – Szalay, L., Lucas diophantine triples, Integers, **9** (2009), 441-457.

[60] Luca, F. – Szalay, L., On the Fibonacci distances of ab, ac and bc, Annal. Math. Inf., **41** (2013), 137-163. (Proceedings of the 15^{th} International Conference on Fibonacci Numbers and Their Applications).

[61] Luca, F. – Szalay, L., On the counting function of triples whose pairwise products are close to Fibonacci numbers, Fibonacci Q., **51** (2013), 228-232.

[62] Luca, F. – Walsh, P. G., The product of like-indexed terms in binary recurrences, J. Number Theory, **96** (2002), 152-173.

[63] Matveev, E. M., An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic numbers, II, Izv. Ross. Akad. Nauk Ser. Mat., **64** (2000), 125-180.

[64] McDaniel, W. L., Square Lehmer numbers, Colloq. Math., **66** (1993), 85-93.

[65] Mc Laughlin, J., Small prime powers in the Fibonacci sequence, arXiv:math.-NT/0110150 v2 (2002).

[66] Mordell, L. J., On the integer solutions of the equation $ey^2 = ax^3 + bx^2 + cx + d$, Proc. London Math. Soc., **21** (1923), 415-419.

[67] Nagell, T., The Diophantine equation $x^2+7 = 2^n$, Norsk Mat. Tidsskr., **30** (1948), 62-64; Ark. F. Mat., **4** (1960), 185-187.

[68] Nemes, I. – Pethő, A., Polynomial values in linear recurrences I., Publ. Math. Debrecen, **31** (1984), 229-233.

[69] Ogilvy, S. C., Tomorrow's math, unsolved problems for the amateur. Oxford University Press, New York, 1962, p. 100.

[70] Pethő, A., Perfect powers in second order linear recurrences, J. Number Theory, **15** (1982), 5-13.

[71] Pethő, A., Full cubes in the Fibonacci sequence, Publ. Math. Debrecen, **30** (1983), 117-127.

[72] Pethő, A., Diophantine properties of linear recursive sequences II., Acta Math. Acad. Paed. Nyházi., **17** (2001), 81-96.

[73] Ramanujan, S., Collected papers, Cambridge Univ. Press, 1927, p. 327.

[74] Rotkiewicz, A. – Złotokowski, W., On the Diophantine equation $1 + p^{\alpha_1} + p^{\alpha_1} + \cdots + p^{\alpha_k} = y^2$, Colloq. Math. Soc. J. Bolyai, 51 Number Theory, Vol II., Eds.: Győry/Halász, North-Holland Publishing Company, Amsterdam - Oxford - New York, 1990, 917-937.

[75] Schlickewei, H. P. – Schmidt, W. M., Linear equations in members of recurrence sequences, Ann. Scuola Norm. Sup. Pisa Cl. Sci., **20** (1993), 219-246.

[76] Scott, R. – Styre, R., On the generalized Pillai equation $\pm a^x \pm b^y = c$, J. Number Theory, **118** (2006), 236-265.

[77] Scott, R., Elementary treatment of $p^x \pm p^y + 1 = x^2$, ArXiv:math/0608796v1 (2006).

[78] Scott, R. The equation $|p^x \pm q^y| = c$ in nonnegative x, y, ArXiv:1112.4548v1 (2011).

[79] Shorey, T. N. – Stewart, C. L., On the Diophantine equation $ax^{2t} + bx^t y + cy^2 = d$ and pure powers in recurrences, Math. Scand., **52** (1983), 24-36.

[80] Stewart, C. L. – Tijdeman, R., On the greatest prime factor of $(ab + 1)(ac + 1)(bc + 1)$, Acta Arith., **79** (1997), 93-101.

[81] Szalay, L., On the diophantine equation $(2^n - 1)(3^n - 1) = x^2$, Publ. Math. Debrecen, **57** (2000), 1-9.

[82] Szalay, L., Some polynomial values in binary recurrences, Rev. Col. Math., **35** (2001), 99-106.

[83] Szalay, L., The equation $2^N \pm 2^M \pm 2^L = z^2$, Indag. Mathem., **13** (2002), 131-142.

[84] Szalay, L., On the resolution of the equations $U_n = \binom{x}{3}$ and $V_n = \binom{x}{3}$, Fibonacci Q., **40** (2002), 9-12.

[85] Szalay L. – Ziegler, V., On an S-unit variant of diophantine m-tuples, Publ. Math. Debrecen, **83** (2013), 97-121.

[86] Szalay L. – Ziegler, V., S-Diophantine quadruples with two primes congruent to 3 modulo 4, Integers, **13** (2013), A80.

[87] Szalay L. – Ziegler, V., S-Diophantine quadruples with $S = \{2, q\}$, (közlésre benyújtva: Int. J. Number Theory).

[88] Tang, Min, A note on the exponential diophantine equation $(a^m - 1)(b^n - 1) = x^2$, J. Math. Res. Exposition, **31** (2011) 1064-1066.

[89] Tang, Bo – Yang, Shichun, Solutions on the Diophantine equation $((10k_1 + 2)^n - 1)((10k_2 + 3)^n - 1) = x^2$, Guangxi Sci., **14** (2007), (oldalszám ismeretlen).

[90] Tengely, Sz., On the Diophantine equation $L_n = \binom{x}{5}$, Publ. Math. Debrecen, **79** (2011), 749-758.

[91] Yang, Shichun – Wu, Wenquan – Zheng, Hui, On the solutions of the Diophantine equation $(a^n - 1)(b^n - 1) = x^2$, J. Southwest Univ. Nationalities (Nat. Sci. Ed.), **37** (2011), 31-34.

[92] Yuan, P. – Zhang, Z., On the diophantine equation $(a^n - 1)(b^n - 1) = x^2$, Publ. Math. Debrecen, **80** (2012), 327-331.

[93] Yuan, Wei, On the solutions of Diophantine equation $[(37k_1 + 6)^n - 1][(37k_2 + 31)^n - 1] = x^2$, China Sci. Techn. Inform., **9** (2009), 5.

[94] Walsh, P. G., On the diophantine equations of the form $(x^n - 1)(y^n - 1) = z^2$, Tatra Mt. Math. Publ., **20** (2000), 87-89.

[95] Ward, H. N., Block designs with SDP parameters, Electron. J. Combin., **19** (2012), Research Paper P11.

[96] De Weger, B., The weighted sum of two S-units being a square, Indag. Mathem., **1** (1990), 243-262.

[97] Waldschmidt, M., Minorations de combinaisons linéaires de logarithmes de nombres algébriques, Canad. J. Math., **45** (1993), 176-224.

[98] Wyler, O., Solution of advanced problem 5080. Amer. Math. Monthly, **71** (1964), 220-222.

[99] Zannier, U., Diophantine equations with linear recurrences. An overwiev of some recent progress, J. Theo. Nombres Bordeaux, **17** (2005), 423-435. (p. 434.)

dc_871_14

dc_871_14

3. Dolgozatok: polinomiális-exponenciális diofantikus egyenletek

dc_871_14

László Szalay

The equations $2^N \pm 2^M \pm 2^L = z^2$

Indag. Math., New Ser., 13 (2002), 131-142.

The equations $2^N \pm 2^M \pm 2^L = z^2$

László Szalay

1 Introduction

In the present paper we solve the title equations. It is easy to see that they lead either to

$$2^n \pm 2^m \pm 1 = x^2 \quad , \tag{1}$$

or to

$$2^n \pm 2^m \pm 2 = x^2 \quad . \tag{2}$$

While the examination of (2) is quite simple, as well as the resolution of $2^n \pm 2^m - 1 = x^2$, the equation

$$2^n + 2^m + 1 = x^2 \tag{3}$$

requires more calculations and the application of some deep results of Beukers [2]. This problem has been posed by professor Tijdeman, and I heard it from Tengely.

From a wider point of view, equations of types similar to (1) and (2) have already been investigated. Gerono [4] proved that a Mersenne-number $M_k = 2^k - 1$ cannot be a power of a natural number if $k > 1$, so the equation $2^k - 1 = x^2$ has only the solutions $(k, x) = (0, 0)$, $(1, 1)$. For another example, it can readily be verified that $2^k + 1 = x^2$ implies $(k, x) = (3, 2)$.

Ramanujan [7] conjectured that the diophantine equation

$$2^k - 7 = x^2 \tag{4}$$

has five solutions, namely $(k, x) = (3, 1)$, $(4, 3)$, $(5, 5)$, $(7, 11)$ and $(15, 181)$. His conjecture was first proved by Nagell [6]. The generalized Ramanujan-Nagell equation

$$2^k + D = x^2 \tag{5}$$

in natural numbers k and x, where $D \neq 0$ is an integer parameter, was considered by several authors. See, for example, Apéry [1], Hasse [5], Beukers [2]. Taking $D = \pm 2^M \pm 2^L$, we investigate infinitely many generalized Ramanujan-Nagell equations.

Our main result is Theorem 1. Theorems 1 and 2 have interesting consequences connected to binary recurrences (Corollary 1). Finally, a corollary of Lemma 5 states that the ratio of two distinct triangular numbers cannot be a power of 4 (Corollary 2).

Acknowledgements. The author would like to thank professor Attila Pethő for the useful discussion we had on this subject matter. Further, thanks are also due to professors Robert Tijdeman and Yann Bugeaud for their kind help, and to the referee for the valuable remarks and suggestions.

2 Results

Theorem 1. If the positive integers n, m and x with $n \geq m$ satisfy

$$2^n + 2^m + 1 = x^2 \quad , \tag{6}$$

then
(i) $(n, m, x) \in \{(2t, t+1, 2^t+1) \mid t \in \mathbb{N},\ t \geq 1\}$ or
(ii) $(n, m, x) \in \{(5, 4, 7)\ ,\ (9, 4, 23)\}$.

Remarks.

I. Equation (6), essentially, asks for odd natural numbers x whose squares contain exactly three 1 digits with respect to the base 2. Theorem 1 says that beside the infinite set $x^2 = 101_2^2 = 11001_2$, $1001_2^2 = 1010001_2$, ..., only $x^2 = 111_2^2 = 110001_2$ and $x^2 = 10111_2^2 = 1000010001_2$ possess the property above.

II. The solutions (i) and (ii) in Theorem 1 enable to determine all $n, m \in \mathbb{Z}$, $x \in \mathbb{Q}$ satisfying (6).

Theorem 2. If the positive integers n, m and x satisfy

$$2^n - 2^m + 1 = x^2 \quad , \tag{7}$$

then
(i) $(n, m, x) \in \{(2t, t+1, 2^t-1) \mid t \in \mathbb{N},\ t \geq 2\}$ or
(ii) $(n, m, x) \in \{(t, t, 1) \mid t \in \mathbb{N},\ t \geq 1\}$ or
(iii) $(n, m, x) \in \{(5, 3, 5)\ ,\ (7, 3, 11)\ ,\ (15, 3, 181)\}$.

Theorem 3. If the positive integers n, m and x with $n \geq m$ satisfy

$$2^n + 2^m - 1 = x^2 \quad , \tag{8}$$

then
(i) $(n, m, x) = (3, 1, 3)$.
Moreover, all the solutions of the equation

$$2^n - 2^m - 1 = x^2 \tag{9}$$

in positive integers n, m and x are given by
(ii) $(n, m, x) = (2, 1, 1)$.

One can find lots of results concerning occurrence of squares and higher powers in binary (or higher order) recurrences. See, for instance, Shorey, Tijdeman [8], Chapter 9. Corollary 1 determines all square terms in certain binary recursive sequences.

Corollary 1. (Corollary of Theorems 1 and 2.) Let d be an arbitrarily fixed natural number. Consider the binary recurrences

$$G_m = 3G_{m-1} - 2G_{m-2} \quad (m \geq 2)\ , \quad G_0 = 2^d + 2\ ,\ G_1 = 2^{d+1} + 3\ ; \tag{10}$$

$$H_m = 3H_{m-1} - 2H_{m-2} \quad (m \geq 2)\ , \quad H_0 = 2^d\ ,\ H_1 = 2^{d+1} - 1\ . \tag{11}$$

(i) The only square occurring in the recursive sequence G is G_{d+2}, except for the following two cases. If $d = 1$, then G contains three squares, namely G_0, $G_3 = G_{d+2}$ and G_4. If $d = 5$, then G_4 and $G_7 = G_{d+2}$ are the squares in G.

(ii) If d is odd, then

$$H_m = w^2 \tag{12}$$

implies $m = d + 2$. If $d > 0$ is even, then equation (12) has exactly two solutions given by $m = 0$ and $m = d + 2$, except for three cases $d = 2, 4, 12$ when there is an additional square, viz. H_3.

The second corollary contributes to the colorful palette of the results concerning triangular numbers.

Corollary 2. (Corollary of Lemma 5.) Let $\triangle_k$ denote the k^{th} triangular number, i.e. $\triangle_k = \frac{k(k+1)}{2}$, $k \geq 1$, $k \in \mathbb{N}$. Then the diophantine equation

$$\frac{\triangle_y}{\triangle_x} = 4^t \quad , \quad y \neq x \tag{13}$$

has no solution in natural numbers x, y and t.

3 Preliminaries

Lemma 1. Let $D_1 \in \mathbb{Z}$, $D_1 \neq 0$. If $|D_1| < 2^{96}$ and $2^n + D_1 = x^2$ has a solution (n, x) then

$$n < 18 + 2\log_2 |D_1| \quad . \tag{14}$$

Proof. This is Corollary 2 in [2] due to Beukers.

Lemma 2. Let p be an odd power of 2. Then for all $x \in \mathbb{Z}$

$$\left| \frac{x}{p^{0.5}} - 1 \right| > \frac{2^{-43.5}}{p^{0.9}} \quad . \tag{15}$$

Proof. We refer again to Beukers, [2].

Lemma 3. Let $D_2 \in \mathbb{N}$ be odd. The equation $2^n - D_2 = x^2$ has two or more solutions in positive integers n, x if and only if $D_2 = 7, 23$ or $2^k - 1$ for some $k \geq 4$. The solutions, in these exceptional cases, are given by the following table.

$D_2 = 7$	$(n, x) = (3, 1), (4, 3), (5, 5), (7, 11), (15, 181),$
$D_2 = 23$	$(n, x) = (5, 3), (11, 45),$
$D_2 = 2^k - 1$, $(k \geq 4)$	$(n, x) = (k, 1), (2k - 2, 2^{k-1} - 1).$

Proof. See Theorem 2 in [2].

Lemma 4. All natural solutions (n, x) of the inequalities

$$0 < |2^n - x^2| < 4 \tag{16}$$

in positive integers n and x are given by $(n, x) \in \{(1, 1), (2, 1), (3, 3), (1, 2)\}$.

Proof. In virtue of Lemma 1, $n < 22$ and the verification of all possible values n gives the solutions above. ■

Lemma 5. Let t be an arbitrary positive integer. If x and y are integers satisfying

$$y^2 - 1 = 2^{2t}\left(x^2 - 1\right) \quad , \quad y > 1 \ , \ x > 1 \quad , \tag{17}$$

then $x = 2^{t-1}$ and $y = 2^{2t-1} - 1$ for $t > 1$.

Proof. It is easy to see that (17) is not solvable if $t = 1$. Suppose that $t > 1$, $y > 1$ and $x > 1$ satisfy (17). Then y is odd and

$$\frac{y-1}{2} \cdot \frac{y+1}{2} = 2^{2t-2}\left(x^2 - 1\right) \quad . \tag{18}$$

The greatest common divisor of $\frac{y-1}{2}$ and $\frac{y+1}{2}$ is 1 and $2^{2t-2} (\geq 4)$ divides exactly one of the terms on the left hand side of (18). Consequently, $y = 2^{2t-1}k \pm 1$ with some integer $k \geq 1$. By (17) we have $y < 2^t x$, therefore $2^{t-1}k \leq x$. Moreover, it follows that

$$2^{2t-2}k^2 - k = x^2 - 1 \qquad \text{or} \qquad 2^{2t-2}k^2 + k = x^2 - 1 \quad . \tag{19}$$

In the first case, clearly, $k = 1$ provides the solution $x = 2^{t-1}$, $y = 2^{2t-1} - 1$. If $k > 1$, then the inequalities

$$x^2 = 2^{2t-2}k^2 - (k - 1) < 2^{2t-2}k^2 \leq x^2 \tag{20}$$

lead to contradiction.

In the second case of (19) it follows that

$$\left(2^{t-1}k\right)^2 < \left(2^{t-1}k\right)^2 + k + 1 = x^2 < \left(2^{t-1}k + 1\right)^2 \quad , \tag{21}$$

which is impossible. ■

Lemma 6. Let n, m and x be positive integers satisfying $2 \leq m < n$ and

$$2^n + 2^m + 1 = x^2 \quad . \tag{22}$$

Then $x = 2^{m-1}(2k+1) \pm 1$ with some $k \in \mathbb{N}$.

Proof. Assume that (n, m, x) is a solution of (22) under the assumptions made. For $m = 2$ the lemma trivially states that x is odd. If $m \geq 3$, then the congruence

$$x^2 \equiv 1 \pmod{2^m} \tag{23}$$

has exactly four incongruent solutions, namely $x \equiv 1$, $x \equiv 2^{m-1} - 1$, $x \equiv 2^{m-1} + 1$ and $x \equiv 2^m - 1 \pmod{2^m}$.

The first and fourth cases are impossible because, by (22), $x = 2^m l \pm 1$, ($l \in \mathbb{N}$, $l \geq 1$) leads to

$$2^{n-m} + 1 = 2^m l^2 \pm 2l \quad . \tag{24}$$

The second and third solutions of (23) provide

$$x = 2^{m-1}(2k+1) \pm 1 \quad , \quad (k \in \mathbb{N}) \quad . \tag{25}$$

■

Lemma 7. If n, m and x are natural numbers for which $m < n$ and $n < 2m - 2$, then

$$2^n + 2^m + 1 = x^2 \tag{26}$$

implies $(n, m, x) = (5, 4, 7)$.

Proof. The conditions of the lemma give $m \geq 4$. Suppose that (n, m, x) satisfy (26). Combining Lemma 6 and (26) we obtain

$$2^n + 2^m + 1 = r^2 2^{2m-2} \pm r2^m + 1 \quad , \tag{27}$$

where r is a positive odd integer. Since $2m - 2 \geq n + 1$, we get

$$2^m(1 \mp r) \geq (2r^2 - 1)2^n \quad . \tag{28}$$

Hence $r = 1$, $x = 2^{m-1} - 1$ and $n \leq m + 1$. By $m < n$ we have $n = m + 1$ and we can conclude that $m = 4$, $n = 5$ and $x = 7$. ■

Lemma 8. If D, k and x are positive integers, $k \geq 3$ and

$$2^{D+8k} + 2^{4k} + 1 = x^2 \quad , \tag{29}$$

then $D > 56k - 32$.

Proof.

Let $\nu_2(n)$ denote the 2-adic value of the integer n . Assume that the integers D, k and x satisfy the conditions of the lemma. By Lemma 6 we have two possibilities for x.

A) First consider the case $x = 2^{4k-1}(2u_0 + 1) + 1$, $(u_0 \geq 0)$. By (29) we obtain

$$2^{D+4k-1} = 2^{4k-3}\left(2u_0 + 1\right)^2 + u_0 \quad , \tag{30}$$

where u_0 must be positive and $u_0 = 2^{4k-3}u_1$ with some positive odd integer u_1. Otherwise, dividing (30) by $2^{\min\{4k-3,\nu_2(u_0)\}}$, it leads to contradition. In the sequel, this type of argument will be applied without any further notice. It follows that

$$2^{D+2} = 2^{8k-4}u_1^2 + 2^{4k-1}u_1 + (u_1 + 1) \quad . \tag{31}$$

Then $u_1 + 1 = 2^{4k-1}u_2$ for some suitable positive odd integer u_2, and by (31) we get

$$2^{D-4k+3} = 2^{4k-3}\left(2^{4k-1}u_2 - 1\right)^2 + 2^{4k-1}u_2 + (u_2 - 1) \quad . \tag{32}$$

Clearly, $u_2 \neq 1$, $u_2 - 1 = 2^{4k-3}u_3$, $(u_3 \in \mathbb{N}, u_3 \equiv 1 \pmod 2)$, further

$$2^{D-8k+6} = 2^{8k-2}\left(2^{4k-3}u_3 + 1\right)^2 - 2^{4k}\left(2^{4k-3}u_3 + 1\right) + 2^{4k-1}u_3 + (u_3 + 5) \quad . \tag{33}$$

It is easy to see that $u_3 + 5 = 2^{4k-1}u_4$, where u_4 is an odd natural number. Hence

$$\begin{aligned} 2^{D-12k+7} \;=\; & 2^{4k-1}\left(2^{4k-3}\left(2^{4k-1}u_4 - 5\right) + 1\right)^2 - \\ & -2^{4k-2}\left(2^{4k-1}u_4 - 5\right) + 2^{4k-1}u_4 + (u_4 - 7) \quad . \end{aligned} \tag{34}$$

By (34) we conclude that $u_4 - 7 = 2^{4k-2}u_5$. Here the odd integer $u_5 = \frac{u_4-7}{2^{4k-2}}$ is positive because $k \geq 3$ and $u_4 > 0$. It follows that

$$\begin{aligned} 2^{D-16k+9} \;=\; & 2^{8k-5}\left(2^{4k-1}\left(2^{4k-2}u_5 + 7\right) - 5\right)^2 + 2^{8k-2}\left(2^{4k-2}u_5 + 7\right) - \\ & -2^{8k-3}u_5 + (u_5 - 12)2^{4k-1} + (u_5 + 21) \quad . \end{aligned} \tag{35}$$

Finally, $u_5 + 21 = 2^{4k-1}u_6$, $(u_6 \in \mathbb{N}, u_6 \equiv 1 \pmod 2)$, and then $u_6 - 33 = 2^{4k-4}u_7$ leads to the equality

$$2^{D-24k+14} = \left(2^{4k-1}\left(2^{4k-2}Q_1 + 7\right) - 5\right)^2 + R_1 + S_1 \quad , \tag{36}$$

where

$$Q_1 = 2^{4k-1}\left(2^{4k-4}u_7 + 33\right) - 21 \quad , \quad R_1 = 2^3\left(2^{4k-2}Q_1 + 7\right) - 2^2Q_1 \quad , \tag{37}$$

$$S_1 = 2^3\left(2^{4k-4}u_7 + 33\right) + u_7 \quad , \quad u_7 \in \mathbb{N}\ ,\ u_7 \equiv 1 \pmod 2\ . \tag{38}$$

Obviously, $Q_1 > 2^{8k-5}$, $S_1 > 0$, $R_1 > 0$. Therefore $2^{D-24k+14} > 2^{32k-16}$ and

$$D > 56k - 30 \quad . \tag{39}$$

B) In the second case replace x by $2^{4k-1}(2u_0+1)-1$, $(u_0 \geq 0)$ in (29) and, similarly as above, the substitutions $u_0 = 2^{4k-3}u_1 - 1$, $u_1 = 2^{4k-1}u_2 + 1$, $u_2 = 2^{4k-3}u_3 - 1$, $u_3 = 2^{4k-1}u_4 + 5$, $u_4 = 2^{4k-2}u_5 - 7$, $u_5 = 2^{4k-1}u_6 + 21$ and $u_6 = 2^{4k-4}u_7 - 33$ lead to the equality

$$2^{D-24k+14} = \left(2^{4k-1}Q_2 + 5\right)^2 - 8Q_2 + R_2 \quad , \tag{40}$$

where

$$Q_2 = 2^{4k-2}\left(2^{4k-1}\left(2^{4k-4}u_7 - 33\right) + 21\right) - 7 \quad , \tag{41}$$

$$R_1 = 2^2\left(2^{4k-1}\left(2^{4k-4}u_7 - 33\right) + 21\right) - 2^3\left(2^{4k-4}u_7 - 33\right) - u_7 \quad , \tag{42}$$

and $u_7 \in \mathbb{N}\ ,\ u_7 \equiv 1 \pmod 2$. It can be proved that $Q_2 > 2^{12k-8}$, $R_2 > 0$ and we have $2^{D-24k+14} > 2^{32k-18}$, which, together with (39), implies $D > 56k - 32$. The proof of Lemma 8 is complete. ■

Lemma 9. If a and c are non-negative integers satisfying

$$a^2 + (a+1)^2 = c^2 \quad , \tag{43}$$

then $a = 2P_nP_{n+1}$, $a + 1 = P_{n+1}^2 - P_n^2$ or conversely, where P_k denotes the k^{th} term of the Pell sequence defined by $P_0 = 0$, $P_1 = 1$ and $P_k = 2P_{k-1} + P_{k-2}$, $(k \geq 2)$.

Proof. Probably this is an old result. For the proof see, for instance, Cohn [3]. ■

4 Proofs

Proof of Theorem 1. Obviously, each element of the set

$$T = \left\{(n,m) \in \mathbb{N}^2 \mid n = 2t, m = t+1, t \in \mathbb{N}, t \geq 1\right\} \tag{44}$$

(with some suitable $x \in \mathbb{N}$) satisfies the relations

$$2^n + 2^m + 1 = x^2 \quad , \quad n \geq m \geq 1 \quad . \tag{45}$$

Let S denote the set of solutions (n, m) of (45), further let $M_1 = (5, 4)$ and $M_2 = (9, 4)$. We have to show that the set of exceptional solutions is $S \setminus T = \{M_1, M_2\}$.

Observe that $2^{n-m} + 1 = \frac{x^2-1}{2^m} \in \mathbb{N}$ if $(n, m) \in S$, further

$$2^{2n-2m} + 2^{n-m+1} + 1 = \left(\frac{x^2 - 1}{2^m}\right)^2 \quad . \tag{46}$$

Hence a solution (n, m) of (45) provides $(2n - 2m, n - m + 1) \in S$, except when $2n - 2m < n - m + 1$, i.e. $n = m$. But Lemma 4 implies that the only solution (n, m) with $n = m$ is $(2, 2) \in T$.

In the sequel, we assume that $n > m$. Then the transformation

$$\tau \ : \ (n, m) \longmapsto (2n - 2m, n - m + 1) \quad , \quad (n > m) \tag{47}$$

induces a map of $S \setminus \{(2, 2)\}$ into S.

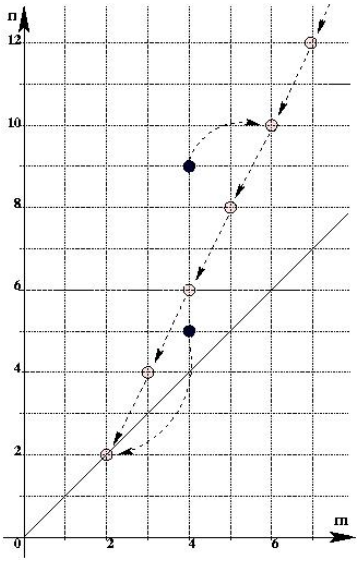

Figure 1: Map τ on the solutions of the equation $2^n + 2^m + 1 = x^2$

The map τ has important properties. If $(n, m) \in S$, then let $\delta(n, m)$ denote the distance $n - m$ of the exponents n and m.

Property 1. $\delta(\tau(n, m)) = \delta(n, m) - 1$. In particular, $\tau(n, m) \neq (n, m)$, i.e. the map has no fixed points.

Property 2. If $(n, m) \in T \setminus \{(2, 2)\}$, more precisely if $(n, m) = (2t, t + 1)$, $t \geq 2$, then $\tau(n, m) = (2(t - 1), t) \in T$ is the '*lower neighbour*' solution of (n, m) in T. Thus the elements of the set T are ordered by τ. Moreover $\delta(\tau(2t, t + 1)) = t - 2$, $(t \geq 2)$ shows that all natural numbers occur as a difference of the exponents in the solution of (45).

Property 3. If (n, m) is an exceptional solution (i.e. $(n, m) \in S \setminus T$), then $\tau(n, m) \in T$ since $\tau(n, m) = (2\delta(n, m), \delta(n, m) + 1)$. Especially, $\tau(5, 4) = (2, 2)$, $\tau(9, 4) = (10, 6)$.

If $m = 1$, then Lemma 4 implies a solution with $n < m$, which contradicts the assertion $n > m$.

Now suppose that the integers n and m satisfy $2 \leq m < n$ and (45). Reconsidering the map

$$\tau \ : \ S \setminus \{(2, 2)\} \longmapsto S \tag{48}$$

with (47), by Properties 1-3 we have to prove that there are exactly two cases when $(n, m) \neq (n_1, m_1)$ and $\tau(n, m) = \tau(n_1, m_1)$. In other words, we must show that the system of the equations

$$2^n + 2^m + 1 \ = \ x^2 \tag{49}$$

$$2^{n+d} + 2^{m+d} + 1 \ = \ y^2 \tag{50}$$

in positive integers n, m, d, x, y with $2 \leq m < n$ has exactly two solutions.

Taking such a solution, obviously both $x > 1$ and $y > 1$ are odd. It follows from (49) and (50) that

$$y^2 - 1 = 2^d \left(x^2 - 1\right) \quad , \tag{51}$$

and by Lemma 5 we infer that d must be odd.

Observe that one of (n, m) and $(n+d, m+d)$ has to belong to the set $T \setminus \{(2, 2)\}$. On the contrary, if both (n, m) and $(n + d, m + d)$ are exceptional, by the properties of the transformation τ there exists a solution $(n_2, m_2) \in T \setminus \{(2, 2)\}$ such that $\tau(n_2, m_2) = \tau(n, m) = \tau(n + d, m + d)$. But in this case one of the distances $|n_2 - n| = |m_2 - m|$ and $|n_2 - (n + d)| = |m_2 - (m + d)|$ has to be even since d is odd, which contradicts again to Lemma 5. Therefore, we distinguish two cases.

A) First let (50) be the exceptional case, consequently $(n, m) \in T \setminus \{(2, 2)\}$, and by (44) it follows that $n = 2m - 2$, which, together with (50), implies

$$2^{2m-2+d} + 2^{m+d} + 1 = y^2 \quad . \tag{52}$$

Here, if $m \geq 3$, then the exponents $m + d$ and $2m - 2 + d$ on the left hand side satisfy the conditions of Lemma 7. Thus we conclude that $m = 3$, $d = 1$, $y = 7$ is the only solution of (52) (and $n = 4$, $x = 5$ of (49)). It gives $M_1 \in S$. On the other hand, if $m = 2$, then $n = 2m - 2 \leq m$ leads to contradiction.

B) The second possibility is that (49) is the exceptional case, while $(n + d, m + d) \in T \setminus \{(2, 2)\}$, i.e. $n = 2m + d - 2$. Then by (49) we have

$$2^{2m+d-2} + 2^m + 1 = x^2 \quad . \tag{53}$$

It is easy to show that one of the exponents must be even in (53). Since d is odd, therefore m has to be even. Put $m = 2r$, where $r \in \mathbb{N}$, $r \geq 1$, and let $D = d - 2$. If $D = -1$, then (53) is equivalent to

$$2^{4r-1} + 2^{2r} + 1 = x^2 \quad . \tag{54}$$

Observe that the left hand side of (54) is a sum of $(2^{2r-1})^2$ and $(2^{2r-1}+1)^2$, hence $a = 2^{2r-1}$, $a+1$ and x form a Pythagorean triple. Since a is even, by Lemma 9 we have $2^{2r-1} = 2P_nP_{n+1}$ with some $n \in \mathbb{N}$. Therefore, both P_n and P_{n+1} are power of 2, which is impossible if $n \geq 2$ because P_n and P_{n+1} are coprime. Since $P_0 = 0$, the only possibility is $n = 1$, but $1 \cdot 2 \neq 2^{2r-2}$.

Consequently, $D \geq 1$ and we have

$$2^{D+4r} + 2^{2r} + 1 = x^2 \quad . \tag{55}$$

The left hand side of (55) is quadratic residue $\pmod 5$ if and only if r is even. Put $r = 2k$, ($k \in \mathbb{N}$, $k \geq 1$). Thus

$$2^{D+8k} + 2^{4k} + 1 = x^2 \quad , \tag{56}$$

which is equivalent to

$$\frac{x}{2^{\frac{D+8k}{2}}} - 1 = \frac{2^{4k}+1}{2^{\frac{D+8k}{2}}\left(x + 2^{\frac{D+8k}{2}}\right)} \quad . \tag{57}$$

Applying Lemma 2 to the left hand side of (57), and using that (56) gives $2^{\frac{D+8k}{2}} < x$, we obtain

$$\frac{2^{-43.5}}{2^{(D+8k)\cdot 0.9}} < \frac{2^{4k}+1}{2 \cdot 2^{D+8k}} \quad . \tag{58}$$

We see that $2^{4k} + 1 < 2^{4k+0.5}$ if $k \geq 1$, and by (58) it follows that

$$D < 32k + 430 \quad . \tag{59}$$

On the other hand, considering (56), Lemma 8 provides $D > 56k - 32$, which, together with (59) implies $k \leq 19$. Finally, applying Lemma 1 to (56) with $D_1 = 2^{4k} + 1$, ($k \leq 19$) we conclude that $D \leq 19$, too. A simple computer search shows that equation (56) with odd $D \leq 19$ and $k \leq 19$ has only one solution $D = 1$, $k = 1$, $x = 23$. Hence we obtain the third exceptional solution of (45): $(n, m) = (D + 8k, 4k) = (9, 4)$, and there are no others. So the proof of Theorem 1 is complete. ■

Proof of Theorem 2. Suppose that $(n, m, x) \in \mathbb{N}^3$ is a positive solution of the diophantine equation

$$2^n - 2^m + 1 = x^2 \quad . \tag{60}$$

Consider the case $n \geq m$. First let $m \geq 4$. Then (60) is equivalent to the equation

$$2^n - D_2 = x^2 \quad , \tag{61}$$

where the positive number $D_2 = 2^m - 1$ is odd. By Lemma 3, we find

$$(n, x) = (m, 1)\ ,\ (2m - 2, 2^{m-1} - 1) \tag{62}$$

as the set of all the solutions of (61) with $m \geq 4$. This result leads to the following solutions of (60):

$$(n, m, x) = (t, t, 1) \quad , \quad t \in \mathbb{N} \, , \, t \geq 4 \quad ; \tag{63}$$

$$(n, m, x) = (2t, t+1, 2^t - 1) \quad , \quad t \in \mathbb{N} \, , \, t \geq 3 \quad . \tag{64}$$

The famous case $m = 3$ of (60) has five solutions given by the table in Lemma 3. Among them $(n, m, x) = (3, 3, 1)$ can be joined to the set (63) with the parameter $t = 3$, moreover, $(n, m, x) = (4, 3, 3)$ to the set (64) with $t = 2$.

If $m = 2$ or $m = 1$, then Lemma 4 gives the result $(n, m, x) = (2, 2, 1)$ or $(n, m, x) = (1, 1, 1)$, respectively. These triplets may be added, for example, to (63) with $t = 2$ and with $t = 1$, respectively.

Finally, it is easy to see that (60) has no solution with $0 < n < m$. Avoiding the repetitions we may summarise the results above as Theorem 2 states. ■

Proof of Theorem 3. Assume that $(n, m, x) \in \mathbb{N}^3$ with $n \geq m > 0$ is a solution of the equation

$$2^n + 2^m - 1 = x^2 \quad . \tag{65}$$

If $m \geq 2$, then $2^n + 2^m - 1$ is a quadratic non-residue modulo 4; if $m = 1$, then apply Lemma 4 to have $(n, m, x) = (3, 1, 3)$.

Now suppose that $(n, m, x) \in \mathbb{N}^3$ is a solution of the equation

$$2^n - 2^m - 1 = x^2 \quad . \tag{66}$$

Clearly, $n > m$ and $m < 2$. For $m = 1$ apply Lemma 4 to prove the statement. ■

Proof of Corollary 1. Both sequences G and H have companion polynomial $c(x) = x^2 - 3x + 2$ with zeros $x = 2$ and $x = 1$. It is well known that the terms G_m (and H_m) can be expressed in explicit form. Here by $a_G = G_1 - G_0 = 2^d + 1$ ($a_H = H_1 - H_0 = 2^d - 1$) and by $b_G = -G_1 + 2G_0 = 1$ ($b_H = -H_1 + 2H_0 = 1$) we have

$$G_m = a_G 2^m + b_G = 2^{m+d} + 2^m + 1 \quad , \tag{67}$$

$$H_m = a_H 2^m + b_H = 2^{m+d} - 2^m + 1 \quad . \tag{68}$$

Thus to determine all the squares in the recurrences G and H is equivalent to solve the equations (6) and (7) with $n = m + d$ (i.e. $n \geq m$). ■

Proof of Corollary 2. $\triangle_y = 4^t \triangle_x$ ($y \neq x$, $y > 0$, $x > 0$) implies

$$y_1^2 - 1 = 4^t \left(x_1^2 - 1 \right) \quad , \tag{69}$$

where $y_1 = 2y + 1 \geq 3$ and $x_1 = 2x + 1 \geq 3$. In virtue of Lemma 5, (69) has no solution under the given conditions. ■

References

[1] Apéry, R., Sur une équation diophantienne, C. R. Acad. Sci. Paris Sér. A **261** (1960), 1263-1264.

[2] Beukers, F., On the generalized Ramanujan-Nagell equation I., Acta Arithm. **XXXVIII** (1981), 389-410.

[3] Cohn, E. M., Complete Diophantine solution of the Pythagorean triple $(a, b = a + 1, c)$, Fibonacci Quart., **8** (1970), 402-405.

[4] Gerono, C. G., Note sur la résolution en nombres entiers et positifs de l' équation $x^m = y^n + 1$, Nouv. Ann. Math. (2) **9**, (1870), 469-471; **10** (1871), 204-206.

[5] Hasse, H., Über eine diophantische Gleichung von Ramanujan-Nagell und ihre Verallgemeinerung, Nagoya Math. J., **27** (1966), 77-102.

[6] Nagell, T., The Diophantine equation $x^2 + 7 = 2^n$, Norsk. Mat Tidsskr. **30** (1948), 62-64; Ark. f. Mat. **4** (1960), 185-187.

[7] Ramanujan, S., Collected papers, Cambridge Univ. Press (1927), 327.

[8] Shorey, T. N. - Tijdeman, R., Exponential diophantine equation, Cambridge University Press, 1986, Chapter 9., 150-168.

dc_871_14

László Szalay

On the Diophantine equation $(2^n - 1)(3^n - 1) = x^2$

Publ. Math. Debrecen, 57 (2000), 1-9.

On the Diophantine equation $(2^n-1)(3^n-1)=x^2$

László Szalay

Abstract

This paper determines all the solutions of the diophantine equations $(2^n-1)(3^n-1)=x^2$, $(2^n-1)(5^n-1)=x^2$ and $(2^n-1)\left((2^k)^n-1\right)=x^2$ in positive integers n and x. The proofs depend on the theory of quadratic residuals in the case of the first two equations. For the third one we use a famous result of Ljunggren.

1 Introduction

In this paper we will study the title equation

$$(2^n-1)(3^n-1)=x^2 \tag{1}$$

in positive integers n and x. We will prove that it has no solution, and using the same method, the equation

$$(2^n-1)(5^n-1)=x^2 \tag{2}$$

will also be investigated. This equation has only one solution: $n=1, x=2$. We will also consider the equation

$$(2^n-1)\left(\left(2^k\right)^n-1\right)=x^2 \tag{3}$$

with $k>1$ ($k\in\mathbb{Z}$).

Let A_1, A_2, R_0, R_1 be integers and $R=R(A_1,A_2,R_0,R_1)$ be a second order linear recurrence defined by

$$R_n=A_1R_{n-1}+A_2R_{n-2} \qquad (n\geq 2) \quad . \tag{4}$$

With integer initial values G_0, G_1, G_2, G_3 and integer coefficients A_1, A_2, A_3, A_4, we also define a fourth order linear recursive sequence G by

$$G_n=A_1G_{n-1}+A_2G_{n-2}+A_3G_{n-3}+A_4G_{n-4} \qquad (n\geq 4) \quad . \tag{5}$$

Let recurrence (5) be denoted by $G(A_1,A_2,A_3,A_4,G_0,G_1,G_2,G_3)$. The terms 2^n-1, 3^n-1, 5^n-1 and $(2^k)^n-1$ satisfy the binary recurrence relations $R^{(2)}(3,-2,0,1)$,

$R^{(3)}(4,-3,0,2)$, $R^{(5)}(6,-5,0,4)$ and $R^{(2^k)}(2^k+1,-2^k,0,2^k-1)$, respectively. As well as the products $(2^n-1)(3^n-1)$, $(2^n-1)(5^n-1)$ and $(2^n-1)\left(\left(2^k\right)^n-1\right)$ satisfy the fourth order linear recursive relations

$$G^{(3)}(12,-47,72,-36,0,2,24,182),$$

$$G^{(5)}(18,-97,180,-100,0,4,72,868)$$

and

$$G^{(2^k)}(3(2^k+1),-(2^{2k+1}+9\cdot 2^k+2),6\cdot 2^k(2^k+1),2^{2k+2},0,2^k-1,3\cdot(2^{2k}-1),7\cdot(2^{3k}-1)),$$

respectively. Thus to solve the mixed exponential-polynomial diophantine equation (1) (or (2) or (3)) is equivalent to the determination of all perfect squares in a fourth order recurrence or in the products of the terms of two binary sequences. This new interpretation provides the equations

$$G_n^{(3)}=x^2 \qquad \text{or} \qquad R_n^{(2)}\cdot R_n^{(3)}=x^2 \quad , \tag{6}$$

$$G_n^{(5)}=x^2 \qquad \text{or} \qquad R_n^{(2)}\cdot R_n^{(5)}=x^2 \quad , \tag{7}$$

and with $k>1$

$$G_n^{(2^k)}=x^2 \qquad \text{or} \qquad R_n^{(2)}\cdot R_n^{(2^k)}=x^2 \quad . \tag{8}$$

In case of the fourth order recurrences only for some classes of Lehmer sequences of first an second kind are known to be similar results. In [6] McDaniel examined the existence of perfect square terms of Lehmer sequences and gained interesting theorems.

Many authors investigated the squares and pure powers in binary recurrences. Cohn [1] and Wyler [13], applying elementary method, proved independently that the only square in Fibonacci numbers are $F_0=0$, $F_1=F_2=1$ and $F_{12}=144$. For Lucas numbers Cohn [2] showed that if $L_n=x^2$ then $n=1,x=1$ or $n=3,x=2$. Pethő [7] gave all pure powers in the Pell sequence. In [10], under some conditions, Ribenboim and McDaniel showed that the square classes of the Lucas sequence $U(P,Q,0,1)$ contain at most 3 elements, except one case. Analogous results are established for the associate sequence V of U. In [11] the same authors determined – under some conditions – all squares in the sequences U and V.

There are more general result concerning pure powers in linear recurrences. Shorey and Stewart [12] proved that the terms of a non-degenerate recurrence sequence cannot be a q-th power for q sufficiently large if the characteristic polynomial of the sequence has a unique zero of largest absolute value. They, and as well as Pethő [8, 9], gained similar theorem for binary recurrences. Unfortunately, this general results gives no information about the low exponents, for example squares belonging to linear recurrences.

In the sequel we denote by $\nu_p(k)$ the p-adic value of integer k, where p is a fixed rational prime number. As usual, $\phi(k)$ denotes the Euler function, $d(k)$ denotes the number of divisors function, and $\sigma(k)$ the sum of divisors function.

2 Theorems

The following theorems formulate precisely the statements mentioned in the introduction. Some corollaries of the results are also described here.

Theorem 1. *The equation*

$$(2^n - 1)(3^n - 1) = x^2 \tag{9}$$

has no solutions in positive integers n and x.

Theorem 2. *The equation*

$$(2^n - 1)(5^n - 1) = x^2 \tag{10}$$

has the only solution $n = 1$, $x = 2$ in positive integers n and x.

Theorem 3. *The equation*

$$(2^n - 1)\left((2^k)^n - 1\right) = x^2 \tag{11}$$

has the only solution $k = 2$, $n = 3$, $x = 21$ in positive integers $k > 1$, n and x.

We have the following immediate consequences of Theorems 1 and 2.

Corollary A. *The equation $2 \cdot \sigma\left(6^n\right) = x^2$ has no solution, the equation $\sigma\left(10^n\right) = x^2$ has the only solution $n = 0$, $x = 1$.*

Proof of Corollary A. We need to use the well-known result of summatory function: $\sigma(k) = \prod_{p_i|k} \frac{p_i^{e_i+1}-1}{p_i-1}$, where $\nu_{p_i}(k) = e_i > 0$.

Corollary B. *The equation $\sum_{i,j=1}^{n} \phi\left(2^i \cdot 3^j\right) = x^2$ has no solution, the equation $\sum_{i,j=1}^{n} \phi\left(2^i \cdot 5^j\right) = x^2$ has only the solution $n = 1$, $x = 2$.*

Proof of Corollary B. These result follow from the multiplicitivity of Euler's ϕ function and from the equality $p^n - 1 = \phi(p^n) + \phi(p^{n-1}) + \cdots + \phi(p)$, where p is a prime number.

It is interesting to observe, that if one replaces Euler's ϕ function by the number of divisors function then for every primes p and q the sum

$$\sum_{i,j=1}^{n} d\left(p^i \cdot q^j\right) = \sum_{i,j=1}^{n} (i+1)(j+1) = \left(\sum_{k=2}^{n+1} k\right)^2 = \left(\frac{n(n+3)}{2}\right)^2 \tag{12}$$

is always a perfect square.

3 Preliminary Lemmas

In our work we shall require Lemma 1, which we state without proof. (For proof see e.g. [3], page 39.) Let $t > 1$ be an arbitrary integer and denote by $(\mathbb{Z}/t\mathbb{Z})^\star$ the multiplicative group of reduced residue classes modulo t.

Lemma 1. *Let $\alpha > 1$ be a rational integer and p be an odd prime number. If g is a primitive root of $(\mathbb{Z}/p\mathbb{Z})^\star$ then*
a) g is a primitive root of $(\mathbb{Z}/p^\alpha\mathbb{Z})^\star$ if $g^{p-1} \not\equiv 1 \pmod{p^2}$, and
b) $g(p+1)$ is a primitive root of $(\mathbb{Z}/p^\alpha\mathbb{Z})^\star$ if $g^{p-1} \equiv 1 \pmod{p^2}$.

Lemma 1 immediately implies the following results by the choice of
a) $p = 3$, $g = 2$ and $g = 5$;
b) $p = 5$, $g = 2$ and $g = 3$.

Corollary of Lemma 1. *If $\alpha > 1$ is a rational integer then*
a) the numbers 2 and 5 are primitive roots of $(\mathbb{Z}/3^\alpha\mathbb{Z})^\star$, and
b) the numbers 2 and 3 are primitive roots of $(\mathbb{Z}/5^\alpha\mathbb{Z})^\star$.

Lemma 2. *Let α and k be positive integers with $k \not\equiv 0 \pmod 5$. If $n = k \cdot 4 \cdot 5^{\alpha-1}$*

then

$$\nu_5\left((2^n-1)(3^n-1)\right)=2\alpha \quad . \tag{13}$$

Proof of Lemma 2. Let us consider the congruences

$$2^n\equiv 1 \pmod{5^\alpha} \qquad \text{and} \qquad 3^n\equiv 1 \pmod{5^\alpha} \quad , \tag{14}$$

where α is a fixed positive integer, and n is unknown. According to Corollary of Lemma 1b) and $\phi(5^\alpha)=4\cdot 5^{\alpha-1}$ we obtain the solutions $n=k\cdot 4\cdot 5^{\alpha-1}$ $(k=1,2,\dots)$ for both congruences. If $k\not\equiv 0 \pmod 5$ then

$$2^n\not\equiv 1 \pmod{5^{\alpha+1}} \qquad \text{and} \qquad 3^n\not\equiv 1 \pmod{5^{\alpha+1}} \quad . \tag{15}$$

So $\nu_5(2^n-1)=\alpha=\nu_5(3^n-1)$, which proves Lemma 2.

Lemma 3. *Let α and k be positive integers with $k\not\equiv 0 \pmod 3$. If $n=k\cdot 2\cdot 3^{\alpha-1}$ then*

$$\nu_3\left((2^n-1)(5^n-1)\right)=2\alpha \quad . \tag{16}$$

The proof of Lemma 3. is very similar to the previous one.

4 Proof of the Theorems

4.1 Proof of Theorem 1

Suppose that the pair (n,x) is a solution of equation (9). Since $2|(3^n-1)$ but $2\not|(2^n-1)$ for every positive integer n, it follows that $2|x$, $4|x^2$ and $4|(3^n-1)$. Consequently n is an even number, but in this case $8|(3^n-1)$ so $4|x$, $16|x^2$ and $16|(3^n-1)$. From the last relation and n is even it follows that n is divisible by 4 and can be uniqely written in the form $n=k\cdot 4\cdot 5^{\alpha-1}$, where $1\le\alpha\in\mathbb{Z}$ and $k\in\mathbb{Z}$, $k\not\equiv 0 \pmod 5$. Then applying Lemma 2, we transform (9) into the form

$$\frac{2^n-1}{5^\alpha}\,\frac{3^n-1}{5^\alpha}=x_1^2 \quad , \tag{17}$$

where $x_1 = \frac{x}{5^\alpha}$ and the prime 5 divides neither the left nor the right hand side of (17). The Legendre symbol $\left(\frac{x_1^2}{5}\right) = 1$ because of $\gcd(x_1, 5) = 1$. On the other hand

$$\left(\frac{\frac{2^n-1}{5^\alpha}\ \frac{3^n-1}{5^\alpha}}{5}\right) = A \cdot B \tag{18}$$

introducing the notation A and B for the Legendre symbols $\left(\frac{(2^n-1)/5^\alpha}{5}\right)$ and $\left(\frac{(3^n-1)/5^\alpha}{5}\right)$, respectively. We shall show that the calculation of A and B leads to a contradiction because the left side of (17) is not a quadratic residue modulo 5. More exactly, we shall prove that $A = \left(\frac{3k}{5}\right)$, $B = \left(\frac{k}{5}\right)$, so $AB = \left(\frac{3}{5}\right) = -1$. It means that the equation $(2^n - 1)(3^n - 1) = x^2$ has no solution in positive integers n and x. Now turn to the calculation of A and B.

Let $R = \alpha - 1$ and first let $k = 1$ (i.e. $n = 4 \cdot 5^R$). We are going to compute the residue of the expressions $\frac{2^{4\cdot 5^R}-1}{5^{R+1}}$ and $\frac{3^{4\cdot 5^R}-1}{5^{R+1}}$ after dividing them by 5.

a) If $R = 0$ then $\frac{2^4-1}{5} = 3 \equiv 3 \pmod 5$, and $\frac{3^4-1}{5} = 16 \equiv 1 \pmod 5$.

b) If $R = 1$ then

$$\frac{2^{4\cdot 5} - 1}{5^2} = \frac{(2^4 - 1)}{5}\frac{\left(1 + 2^4 + \cdots + (2^4)^4\right)}{5} = \frac{(2^4 - 1)}{5}\frac{Q_1}{5} \tag{19}$$

and

$$\frac{3^{4\cdot 5} - 1}{5^2} = \frac{(3^4 - 1)}{5}\frac{\left(1 + 3^4 + \cdots + (3^4)^4\right)}{5} = \frac{(3^4 - 1)}{5}\frac{Q_2}{5} \quad . \tag{20}$$

Since $Q_1 \equiv Q_2 \equiv 5 \pmod{5^2}$ therefore $\frac{Q_1}{5} \equiv \frac{Q_2}{5} \equiv 1 \pmod 5$ and $\frac{2^{4\cdot 5}-1}{5^2} \equiv 3 \cdot 1 = 3 \pmod 5$, $\frac{3^{4\cdot 5}-1}{5^2} \equiv 1 \cdot 1 = 1 \pmod 5$.

c) If $R > 1$ then replace 2^4 by y in the first case and replace 3^4 by y in the second case. Thus for both cases

$$\frac{y^{5^R} - 1}{5^{R+1}} = \tag{21}$$

$$= \frac{(y-1)(1 + y + \cdots + y^4)(1 + y^5 + \cdots + y^{4\cdot 5}) \cdots (1 + y^{5^{R-1}} + \cdots + y^{4\cdot 5^{R-1}})}{5^{R+1}}.$$

Observe that $y^5 \equiv 1 \pmod{5^2}$, so each factor of the numerator is divisible by 5, but none of them is divisible by 5^2, consequently $\frac{y^{5^R}-1}{5^{R+1}} \equiv m \cdot 1 \cdots 1 \pmod 5$, where $m = 3$ if $y = 2^4$ and $m = 1$ if $y = 3^4$.

These results make it possible to calculate the general case, when k is an arbitrary positive integer. Since $\frac{y^{5^R}-1}{5^{R+1}} \equiv m \pmod 5$, therefore

$$y^{5^R} \equiv 1 + m \cdot 5^{R+1} \pmod{5^{R+2}} \quad , \tag{22}$$

so

$$\left(y^{5^R}\right)^k \equiv \left(1 + m \cdot 5^{R+1}\right)^k \equiv 1 + k \cdot m \cdot 5^{R+1} \pmod{5^{R+2}} \quad , \tag{23}$$

which means that

$$\frac{y^{k \cdot 5^R} - 1}{5^{R+1}} \equiv k \cdot m \pmod 5 \quad . \tag{24}$$

Our result concerning A and B follows from the last congruence. ■

4.2 Proof of Theorem 2

Suppose that (n, x) is a solution of equation (10).

a) First we assume that n is even. Then n can be uniquely written in the form $n = k \cdot 2 \cdot 3^{\alpha-1}$, where $1 \leq \alpha \in \mathbb{Z}$ and $k \in \mathbb{Z}$, $k \not\equiv 0 \pmod 3$. According to Lemma 3 we may transform (10) into the form

$$\frac{2^n - 1}{3^\alpha} \, \frac{5^n - 1}{3^\alpha} = x_1^2 \quad , \tag{25}$$

where $x_1 = \frac{x}{3^\alpha}$ and $\gcd(x_1, 3) = 1$, $\gcd(\frac{2^n-1}{3^\alpha}, 3) = 1$ and $\gcd(\frac{5^n-1}{3^\alpha}, 3) = 1$. To finish the proof of case a) we have to use the same method step by step as we did above, during the proof of Theorem 1. We will show the insolubility of equation (10) by evaluating Legendre symbols of both sides of (10).

b) Let us continue the proof of Theorem 2 with the second case, when n is an odd integer.

If $n \equiv 3 \pmod 4$ then we may write

$$\left(2^{4k+3} - 1\right)\left(5^{4k+3} - 1\right) = x^2 \quad , \quad (k \geq 0) \tag{26}$$

and it is easy to see that $2^{4k+3} - 1 \equiv 7 \pmod{10}$ and $5^{4k+3} - 1 \equiv 4 \pmod{10}$, from which follows, in our case, that the left side of (26) is not a quadratic residue modulo 10.

Only the case $n \equiv 1 \pmod 4$ remains. If $2 \leq n$ then equation (10) is equivalent to the equation

$$(2^n - 1)(5^{n-1} + \cdots + 5 + 1) = x_1^2 \quad , \tag{27}$$

where $x_1 = \frac{x}{2}$. The corresponding congruence modulo 4 is

$$x_1^2 \equiv 3(1 + \cdots + 1) = 3n \equiv 3 \pmod 4 \quad . \tag{28}$$

It is impossible, so we must finally check the case $n = 1$. This provides the only solution of equation (10) since $(2^1 - 1)(5^1 - 1) = 2^2$. And this is the assertion of Theorem 2. ■

4.3 Proof of Theorem 3

Suppose that the triple (k, n, x) is a solution of equation (11). Let $y = 2^n$ and we have the equality

$$x^2 = (y-1)^2(y^{k-1} + \cdots + y + 1) = (y-1)^2 \left(\frac{y^k - 1}{y - 1} \right) \quad . \tag{29}$$

Thus $\frac{y^k-1}{y-1}$ must be a square. In [5] Ljunggren proved that

$$\frac{y^k - 1}{y - 1} = x_1^2 \quad , \quad (k > 2) \tag{30}$$

is impossible in integers $y > 1$ and x_1, except when $k = 4$, $y = 7$, $x_1 = 20$ and $k = 5$, $y = 3$, $x_1 = 11$. But neither $y = 7$ nor $y = 3$ is a power of 2, so the equation (11) is not soluble if $k > 2$. However in case of $k = 2$ only $n = 3$ and $x = 21$ satisfies the equation

$$(2^n - 1)^2(2^n + 1) = x^2 \tag{31}$$

since $2^n + 1$ is a perfect square if and only if $n = 3$ (see e.g. [4]). This completes the proof of Theorem 3. ■

References

[1] Cohn, J. H. E., On square Fibonacci numbers, J. London Math. Soc., **39** (1964), 537-540.

[2] Cohn, J. H. E., Lucas and Fibonacci numbers and some Diophantine equations, Proc. Glasgow Math. Assoc., **7** (1965), 24-28.

[3] Koblitz, N., A course in number theory and cryptography, Springer-Verlag, 1987.

[4] Lebesque, V. A., Sur l'impossibilité, en nombres entiers, de l'équation $x^m = y^2 + 1$, Nouv. Ann. Math. **9** (1850), 178-81.

[5] Ljunggren, W., Some theorems on indeterminate equations of the form $(x^n-1)/(x-1) = y^q$ (Norvegian), Norsk Mat. Tidsskr. **25** (1943), 17-20.

[6] McDaniel W. L., Square Lehmer numbers, Colloq. Math., **66** (1993), 85-93.

[7] Pethő, A., The Pell sequence contains only trivial perfect powers, Colloq. Math. Soc. János Bolyai 60, Sets, Graphs and Numbers Budapest (Hungary), 1991, 561-568.

[8] Pethő, A., Perfect powers in second order linear recurrences, J. Num Theory, **15** (1982), 5-13.

[9] Pethő, A., Perfect powers in second order recurrences, Colloq. Math. Soc. János Bolyai 34, Topics in Classical Number Theory Budapest (Hungary), 1981, 1217-1227.

[10] Ribenboim, P. – McDaniel, W. L., The square classes in Lucas sequences with odd parameters, C. R. Math. Acad. Sci., Soc. R. Can., **18** (1996), 223-227.

[11] Ribenboim, P. – McDaniel, W. L., The square terms in Lucas sequences, J. Number Theory, **58** (1996), 204-123.

[12] Shorey, T. N. - Stewart, C. L., On the diophantine equation $ax^{2t} + bx^t y + cy^2 = d$ and pure powers in recurrence sequences, Math. Scand., **52** (1983), 24-36.

[13] Wyler, O., In the Fibonacci series $F_1 = 1$, $F_2 = 1$, $F_{n+1} = F_n + F_{n-1}$ the first, second and twelfth terms are squares, Amer. Math. Monthly, **71** (1964), 220-222.

László Szalay
University of Sopron
Institute of Mathematics
Sopron, Bajcsy Zs. u. 4.
H-9400, Hungary
e-mail:laszalay@efe.hu

dc_871_14

dc_871_14

Lajos Hajdu, László Szalay

On the Diophantine equations $(2^n-1)(6^n-1)=x^2$ and $(a^n-1)\left(a^{kn}-1\right)=x^2$

Period. Math. Hung., 40 (2000), 141-145.

On the Diophantine equations $(2^n-1)(6^n-1)=x^2$ and $(a^n-1)\left(a^{kn}-1\right)=x^2$

Lajos Hajdu, László Szalay

Abstract

In this paper[1] [2] we prove that the equation $(2^n-1)(6^n-1)=x^2$ has no solutions in positive integers n and x. Furthermore, the equation $(a^n-1)\left(a^{kn}-1\right)=x^2$ in positive integers $a>1$, n, $k>1$ ($kn>2$) and x is also considered. We show that this equation has the only solutions $(a,n,k,x)=(2,3,2,21)$, $(3,1,5,22)$ and $(7,1,4,120)$.

1 Introduction

In the present paper we prove two results.

Theorem 1. *The equation*

$$(2^n-1)(6^n-1)=x^2 \tag{1}$$

has no solutions in positive integers n and x.

Theorem 2. *The equation*

$$(a^n-1)\left(a^{kn}-1\right)=x^2 \tag{2}$$

has the only solutions $(a,n,k,x)=(2,3,2,21)$, $(3,1,5,22)$ and $(7,1,4,120)$ in positive integers $a>1$, n, $k>1$ ($kn>2$) and x.

The left hand sides of these equations satisfy a fourth order linear recursive relations. Thus the solution of these mixed exponential-polynomial diophantine equations is equivalent to the determination of all perfect squares in fourth order recurrences.

[1]Research supported in part by the Hungarian Academy of Sciences, and by Grants T29330 and 023800 from the Hungarian National Foundation for Scientific Research.

[2]Research supported by Hungarian National Foundation for Scientific Research Grant No. 25157/1998.

In case of fourth order recurrences there are results which are similar to Theorem 1 only for some classes of Lehmer sequences of first and second kind. These were obtained by McDaniel, who examined the existence of perfect square terms of Lehmer sequences in [3].

The second author of this paper has shown (see [4]) that the equation $(2^n-1)(3^n-1)=x^2$ has no positive integer solutions, and the equation $(2^n-1)(5^n-1)=x^2$ has the only solution $n=1$, $x=2$ in positive integers n and x. In [4] the second title equation has also been examined in the special case $a=2$. Thus our Theorem 2 generalizes that result.

Let p be a rational prime number and n be an integer. In the sequel $\left(\frac{n}{p}\right)$ denote the Legendre symbol with respect to these numbers.

2 Preliminaries

We need the following theorems in the proof of Theorem 2.

Theorem A. (Ljunggren, [2]) *The diophantine equation*

$$\frac{x^n-1}{x-1}=y^2 \quad , \quad (n>2)$$

is impossible in integers x, y $(|x|>1)$*, except when* $n=4$*,* $x=7$ *and* $n=5$*,* $x=3$*.*

Theorem B. (Chao Ko, [1]) *The equation*

$$x^p+1=y^2 \quad ,$$

where p *is a prime greater than 3, has no solution in integers* $x\neq 0$ *and* y*.*

3 Proof of the Theorems

3.1 Proof of Theorem 1

Suppose that (n,x) is a solution of equation (1). If n is odd then $(2^n-1)(6^n-1)\equiv -1 \pmod 3$ which cannot be a square. Now we can assume that n is even and distinguish two cases.

I. First put $n=4t$ with some positive integer t, and write $t=k\cdot 5^{\alpha-1}$, where k and α are positive integers with $5\not| k$.

Then we have $(2^n-1)(6^n-1) = \left(16^{k5^\alpha}-1\right)\left(1296^{k5^\alpha}-1\right)$. Since $1296 \equiv 1-5 \pmod{5^2}$ it follows that $1296^5 \equiv 1-5^2 \pmod{5^3}$ and inductively $1296^{5^{\alpha-1}} \equiv 1-5^\alpha \pmod{5^{\alpha+1}}$. Thus $1296^t \equiv 1-k\cdot 5^\alpha \pmod{5^{\alpha+1}}$. Similarly (or by [4]), $16^t \equiv 1+3k\cdot 5^\alpha \pmod{5^{\alpha+1}}$. Consequently $\frac{2^n-1}{5^\alpha} \equiv 3k \pmod 5$ and $\frac{6^n-1}{5^\alpha} \equiv -k \pmod 5$, and we can re-write equation (1) as

$$\frac{2^n-1}{5^\alpha}\,\frac{6^n-1}{5^\alpha} = x_1^2 \quad , \tag{3}$$

where $x_1 = \frac{x}{5^\alpha}$ and the prime 5 divides neither the left nor the right hand side of (3). However, for the Legendre symbol of the left hand side of (3) we obtain

$$\left(\frac{\frac{2^n-1}{5^\alpha}\,\frac{6^n-1}{5^\alpha}}{5}\right) = \left(\frac{3k}{5}\right)\left(\frac{-k}{5}\right) = \left(\frac{-3}{5}\right) = -1 \quad ,$$

which is a contradiction. Thus Theorem 1 is proved in case I.

II. Now let $n = 4t+2 = 2(2t+1)$, where t is a natural number. In this case we must investigate the equation $(4^u-1)(36^u-1) = x^2$ for odd $u = 2t+1$. This last equation is also satisfied $\pmod{18}$, hence it is easy to verify that 3 must divide u. Then we have to solve the equation

$$(64^w-1)\,(46656^w-1) = x^2$$

in odd positive integers $w = \frac{u}{3}$. To show the insolvability of this equation, we give two positive integers such that no term of the sequence $(64^w-1)(46656^w-1)$ is a quadratic residue for both the given two numbers as moduli. For example, 17 and 97 are such numbers.

To prove this, let $I_w = (64^w-1)(46656^w-1)$. Then

$$I_w \equiv ((-4)^w-1)(8^w-1) \pmod{17} \quad .$$

Since

$$(-4)^4 \equiv 1 \pmod{17} \text{ and } 8^8 \equiv 1 \pmod{17} \quad ,$$

it is sufficient to examine the cases $w = 1, 3, 5, 7$.

$$I_1 \equiv 16 \pmod{17} \text{ and } I_7 \equiv 8 \pmod{17}$$

are quadratic residues, while

$$I_3 \equiv 3 \pmod{17} \text{ and } I_5 \equiv 11 \pmod{17}$$

are not quadratic residues $\pmod{17}$.

On the other hand,

$$I_w \equiv (64^w-1)((-1)^w-1) \equiv (64^w-1)(-2) \pmod{97} \quad .$$

Since $64^8 \equiv 1 \pmod{97}$, we must investigate the cases $w = 1, 3, 5, 7$.

$$I_1 \equiv 68 \pmod{97} \text{ and } I_7 \equiv 5 \pmod{97}$$

are not quadratic residues, but

$$I_3 \equiv 96 \pmod{97} \text{ and } I_5 \equiv 33 \pmod{97}$$

are quadratic residues (mod 97). This completes the proof of the Theorem. ■

3.2 Proof of Theorem 2

Suppose that the four-tuple (a, n, k, x) $(a > 1, k > 1, kn > 2)$ is a solution of equation (2). Let $y = a^n$. Now we have the equality

$$x^2 = (y-1)^2(y^{k-1} + \cdots + y + 1) = (y-1)^2 \left(\frac{y^k - 1}{y - 1}\right) \quad .$$

Thus $\frac{y^k-1}{y-1}$ must be a square. By Theorem A, if $k > 2$ then $k = 4$ or $k = 5$. Consequently from $y = a^n = 7$ it follows that $a = 7, n = 1, x = 120$ and $y = a^n = 3$ gives $a = 3, n = 1, x = 22$. These two cases provide the solutions $(a, k, n, x) = (7, 4, 1, 120)$ and $(3, 5, 1, 22)$ of (2).

Now suppose that $k = 2$. Then $(y-1)^2(y+1) = x^2$ and

$$y + 1 = a^n + 1 \tag{4}$$

must be a square. Since $kn > 2$, it follows that $n > 1$. Without loss of generality we may assume that n is a prime. If $n = 2$ then (4) cannot be a square, and it is well known that if $n = 3$ then for a positive integer a, (4) is a square only in case of $a = 2$. Thus equation (2) has one more solution: $(a, k, n, x) = (2, 2, 3, 21)$. Finally, by Theorem B (4) cannot be a square if $n > 3$. This completes the proof of Theorem 2. ■

Remark. If $k = 1$ then $(a^n - 1)(a^n - 1)$ is always square number. If $k = 2$ and $n = 1$ then $(a-1)(a^2-1) = (a-1)^2(a+1)$ may be square infinitely many times when $a + 1$ is a square.

Acknowledgements. The authors are grateful to the referee for his many useful remarks and suggestions.

References

[1] Chao Ko, On the Diophantine equation $x^2 = y^n + 1$, $xy \neq 0$, Scientia Sinica (Notes), **14** (1965), 457-460.

[2] Ljunggren, W., Some theorems on indeterminate equations of the form $(x^n-1)/(x-1) = y^q$ (Norvegian), Norsk Mat. Tidsskr. **25** (1943), 17-20.

[3] McDaniel W. L., Square Lehmer numbers, Colloq. Math., **66** (1993), 85-93.

[4] Szalay, L., On the diophantine equation $(2^n - 1)(3^n - 1) = x^2$, accepted for publication in Publ. Math. Debrecen

Lajos Hajdu
Kossuth Lajos University
Institute of Mathematics and Informatics
Debrecen, P.O.Box 12.
H-4010, Hungary
e-mail: hajdul@math.klte.hu

László Szalay
University of Sopron
Institute of Mathematics
Sopron, Bajcsy Zs. u. 4.
H-9400, Hungary
e-mail: laszalay@efe.hu

dc_871_14

dc_871_14

Li Lan, László Szalay

On the exponential diophantine equation $(a^n - 1)(b^n - 1) = x^2$

Publ. Math. Debrecen, 77 (2010), 465-470.

On the exponential diophantine equation $(a^n-1)(b^n-1)=x^2$

Li Lan, László Szalay

Abstract

Let a and b be fixed positive integers such that $a \neq b$ and $\min(a,b) > 1$. In this paper, we combine some divisibility properties of the solutions of Pell equations with elementary arguments to prove that if $a \equiv 2 \pmod 6$ and $b \equiv 0 \pmod 3$, then the title equation $(a^n-1)(b^n-1) = x^2$ has no positive integer solution (n,x). Moreover, we show that in case of $a \equiv 2 \pmod{20}$ and $b \equiv 5 \pmod{20}$, where $b-1$ is a full square, the only possible solution belongs to $n=1$.

1 Introduction

Let $\mathbb{N}^+$ denote the set of all positive integers, further let a and b be distinct fixed positive integers such that $\min(a,b) > 1$. In this paper, we discuss the problem of the solution to the exponential diophantine equation

$$(a^n-1)(b^n-1) = x^2, \quad n, x \in \mathbb{N}^+ \tag{1}$$

in some particular cases.

The literature of this equation and its alternations is very rich, see e.g. the papers [6, 2, 1, 5, 4] and the references given there. First, Szalay [6], using a relatively complicated method, proved that if $(a,b) = (2,3)$ then equation (1) has no solution. He also showed that only $(n,x) = (1,2)$ satisfies $(2^n-1)(5^n-1) = x^2$. Then, Hajdu and Szalay [2] justified the insolubility of (1) when $(a,b) = (2,6)$, further they determined all the solutions if $a > 1$ is an arbitrary integer and $b = a^k$. This result was extended by Cohn [1] to the case $a^k = b^l$. He also proved that there is no solution to (1) when $4 \mid n$, except for $(a,b) = (13,239)$. Luca and Walsh [5] described a computational method for solving (1), and their approach was used to solve completely the equations for almost all pairs (a,b) in the range $1 < a < b \leq 100$. Recently, Le [4] showed that equation (1) is insoluble if $a = 2$ and $3 \mid b$.

Several problems and conjectures linked to the title equation have already been posed (see [1, 5, 4]).

The main purpose of this paper is to prove the following general results by combining certain divisibility properties of the solutions of Pell equations, and partially applying the techniques described in [4] and [5].

Theorem 1. *If* $a \equiv 2 \pmod 6$ *and* $b \equiv 0 \pmod 3$ *then the equation* $(a^n-1)(b^n-1) = x^2$ *has no positive integer solution* (n, x).

Theorem 2. *Suppose that* $b - 1 = t^2$ *is a full square. If* $a \equiv 2 \pmod{20}$ *and* $b \equiv 5 \pmod{20}$ *then the only possible solution to the equation* $(a^n-1)(b^n-1) = x^2$ *is*

$$(n, x) = (1, t\sqrt{a-1}\,).$$

Theorem 1 states that there is no solution in at least $\frac{1}{18}$ part of the possible integer pairs (a, b). At the same time, this theorem generalizes the results appearing in [6] (Theorem 1), in [2] (Theorem 1), and in [4], while Theorem 2 extends Theorem 2 of [6].

It is worthwhile noting that if one replaces the condition $b \equiv 5 \pmod{20}$ in Theorem 2 by the weaker relation $b \equiv 0 \pmod 5$ then our approach does not work. Although, the cases $b \equiv -5 \pmod{20}$ and $b \equiv 0 \pmod{20}$ can be handled trivially by applying modulo 20 arithmetic, in case of $b \equiv 10 \pmod{20}$ the method fails.

Obviously, there are infinitely many pairs (a, b) satisfying the conditions of Theorem 2. In particular, by choosing a such that $a - 1$ is a perfect square, we get equations (1) having unique solutions.

2 Divisibility properties of the solutions of Pell equation

Let D be a positive integer which is not a square. It is well known (see, for example, [3] (Theorems 10.9.1 and 10.9.2)) that the Pell equation

$$u^2 - Dv^2 = 1, \quad u, v \in \mathbb{N}^+ \tag{2}$$

has infinitely many solutions (u, v). If $(u, v) = (u_1, v_1)$ denotes the smallest non-trivial positive solution to equation (2) then every positive solution (u_k, v_k) $(k \in \mathbb{N}^+)$ can be generated by

$$u_k + v_k\sqrt{D} = (u_1 + v_1\sqrt{D})^k. \tag{3}$$

The trivial solution $(u, v) = (1, 0)$ is denoted by (u_0, v_0).

The proof of the Theorems 1 and 2 partially relies on

Lemma 1. *(i) If* $2 \mid k$ *then* $2 \nmid u_k$.
(ii) If $2 \mid k$ *then each prime factor* p *of* u_k *satisfies* $p \equiv \pm 1 \pmod 8$.
(iii) If $2 \nmid k$ *then* $u_1 \mid u_k$.
(iv) If q *is a prime in the set* $\{2, 3, 5\}$ *then* $q \mid u_k$ *implies* $q \mid u_1$.

We remark that the feature (iv) is not valid longer in its form for $p \geq 7$ since, for instance, the fundamental solution to $u^2 - 3v^2 = 1$ is $(u_1, v_1) = (2, 1)$, $7 \mid u_2 = 7$ but $7 \nmid u_1$.

Proof of Lemma 1.

(i) Let $k = 2t$, where t is positive integer. By (3), we have

$$u_k + v_k\sqrt{D} = (u_1 + v_1\sqrt{D})^{2t} = \left((u_1 + v_1\sqrt{D})^t\right)^2 = (u_t + v_t\sqrt{D})^2 = (u_t^2 + Dv_t^2) + 2u_tv_t\sqrt{D}. \tag{4}$$

Further, $u_t^2 - Dv_t^2 = 1$ holds since $(u, v) = (u_t, v_t)$ is the solution to equation (2). Consequently,

$$u_k = u_t^2 + Dv_t^2 = 2u_t^2 - 1 \tag{5}$$

implies that u_k is an odd number. In other words, if u_k is an even number then the subscript k must be odd.

(ii) From part (i) of Lemma 1 it follows, that if k is even then all prime factors p of u_k are odd. For such a p, by (5), the Legendre symbol $\left(\frac{2}{p}\right)$ equals 1. Thus $p \equiv \pm 1 \pmod 8$.

(iii) If $2 \nmid k$, then by (3), together with the binomial theorem, we obtain immediately

$$u_k = u_1 \sum_{i=0}^{(k-1)/2} \binom{k}{2i} u_1^{k-2i-1}(Dv_1^2)^i, \tag{6}$$

which implies $u_1 \mid u_k$.

(iv) It is easy to see, that the terms of the sequence of u_k satisfy the recurrence relation $u_{k+1} = 2u_1u_k - u_{k-1}$. Since the sequence u_k is periodic modulo any positive integer, so if $p = 2, 3, 5$, we have to eliminate those cases where $p \mid u_k$ occurs. Recall, that $u_0 = 1$ and note that the recurrence $u_{k+1} = 2u_1u_k - u_{k-1}$ is valid modulo p, too. We find that by any of the three possibilities for p,

$$p \mid u_k \quad \text{if and only if} \quad k \equiv 1 \pmod 2 \quad \text{and} \quad u_1 \equiv 0 \pmod p. \ \blacksquare$$

3 Proof of the theorems

Proof of Theorem 1. Let $a \equiv 2 \pmod 6$ and $b \equiv 0 \pmod 3$, and suppose that the pair (n, x) is a solution to equation (1). Put $D = \gcd(a^n - 1, b^n - 1)$. By (1), we get

$$a^n - 1 = Dy^2, \quad b^n - 1 = Dz^2, \quad x = Dyz, \qquad D, y, z \in \mathbb{N}^+. \tag{7}$$

Since $3 \mid b$, by $b^n - 1 = Dz^2$ it follows that $3 \nmid D$ and $3 \nmid z$. Hence $z^2 \equiv 1 \pmod 3$. Consequently,

$$D \equiv Dz^2 = b^n - 1 \equiv 2 \pmod 3. \tag{8}$$

Now we distinguish two cases. Firstly, if $3 \nmid y$, then $y^2 \equiv 1 \pmod 3$, and (7), together with (8) implies

$$a^n = Dy^2 + 1 \equiv D + 1 \equiv 0 \pmod 3. \tag{9}$$

However, it contradicts $a \equiv 2 \pmod 3$. Thus we can exclude $3 \nmid y$.

Assume now that $3 \mid y$. Since $a \equiv 2 \pmod 3$, by $a^n - 1 = Dy^2$ we obtain

$$2^n \equiv a^n = Dy^2 + 1 \equiv 1 \pmod 3. \tag{10}$$

Clearly, $2^n \equiv \pm 1 \pmod 3$, and $+1$ is occurring exactly when n is even.

Put $n = 2m$. Therefore, by (7), D cannot be a square, and the corresponding Pell equation $u^2 - Dv^2 = 1$ has two solutions

$$(u, v) = (a^m, y),\ (b^m, z). \tag{11}$$

Since $a \neq b$, there exist distinct positive integers r and s such that

$$(a^m, y) = (u_r, v_r) \quad \text{and} \quad (b^m, z) = (u_s, v_s)$$

hold.

If s is even , by (ii) of Lemma 1 we know that any prime factor p of b satisfies $p \equiv \pm 1 \pmod 8$. But it is impossible since $3 \mid b$. Therefore, s must be odd. Hence, by (iv) of Lemma 1 and $3 \mid b$ we obtain $3 \mid u_1$. On the other hand, $2 \mid a$ which, together with (i) of Lemma 1 and $(a^m, y) = (u_r, v_r)$ shows that r is odd. However, by the statement (iii) of Lemma 1 and $3 \mid u_1$ we have $3 \mid a^m$, which leads to a contradiction, since $a \equiv 2 \pmod 6$. This completes the proof of Theorem 1. ■

Proof of Theorem 2. Now let $a \equiv 2 \pmod{20}$ and $b \equiv 5 \pmod{20}$, where $b - 1$ is a square of a nonzero integer t. First, we deal with even exponents n in the proof of Theorem 2. Replace the prime 3 by 5 in the proof of Theorem 1, and repeat step by step arguments handling the case $n = 2m$ to obtain the statement in this case .

Assume now that n is odd. Suppose that there is a non-negative integer m such that $n = 4m + 3$. Consider the equation $(a^n - 1)(b^n - 1) = x^2$ modulo 10. Obviously,

$$x^2 = (a^{4m+3} - 1)(b^{4m+3} - 1) \equiv (2^{4m+3} - 1)(5^{4m+3} - 1) \equiv 7 \cdot 4 \equiv 8 \pmod{10},$$

which is impossible since 8 is not a quadratic residue modulo 10.

Finally, let $n = 4m + 1$ for some non-negative integer m. Recall, that $b - 1 = t^2$. Thus, if (n, x) is a solution to (1) then

$$(a^{4m+1} - 1)(b^{4m} + b^{4m-1} + \cdots + b + 1) = \left(\frac{x}{t}\right)^2 \in \mathbb{N}. \tag{12}$$

Suppose that $m > 0$ and consider (12) modulo 4 to obtain $(2^{4m+1}-1)(4m+1) \equiv 3 \cdot 1 = 3$, which is not a quadratic residue modulo 4. Thus we arrive at a contradiction. If $m = 0$, equation (12) simplifies

$$\left(\frac{x}{t}\right)^2 = a - 1.$$

That is, if $a-1$ is a full square then there is exactly one solution $(n, x) = (1, t\sqrt{a-1}\,)$. The proof of Theorem 2 is complete. ■

References

[1] Cohn, J. H. E., The diophantine equation $(a^n-1)(b^n-1) = x^2$, *Period. Math. Hungar.*, 2002, **44**(2), 169-175.

[2] Hajdu, L. - Szalay, L., On the diophantine equation $(2^n - 1)(6^n - 1) = x^2$ and $(a^n - 1)(a^{kn} - 1) = x^2$, *Period. Math. Hungar.*, 2000, **40**(2), 141-145.

[3] Lua, L. G., Introduction to number theory, Beijing, *Science Press*, 1979. (in Chinese)

[4] Le, M. H., A note on the exponential diophantine equation $(2^n - 1)(b^n - 1) = x^2$, *Publ. Math. Debrecen*, 2009, **74**(3-4), 453-455.

[5] Luca, F. - Walsh, P. G., The product of like-indexed terms in binary recurrences. *J. Number Theory*, 2002, **96**(1), 152-173.

[6] Szalay, L., On the diophantine equation $(2^n-1)(3^n-1) = x^2$, *Publ. Math. Debrecen*, 2000, **57**(1), 1-9.

dc_871_14

dc_871_14

László Szalay

On the resolution of the equations $U_n = \binom{x}{3}$ and $V_n = \binom{x}{3}$

Fibonacci Q., 40 (2002), 9-12.

On the resolution of the equations $U_n = \binom{x}{3}$ and $V_n = \binom{x}{3}$

László Szalay

1 Introduction

The purpose of the present paper is to prove that there are finitely many binomial coefficients of the form $\binom{x}{3}$ in certain binary recurrences, and give a simple method for the determination of these coefficients. We illustate the method by the Fibonacci, the Lucas and the Pell sequences. First we transform both of the title equations into two elliptic equations and apply a theorem of MORDELL [10, 11] to them. (Later SIEGEL [16] generalized MORDELL's result, and in 1968 BAKER gave its effective version.) After showing the finiteness we use the program package SIMATH [15] which is a computer algebra system, especially useful for number theoretic purposes, and is able to find all the integer points on the corresponding elliptic curves. The algorithms of SIMATH are based on some deep results of GEBEL, PETHŐ and ZIMMER [5].

Before going into details we present a short historical survey. Several authors have investigated the occurence of special figurate numbers in the second order linear recurrences. One such problem is, for example, to determine which Fibonacci numbers are square. COHN [2, 3] and WYLER [18], applying elementary methods, proved independently that the only square Fibonacci numbers are $F_0 = 0$, $F_1 = F_2 = 1$ and $F_{12} = 144$. A similar result for the Lucas numbers was obtained by COHN [4]: if $L_n = x^2$ then $n = 1$ or $n = 3$. LONDON and FINKELSTEIN [6] established full Fibonacci cubes. PETHŐ [12] gave a new proof of the theorem of LONDON and FINKELSTEIN, applying the Gel'fond-Baker method and computer investigations. Later PETHŐ found all the fifth power Fibonacci numbers [14], and all the perfect powers in the Pell sequence [13].

Another special interest was to determine the triangular numbers $T_x = \frac{x(x+1)}{2}$ in certain recurrences. HOGGATT conjectured that there are only five triangular Fibonacci numbers. This problem was originally posed by TALLMAN [17] in the Fibonacci Quarterly. In 1989 MING [8] proved HOGATT's conjecture by showing that the only Fibonacci numbers which are triangular are $F_0 = 0$, $F_1 = F_2 = 1$, $F_4 = 3$, $F_8 = 21$ and $F_{10} = 55$. MING also proved in [9] that the only triangular Lucas numbers are $L_1 = 1$, $L_2 = 3$ and $L_{18} = 5778$. Moreover, the only triangular Pell number is $P_1 = 1$ (MCDANIEL [7]).

Since the number T_{x-1} is equal to the binomial coefficient $\binom{x}{2}$, it is natural to ask whether the terms $\binom{x}{3}$ occur in binary recurrences or not. As we will see, the second order linear recurrences, for instance the Fibonacci, the Lucas and the Pell sequences have few such terms.

Now we introduce some notation. Let the sequence $\{U_n\}_{n=0}^{\infty}$ be defined by the initial

terms U_0, U_1 and by the recurrence relation

$$U_n = AU_{n-1} + BU_{n-2} \qquad (n \geq 2) \quad , \tag{1}$$

where $U_0, U_1, A, B \in \mathbb{Z}$ with the conditions $|U_0| + |U_1| > 0$ and $AB \neq 0$. Moreover, let α and β be the roots of the polynomial

$$p(x) = x^2 - Ax - B \quad , \tag{2}$$

and we denote the discriminant A^2+4B of $p(x)$ by D. Suppose that $D \neq 0$ (i.e. $\alpha \neq \beta$). Throughout this paper we also assume that $U_0 = 0$ and $U_1 = 1$.

The sequence

$$V_n = AV_{n-1} + BV_{n-2} \qquad (n \geq 2) \quad , \tag{3}$$

with the initial values $V_0 = 2$ and $V_1 = A$ is the associate sequence of U. The recurrences U and V satisfy the relation $V_n^2 - DU_n^2 = 4(-B)^n$.

Finally, it is even assumed that $|B| = 1$. Then

$$V_n^2 - DU_n^2 = 4(\pm 1)^n = \pm 4 \quad . \tag{4}$$

As usual, denote by F_n, L_n and P_n the n^{th} term of the Fibonacci, the Lucas and the Pell sequences, respectively.

The following theorems formulate precisely the new results.

Theorem 1. *Both the equations* $U_n = \binom{x}{3}$ *and* $V_n = \binom{x}{3}$ *have only a finite number of solutions* (n, x) *in the integers* $n \geq 0$ *and* $x \geq 3$.

Theorem 2. *All the integer solutions of the equation*
i) $F_n = \binom{x}{3}$ *are* $(n, x) = (1, 3)$ *and* $(2, 3)$,
ii) $L_n = \binom{x}{3}$ *are* $(n, x) = (1, 3)$ *and* $(3, 4)$,
iii) $P_n = \binom{x}{3}$ *is* $(n, x) = (1, 3)$.

2 Proof of Theorem 1

Let U and V be binary recurrences specified above. We distinguish two cases.

Part I. First we deal with the equation

$$U_n = \binom{x}{3} \tag{5}$$

in the integers n and x. Applying (4) together with $y = V_n$ and $x_1 = x - 1$, we have $U_n = \binom{x_1+1}{3}$ and

$$y^2 - D\left(\frac{x_1^3 - x_1}{6}\right)^2 = \pm 4 \quad . \tag{6}$$

Take the 36 times of the equation (6). Let $x_2 = x_1^2$ and $y_1 = 6y$, and using these new variables, from (6) we get

$$y_1^2 = Dx_2^3 - 2Dx_2^2 + Dx_2 \pm 144 \quad . \tag{7}$$

Multiplying by 3^6D^2 the equation (7), together with $k = 3^3Dy_1$ and $l = 3D(3x_2 - 2)$ it follows that

$$k^2 = l^3 - 27D^2l + (54D^3 \pm 104976D^2) \quad . \tag{8}$$

By a theorem of Mordell [10, 11] it is sufficient to show that the polynomial $u(l) = l^3 - 27D^2l + (54D^3 \pm 104976D^2)$ has three distinct roots. Suppose that the polynomial $u(l)$ has a multiple root $\tilde{l}$. Then $\tilde{l}$ satisfies the equation $u'(l) = 3l^2 - 27D^2 = 0$, i.e. $\tilde{l} = \pm 3D$. Since $u(3D) = \pm 104976D^2$ it follows that $D = 0$ which is impossible. Moreover, $u(-3D) = 108D^3 \pm 104976D^2$ implies that $D = 0$ or $D = \pm 972$. But $D \neq 0$ and by $|B| = 1$ there are no integer A for which $D = A^2 + 4B = \pm 972$. Consequently, $u(l)$ has three distinct zeros.

Part II. The second case consists of the examination of the diophantine equation

$$V_n = \binom{x}{3} \tag{9}$$

in the integers n and x. Let $y = U_n$ and $x_1 = x - 1$. Applying the method step by step as above in part I, it leads to the elliptic equation

$$k^2 = l^3 - 27D^2l + cD^3 \quad , \tag{10}$$

where $c = -104922$ if n is even and $c = 105030$ otherwise. The polynomial $v(l) = l^3 - 27D^2l + cD^3$ has also three distinct roots because $v'(l) = 3l^2 - 27D^2$, $\tilde{l} = \pm 3D$ and $v(\pm 3D) = 0$ implies $D = 0$.

Thus the proof of Theorem 1 is complete.

3 Proof of Theorem 2

The corresponding elliptic curves of the equations (8) and (10) are in short Weierstrass normal form, whence for a given discriminant D it can be solved by SIMATH.

By (8) and (10) one can compute the coefficients of the elliptic curves in case of the Fibonacci, the Lucas and the Pell sequences. The calculations are summarized in Table 1, as well as all the integer points belonging to them. Every binary recurrence leads to two elliptic equations because of the even and odd suffixes. For the Fibonacci and Lucas sequences $D = 5$, and for the Pell sequence and its associate sequence $D = 8$.

Equation	*Transformed equations*	*All the integer solutions* (l, k)
$F_n = \binom{x}{3}$	$k^2 = l^3 - 675l + 2631150$	$(15, 1620)$, $(-30, 1620)$, $(5199, 374868)$, $(735, 19980)$, $(150, 2430)$, $(-129, 756)$
$F_n = \binom{x}{3}$	$k^2 = l^3 - 675l - 2617650$	$(150, 810)$, $(555, 12960)$, $(1014, 32238)$, $(195, 2160)$, $(451, 9424)$, $(4011, 254016)$
$L_n = \binom{x}{3}$	$k^2 = l^3 - 675l - 13115250$	no solution
$L_n = \binom{x}{3}$	$k^2 = l^3 - 675l + 13128750$	$(375, 8100)$, $(-74, 3574)$, $(150, 4050)$, $(-201, 2268)$, $(2391, 116964)$
$P_n = \binom{x}{3}$	$k^2 = l^3 - 1728l + 6746112$	$(-192, 0)$, $(24, 2592)$, $(-48, 2592)$, $(97, 2737)$ $(312, 6048)$, $(564, 13608)$, $(5208, 375840)$
$P_n = \binom{x}{3}$	$k^2 = l^3 - 1728l - 6690816$	$(240, 2592)$, $(609, 14769)$

Table 1

The last step is to calculate x and y from the solutions (l, k). By the proof of Theorem 1 it follows that $x = 1 + \sqrt{\frac{l+6D}{9D}}$, $y = \frac{k}{162D}$ in case of the equation (5) and $y = \frac{k}{162D^2}$ in case of the associate sequence. Except for some values x and y, they are not integer if $x \geq 3$. The exceptions provide all the solutions of the equations (8) and (10). Then the proof of Theorem 2 is complete.

Acknowledgement. The author is grateful to Professor PETHŐ for his valuable remarks.

References

[1] Baker, A., The diophantine equation $y^2 = ax^3 + bx^2 + cx + d$, J. London Math. Soc., **43** (1968), 1-9.

[2] Cohn, J. H. E., Square Fibonacci numbers, etc..., Fib. Quarterly, **2** (1964), 109-113.

[3] Cohn, J. H. E., On square Fibonacci numbers, J. London Math. Soc., **39** (1964), 537-540.

[4] Cohn, J. H. E., Lucas and Fibonacci numbers and some Diophantine equations, Proc. Glasgow Math. Assoc., **7** (1965), 24-28.

[5] Gebel, L. - Pethő, A. - Zimmer, H. G., Computing integral points on elliptic curves, Acta Arithm. **68** (1994), 171-192.

[6] London, H. - Finkelstein, R., On Fibonacci and Lucas numbers which are perfect powers, Fib. Quarterly, **7** (1969), 476-481, 487.

[7] McDaniel, W. L., Triangular numbers in the Pell sequence, Fib. Quarterly, **34** (1996), 105-107.

[8] Ming, L., On triangular Fibonacci numbers, Fib. Quarterly, **27** (1989), 98-108.

[9] Ming, L., On triangular Lucas numbers, Applications of Fibonacci Numbers, Vol 4., Dordrecht, Netherlands: Kluwer, 1991, 231-240.

[10] Mordell, L. J., Note on the integer solutions of the equation $Ey^2 = Ax^3 + Bx^2 + Cx + D$, Messenger Math., **51** (1922), 169-171.

[11] Mordell, L. J., On the integer solutions of the equation $ey^2 = ax^3 + bx^2 + cx + d$, Proc. London Math. Soc. (2), **21** (1923), 415-419.

[12] Pethő, A., Full cubes in the Fibonacci sequence, Publ. Math. Debrecen, **30** (1983), 117-127.

[13] Pethő, A., The Pell sequence contains only trivial perfect powers, Colloq. Math. Soc. János Bolyai 60, Sets, Graphs and Numbers Budapest (Hungary), 1991, 561-568.

[14] Pethő, A., Perfect powers in second order recurrences, Colloq. Math. Soc. János Bolyai 34, Topics in Classical Number Theory Budapest (Hungary), 1981, 1217-1227.

[15] SIMATH Manual, Saarbrücken, 1996.

[16] Siegel, C. L. (under the pseudonym X), The integer solutions of the equation $y^2 = ax^n + bx^{n-1} + \cdots + k$, J. London Math. Soc., **1** (1926), 66-68.

[17] Tallman, M. H., Fib. Quarterly, **1** (1963), 47.

[18] Wyler, O., In the Fibonacci series $F_1 = 1$, $F_2 = 1$, $F_{n+1} = F_n + F_{n-1}$ the first, second and twelfth terms are squares, Amer. Math. Monthly, **71** (1964), 221-222.

dc_871_14

dc_871_14

4. Dolgozatok: polinomiális-exponenciális diofantikus egyenletrendszerek: diofantikus halmazok

dc_871_14

Clemens Fuchs, Florian Luca, László Szalay

Diophantine Triples with Values in Binary Recurrences

Ann. Sc. Norm. Super. Pisa Cl. Sci., 5 (2008), 579-608.

Diophantine triples with values in binary recurrences

Clemens Fuchs, Florian Luca, László Szalay

Abstract

In this paper, we study triples a, b and c of distinct positive integers such that $ab+1$, $ac+1$ and $bc+1$ are all three members of the same binary recurrence sequence.

1 Introduction

A *Diophantine m-tuple* is a set $\{a_1, \ldots, a_m\}$ of positive integers such that $a_i a_j + 1$ is a perfect square (i.e. a square of a number in $\mathbb{Z}$) for all $1 \leq i < j \leq m$. Finding such sets was already investigated by Diophantus and he found the *rational* quadruple $\{1/16, 33/16, 68/16, 105/16\}$. The first quadruple in integers, the set $\{1, 3, 8, 120\}$, was found by Fermat. Infinitely many Diophantine quadruples are known and it is conjectured that there is no Diophantine quintuple. This was almost proved by Dujella [7], who showed that there can be at most finitely many Diophantine quintuples and all of them are, at least in theory, effectively computable. Several variants of this problem have been studied in the past. For example, Bugeaud and Dujella [2], proved upper bounds for the size m of sets of positive integers with the property that the product of any two distinct elements plus one is a perfect k-th power for fixed k, namely m is bounded by 7 for $k = 3$, by 5 for $k = 4$, by 4 for $5 \leq k \leq 176$, and by 3 for $k \geq 177$. Another variant studied previously is concerned with perfect powers instead of squares or k-th powers for fixed k. The second author proved that the *abc*-conjecture implies that the size of such sets is bounded by an absolute constant, whereas unconditionally there are bounds depending on the largest element in the set (see [13] and the papers cited therein). For further results on Diophantine m-tuples and its variants, we refer to [8].

In this paper, we treat another variant of this problem. Let r and s be nonzero integers such that $\Delta = r^2 + 4s \neq 0$. Let $(u_n)_{n \geq 0}$ be a binary recurrence sequence of integers satisfying the recurrence

$$u_{n+2} = r u_{n+1} + s u_n \quad \text{for all} \quad n \geq 0.$$

It is well-known that if we write α and β for the two roots in $\mathbb{C}$ of the *characteristic equation* $x^2 - rx - s = 0$, then there exist constants $\gamma, \delta \in \mathbb{K} = \mathbb{Q}[\alpha]$ such that

$$u_n = \gamma \alpha^n + \delta \beta^n \tag{1}$$

holds for all $n \geq 0$. We shall assume in what follows that the sequence $(u_n)_{n\geq 0}$ is *nondegenerate*, which means that $\gamma\delta \neq 0$ and α/β is not root of unity. We shall also make the convention that $|\alpha| \geq |\beta|$. Note that $|\alpha| > 1$.

Here, we look for Diophantine triples with values in the set $\mathcal{U} = \{u_n : n \geq 0\}$, namely sets of three distinct positive integers $\{a, b, c\}$, such that $ab+1,\ ac+1,\ bc+1$ are all in $\mathcal{U}$. Clearly, there are always such pairs as e.g. $\{1, u_n - 1\}$. Note that if $u_n = 2^n + 1$ for all $n \geq 0$, then there are infinitely many such triples (namely, take a, b, c to be any distinct powers of two); in this situation, we can even get arbitrarily large sets $\{a_1, \ldots, a_m\}$ with the property that $a_i a_j + 1 \in \mathcal{U}$ for all $1 \leq i < j \leq m$. Our main result is that the above example is representative for the sequences $(u_n)_{n\geq 0}$ with real roots for which there exist infinitely many Diophantine triples with values in $\mathcal{U}$. More precisely we prove the following.

Theorem 1. *Assume that $(u_n)_{n\geq 0}$ is a nondegenerate binary recurrence sequence with $\Delta > 0$ such that there exist infinitely many sextuples of nonnegative integers*

$$(a, b, c; x, y, z)$$

with $1 \leq a < b < c$ such that

$$ab + 1 = u_x, \qquad ac + 1 = u_y, \qquad bc + 1 = u_z. \tag{2}$$

Then $\beta \in \{\pm 1\}, \delta \in \{\pm 1\}$, $\alpha, \gamma \in \mathbb{Z}$. Furthermore, for all but finitely many of the sextuples $(a, b, c; x, y, z)$ as above one has $\delta\beta^z = \delta\beta^y = 1$ and one of the following holds:

(i) $\delta\beta^x = 1$. In this case, one of γ or $\gamma\alpha$ is a perfect square;

(ii) $\delta\beta^x = -1$. In this case, $x \in \{0, 1\}$.

Theorem 1, of course, implies that there are only finitely many triples of positive integers such that the product of any two plus one is in $\mathcal{U}$, except in the cases described (and these cases really occur as we saw above). We mention that the problem can be reformulated as a Diophantine equation of polynomial-exponential type with three independent exponential variables and three additional polynomial variables, namely

$$(ab + 1 - u_x)^2 + (ac + 1 - u_y)^2 + (bc + 1 - u_z)^2 = 0.$$

It is well-known that the Subspace theorem is a powerful tool for such problems, e.g. it was also used to classify the solutions to the equation $Au_x + Bu_y + Cu_z = 0$ for fixed $A, B, C \in \mathbb{Z}$ in [17] (see [18] for a survey on such equations). A new development in applying the Subspace theorem was startet by Corvaja and Zannier (see [22, 23, 10]), and their techniques will also be used in our proof (especially we use [6, 11] and [5]). We could not prove any finiteness result for the case when $\Delta < 0$, the reason being

that in this case there is no *dominant root* in the polynomial-exponential Diophantine equation, which is the main restriction in applying the Subspace theorem with these techniques at present.

For example, it follows for the particular case of the Fibonacci sequence $(F_n)_{n\geq 0}$, given by $(r,s)=(1,1)$, $F_0=0$ and $F_1=1$, that there are at most finitely many triples of positive integers such the product of any two plus one is a Fibonacci number F_n. In the subsequent paper [16] the second and third author show that there is in fact no triple of distinct positive integers $a,\ b$ and c such that $ab+1,\ ac+1$ and $bc+1$ are all three Fibonacci numbers.

2 A bird's-eye-view of the proof

For the convenience of the reader we will give an overview of the proof of the theorem, since the proof is rather long and becomes more and more technical towards the end. We mention that throughout the paper the symbols $o, O, \sim, \ll, \gg, \asymp$, are used with their usual meaning.

Since $\Delta > 0$, it follows that $|\alpha| > |\beta|$. We shall show that one may assume that both α and γ are positive. We assume that we have infinitely many solutions $(a,b,c;x,y,z)$ to equation (2). Then $z\to\infty$, $x<y<z$ if z is sufficiently large, and $c \mid \gcd(u_y-1, u_z-1)$. The case $\delta\beta^z=1$ is not hard to handle. When $\delta\beta^z\neq 1$, results from Diophantine approximations relying on the Subspace Theorem, as the finiteness of the number of solutions of nondegenerate unit equations with variables in a finitely generated multiplicative group and bounds for the greatest common divisors of values of rational functions at units points in the number fields setting, allow us to reduce the problem to elementary considerations concerning polynomials. By using unit equations, we first conclude that $\log b$ and $\log c$ have the same orders of magnitude, therefore $x\asymp y\asymp z$. Then we show that a is also large which will come in handy lateron. These preliminaries can be found in the next two sections (see Section 3 and 4). Next, since the multi-recurrence $((u_x-1)(u_y-1)(u_z-1))_{x<y<z}$ has a dominant root and comparable positive integer subscripts, a result of the first author from [11] tells us that for infinitely many of our solutions, the positive integer abc is a linear combination of finitely many of the monomials in $\alpha^x,\ \beta^x,\ \alpha^y,\ \beta^y,\ \alpha^z,\ \beta^z$ appearing in the formal Puiseux expansion of $\sqrt{(u_x-1)(u_y-1)(u_z-1)}$. Hence, the relation $(abc)^2=(u_x-1)(u_y-1)(u_z-1)$, may now be regarded as a unit equation with unknowns in the multiplicative group generated by α and β, and it remains to deal with it (equivalently, it can be viewed as the problem of calculating the zeroes of a multi-recurrence; this is not an easy task, see e.g. Remark 5 in [11]). The proof now falls in two distinct cases: the case when α and β are multiplicatively independent or multiplicatively dependent. In case α and β are multiplicatively independent (which together with the considerations outlined above is handled in Section 5), listing the first few dominant units in both sides of the

equation and identifying them, one gets a few linear relations among the exponents x, y and z. It turns out that if one goes back to the original equations, these few linear relations are enough to get a contradiction in this case. In case when α and β are multiplicatively dependent (see Section 6), we argue without going back to the before mentioned multi-recurrence. Instead, we show first in an elementary way (using just the pigeon hole principle), that there are only finitely many lines in $\mathbb{Z}^3$ the union of which contain all possible triples (x, y, z) leading to a solution of our problem. Since we have infinitely many solutions, we may assume that for infinitely many of them we have $x = d_1t + e_1,\ y = d_2t + e_2,\ z = d_3t + e_3$, where $d_1, d_2, d_3, e_1, e_2, e_3$ are fixed integers with the first three positive and t is some positive integer variable. But in this case, since α and β are also multiplicatively dependent, it follows that $u_x - 1,\ u_y - 1,\ u_z - 1$ are all polynomials in ρ^t, where ρ is some number such that $\alpha = \rho^i$ and $\beta = \pm\rho^j$ for some integers i and j. Since any two of these numbers have large greatest common divisors, it follows that these three polynomials have common roots any two of them and their product is the square of some other polynomial. The proof ends by a careful analysis of how these polynomials might share their roots with a view of getting a contradiction.

3 Preparations

Let $\mathbb{L}$ be any algebraic number field and $\mathcal{S}$ be a finitely generated multiplicative subgroup of $\mathbb{L}$. Given $N \geq 1$, a unit equation is an equation of the form

$$\sum_{i=1}^{N} a_i x_i = 1, \tag{3}$$

where $a_1, \ldots, a_N \in \mathbb{L}$ are fixed nonzero coefficients and $x_1, \ldots, x_N \in \mathcal{S}$. A solution $(x_1, \ldots, x_N)$ of the above unit equation is called *nondegenerate* if $\sum_{i \in I} a_i x_i \neq 0$ for all proper subsets $I \in \{1, \ldots, N\}$. In such a case, we will call the unit equation (3) itself nondegenerate. We record the following result about unit equations.

Lemma 2. *There are only finitely many nondegenerate solutions* $\mathbf{x} = (x_1, \ldots, x_N) \in \mathcal{S}^N$ *to the unit equation* (3).

We will use Lemma 2 several times in what follows. In our case (and for the rest of the paper), $\mathcal{S}$ is the multiplicative group generated by α and β inside $\mathbb{K}$; i.e., $\mathcal{S} = \{\alpha^n \beta^m : n, m \in \mathbb{Z}\}$. In this special case (3) can be rewritten as

$$\sum_{i=1}^{N} a_i \alpha^{n_i} \beta^{m_i} = 1 \tag{4}$$

to be solved in integers $n_1, \ldots, n_N, m_1, \ldots, m_N$. Lemma 2 tells us that there are only finitely many $(n_1, \ldots, n_N, m_1, \ldots, m_N) \in \mathbb{Z}^{2N}$ such that no subsum on the left of (4)

vanishes. In the case when the right hand side of (4) is 0, then Lemma 2 implies that the differences $n_i - n_j, m_i - m_j$ are bounded for all $1 \le i < j \le N$ and for all $n_1, \ldots, n_N, m_1, \ldots, m_N$ such that no subsum on the left vanishes. We mention that the set of all $\mathbb{K}$-linear combinations of elements in $\mathcal{S}$ is easily understood: it is isomorphic to $\mathbb{K}[X^{\pm 1}, Y^{\pm 1}]$ in the case when α and β are multiplicatively independent and isomorphic to $\mathbb{K}[X^{\pm 1}]$ otherwise.

We will also need the following lemma. Assume that $(u_n)_{n \ge 0}$ is the nondegenerate binary recurrent sequence whose general term is given by the formula (1). Assume further that $\Delta > 0$, therefore that $|\alpha| > |\beta|$. We have the following result.

Lemma 3. *There exists constants $\kappa_0 \in (0,1)$ and z_0 such that if y and z are positive integers with $z > \max\{y, z_0\}$, $\delta\beta^z \ne 1$ and $u_y \ne 1$, then*

$$\gcd(u_y - 1, u_z - 1) < |\alpha|^{\kappa_0 z}.$$

Proof. Clearly, $|u_y - 1| \ll |u_y| \ll |\alpha|^y$. Thus, if for some small $\varepsilon > 0$ but fixed we have $y < (1-\varepsilon)z$, then we can take $\kappa_0 = 1 - \varepsilon/2$ and the desired inequality holds for large z. From now on, we shall assume that the inequalities $(1-\varepsilon)z < y < z$ hold with some small $\varepsilon > 0$ to be fixed later. Put $\lambda = z - y \in (0, \varepsilon z)$. Let $D = \gcd(u_y - 1, u_z - 1)$. Then

$$D \mid \gamma\alpha^y + \delta\beta^y - 1 \qquad \text{and} \qquad D \mid \gamma\alpha^{y+\lambda} + \delta\beta^{y+\lambda} - 1. \tag{5}$$

Multiplying the first divisibility relation above (5) by the algebraic integer α^λ, we also have that $D \mid \gamma\alpha^{y+\lambda} + \delta\beta^y\alpha^\lambda - \alpha^\lambda$. From this and the second relation (5), we get

$$D \mid \delta\beta^y(\alpha^\lambda - \beta^\lambda) - (\alpha^\lambda - 1). \tag{6}$$

Let us first assume that the algebraic integer appearing in the right hand side above is zero. We then get

$$1 = \alpha^\lambda + \delta\beta^z - \delta\beta^y\alpha^\lambda. \tag{7}$$

This is a unit equation in four terms. If it is nondegenerate, then it has only finitely many solutions. Thus, taking z_0 sufficiently large, it follows that if equation (7) holds, then it must be degenerate. In this case, one of α^λ, $\delta\beta^z$, or $-\delta\beta^y\alpha^\lambda$ equals 1. The case $\delta\beta^z = 1$ is excluded by hypothesis. The case $\alpha^\lambda = 1$ leads to $\lambda = 0$, which is impossible. Finally, the case $-\delta\beta^y\alpha^\lambda = 1$ leads to $\delta\beta^z + \alpha^\lambda = 0$, or $|\alpha|^\lambda = |\delta||\beta|^z$. If $|\beta| \ne 1$, we then get that $z\log|\beta| + \log|\delta| = \lambda\log|\alpha|$. Since $\lambda < \varepsilon z$, it follows that the above relation is impossible for large z if we choose $\varepsilon < \log|\beta|/(2\log|\alpha|)$. Thus, if $z > z_0$, then we must have $|\beta| = 1$, therefore $|\alpha|^\lambda = |\delta|$. Now the relation $-\delta\beta^y\alpha^\lambda = 1$ leads to $|\alpha|^\lambda = |\delta|^{-1}$. Thus, $|\alpha|^\lambda = |\delta| = |\delta|^{-1}$, leading to $|\delta| = 1$. We next get $|\alpha|^\lambda = 1$, therefore $\lambda = 0$, which is a contradiction.

From now on, we may assume that z is sufficiently large, and therefore that relation (7) does not hold.

Assume first that $\mathbb{K} = \mathbb{Q}$. Then the nonzero integer appearing in the right hand side of (6) is of size

$$\begin{aligned} \left|\delta\beta^y(\alpha^\lambda - \beta^\lambda) - (\alpha^\lambda - 1)\right| &\ll \exp(y\log|\beta| + \lambda\log|\alpha|) \\ &\leq \exp\left(z\left(\log|\beta| + \varepsilon\log|\alpha|\right)\right) < |\alpha|^{\kappa_0 z}, \end{aligned}$$

for a certain $\kappa_0 < 1$ (depending on ε) provided that we first choose $\varepsilon < (\log|\alpha| - \log|\beta|)/\log|\alpha|$, and then we let z be sufficiently large. This finishes the proof of the lemma in this case.

Assume now that $\mathbb{K}$ is quadratic. Conjugating (6) by the nontrivial Galois automorphism of $\mathbb{K}$ over $\mathbb{Q}$, we get

$$D \mid \gamma\alpha^y(\beta^\lambda - \alpha^\lambda) - (\beta^\lambda - 1). \tag{8}$$

Multiplying relations (6) and (8), we get

$$D^2 \mid \left(\delta\beta^y(\alpha^\lambda - \beta^\lambda) - (\alpha^\lambda - 1)\right)\left(\gamma\alpha^y(\beta^\lambda - \alpha^\lambda) - (\beta^\lambda - 1)\right),$$

and the right hand side above is a nonzero integer. Hence,

$$D^2 \ll \exp\left(y\log|\alpha\beta|\right) + 2\lambda\log|\alpha|) \leq \exp\left((\log|\alpha\beta| + 2\varepsilon\log|\alpha|)z\right).$$

Choosing $\varepsilon < (\log|\alpha| - \log|\beta|)/(2\log|\alpha|)$, one checks easily that the last inequality above leads to the conclusion that $D \leq |\alpha|^{\kappa_0 z}$ for a certain $\kappa_0 \in (0,1)$ (depending on ε) provided that z is sufficiently large. This completes the proof of Lemma 3. □

We mention that Bugeaud, Corvaja and Zannier (see [1]), showed by using the Subspace theorem that if $a > b > 1$ are multiplicatively independent integers, then for all $\varepsilon > 0$ there exists n_ε such that $\gcd(a^n - 1, b^n - 1) < \exp(\varepsilon n)$ if $n > n_\varepsilon$. Afterwards, this result was extended in various ways by various authors (see [5], [9], [14] and [20] for a sample of such extensions). The last lemma is a weak form of such a result, which is enough for our purpose, and admits an easier proof. Furthermore, we point out that a generalisation of these results to the number-field setting can be found in [5], which will also be used later.

4 Further Preliminaries and the case $\delta\beta^z = 1$

In this section, we will prove some useful information on the solutions of our problem. Especially, we will handle the case when $\delta\beta^z = 1$, which gives the exceptional solutions in the theorem.

4.1 Both z and y are large

Assume that $1 \le a < b < c$ and that $ab + 1 = u_x,\ ac + 1 = u_y$ and $bc + 1 = u_z$. We may assume that there are infinitely many such triples, therefore that $c \to \infty$. Since $|\alpha| > |\beta|$, we have

$$|u_n| = |\gamma||\alpha|^n|1 - dc^{-1}(\beta/\alpha)^n|,$$

and $(\beta/\alpha)^n$ tends to zero as $n \to \infty$. This shows that if $n > n_0$ is sufficiently large, then $|u_n| < |u_m|$ means $n < m$. Since

$$u_z = bc + 1 > \max\{u_x, u_y\} = \max\{|u_x|, |u_y|\},$$

we get that $z > \max\{x, y\}$. Further, since c is arbitrarily large and $u_y = ac + 1 > c$, it follows that y is arbitrarily large. Since $u_y = ac + 1 > ab + 1 = u_x$, it follows that if c is sufficiently large, then $y > x$. Thus, we may assume that $x < y < z$. Clearly, z tends to infinity. We shall assume that $z > z_0$, where z_0 is a sufficiently large number, not necessarily the same at each occurrence. Note that

$$u_z = |\gamma||\alpha|^z|1 - dc^{-1}(\beta/\alpha)^z| = bc + 1 \in [c, c^2],$$

showing that

$$\log c \le z \log |\alpha| + O(1) \le 2 \log c. \tag{9}$$

Since

$$u_y = |\gamma||\alpha^y||1 - dc^{-1}(\beta/\alpha)^y| = ac + 1 > c,$$

we get that

$$\log c \le y \log |\alpha| + O(1). \tag{10}$$

Estimates (9) and (10) show that $z \le 2y + O(1)$.

4.2 The case when $\delta\beta^z = 1$

Since z is large, the above relation implies $\beta = \pm 1$, therefore $\delta = \pm 1$. Hence, $\alpha \in \mathbb{Z}$. Furthermore, since $\gamma = u_0 - \delta = u_0 \pm 1$, we get that $\gamma \in \mathbb{Z}$. Moreover, $\delta\beta^y$ and $\delta\beta^x$ are both in $\{\pm 1\}$. If $\delta\beta^y = -1$, we then have

$$bc = \gamma\alpha^z \qquad \text{and} \qquad ac = \gamma\alpha^y - 2.$$

It is easy to see that for large z we have $\gcd(\gamma\alpha^z, \gamma\alpha^y - 2) = O(1)$. This shows that $c = O(1)$, therefore that $z = O(1)$. This leads to only finitely many solutions. Thus, if z is sufficiently large, then $\delta\beta^y = 1$. If also $\delta\beta^x = 1$, then

$$ab = \gamma\alpha^x, \qquad ac = \gamma\alpha^y, \qquad bc = \gamma\alpha^z,$$

therefore $(abc)^2 = \gamma^3\alpha^{x+y+z}$, implying that either γ or $\gamma\alpha$ is a perfect square, according to whether $x+y+z$ is even or odd, respectively. Assume now that $\delta\beta^x = -1$. Then

$$ab = \gamma\alpha^x - 2, \qquad ac = \gamma\alpha^y, \qquad bc = \gamma\alpha^z.$$

Furthermore, since $\delta\beta^y = \delta\beta^z = 1$ but $\delta\beta^x = -1$, it follows that $\beta = -1$, y and z have the same parity, and x has opposite parity. Since $abc^2 = \gamma^2\alpha^{y+z}$ and y and z have the same parity, it follows that ab is a perfect square. Assume now that $x \geq 2$. Then

$$ab + 2 = \gamma\alpha^x. \tag{11}$$

But since a and b divide $\gamma\alpha^y$ and $\gamma\alpha^z$, respectively, it follows that all primes dividing ab divide $\gamma\alpha$. The last relation above (11) shows now that the only prime factor of ab is 2. Hence, ab is a power of 2 and since it is a square, it is ≥ 4. Thus, $2\|ab+2$ (i.e. $2|ab+2$, but 4 does not), therefore $2\|\gamma\alpha^x$, and since $x \geq 2$, we get that $2\|\gamma$ and α is odd. Now the relations $ac = \gamma\alpha^y$ and $bc = \gamma\alpha^z$ together with the fact that ab is a power of 2, show that $a \in \{1,2\}$ and $b \in \{1,2\}$, therefore $ab \in \{1,2,4\}$. This is impossible since $1 \leq a < b$ and ab must be a perfect square. Thus, if $\delta\beta^x = -1$, then $x \in \{0,1\}$. This takes care of the exceptions (i) and (ii) appearing in the text of Theorem 1.

4.3 All three x, y and z are large

From now on, we assume that $\delta\beta^z \neq 1$. Note that $u_y = ac + 1 > 1$. Lemma 3 shows that there exists a positive constant $\kappa_0 < 1$ such that the inequality

$$\gcd(u_z - 1, u_y - 1) < |\alpha|^{\kappa_0 z}$$

holds provided that z is sufficiently large. Thus, the fact that c divides $\gcd(ac, bc) = \gcd(u_z - 1, u_y - 1)$ shows that $c < |\alpha|^{\kappa_0 z}$, leading to

$$b = \frac{u_z - 1}{c} \gg |\alpha|^{(1-\kappa_0)z}.$$

Since $|\alpha|^x \gg u_x = ab + 1 > b \gg |\alpha|^{(1-\kappa_0)z}$, it follows that $x \geq (1-\kappa_0)z + O(1)$. Thus, x tends to infinity with c also and, in fact,

$$x \asymp y \asymp z. \tag{12}$$

This will be essential when applying the Subspace theorem.

4.4 Signs of γ and α

Here, we comment on the signs of α and γ. Assume that $\alpha > 0$. Then the sign of u_n is the same as the sign of γ once $n > n_0$ is sufficiently large. Thus, if $\gamma < 0$, then there

are only finitely many n such that u_n is positive, and we obtain a contradiction. Hence, $\gamma > 0$ when $\alpha > 0$.

Assume now that $\alpha < 0$. Then for large n, the sign of u_n alternates; namely, the sign of u_n is the sign of $\gamma(-1)^n$. Thus, if $\gamma > 0$, then for large c the three numbers $x,\ y,\ z$ are even, while if $\gamma < 0$, then for large c the three numbers $x,\ y,\ z$ are odd. Thus, we may replace the pair of roots (α, β) by the pair (α^2, β^2), and keep the pair of coefficients (γ, δ) (if $\gamma > 0$), or replace it by $(\gamma\alpha, \delta\beta)$ (if $\gamma < 0$), and consequently suppose again that both α and γ are positive. From now on, we work under this assumption, namely that α and γ are positive.

4.5 a is large

Here, we shall prove a fact that will turn out to be useful later.

Lemma 4. *We have $a \to \infty$ as $z \to \infty$ through integer values such that $\delta\beta^z \neq 1$. Furthermore, in case α and β are multiplicatively independent, there exists a positive constant κ_1 such that $a > |\alpha|^{\kappa_1 z}$ when $z > z_0$.*

Proof. We start by assuming that for each $\varepsilon > 0$ there are infinitely many solutions with $a < |\alpha|^{\varepsilon z}$. We will see that this condition with a sufficiently small $\varepsilon > 0$ and a sufficiently large z entails that $a = O(1)$ when α and β are multiplicatively independent. Then we shall show that this last condition leads to a contradiction without any assumption on α and β with regard to their multiplicative independence.

The equation

$$a^2 = \frac{(u_x - 1)(u_y - 1)}{(u_z - 1)} \tag{13}$$

implies

$$|a^2\alpha^z - \gamma\alpha^{x+y}| \ll a^2 \max\{|\alpha|^y|\beta|^x, |\alpha|^y, |\beta|^z\}. \tag{14}$$

By estimate (12), it follows easily that there exists a constant $\kappa_2 \in (0, 1)$ such that if $\varepsilon > 0$ is sufficiently small, then

$$|a^2\alpha^z - \gamma\alpha^{x+y}| < |\alpha|^{\kappa_2 \max\{x+y,z\}}. \tag{15}$$

Indeed, putting κ_3 for a positive constant such that $\min\{x/z, x/(x + y)\} > \kappa_3$, a little calculation shows that the estimate (15) is implied by the estimate (14) for large z when

$$\varepsilon < 2^{-1}\kappa_3 \min\{\log|\alpha|, \log|\alpha/\beta|\}$$

with some constant κ_2 (depending on ε) provided that $z > z_0$ (here, z_0 also depends on ε). Assume that $x + y \geq z$ since the other case can be dealt with similarly. Then

$$|a^2\alpha^{z-x-y} - \gamma| < \frac{1}{|\alpha|^{(1-\kappa_2)(x+y)}}. \tag{16}$$

This shows that $z-x-y=O(\varepsilon z)$. Our next aim is to deduce for $z>z_0$ that the left hand side of (16) has to be zero. Indeed, if $\mathbb{K}=\mathbb{Q}$, and the left hand side is not zero, then its naïve height is $\exp(O(\varepsilon z))$. By the Liouville principle, if ε is sufficiently small and z is large, then inequality (16) cannot hold. If $\mathbb{K}$ is quadratic, and the right hand side is not zero, then its conjugate is $a^2\beta^{z-x-y}-\delta$. Thus, the height of this number is again $\exp(O(\varepsilon z))$. By the Liouville principle again, we arrive at a contradiction in inequality (16) for small $\varepsilon>0$, assuming that its left hand side is nonzero.

Hence, for $z>z_0$, it follows that $a=\pm\gamma^{1/2}\alpha^{(x+y-z)/2}$. Now equation (13) is

$$\begin{aligned} a^2\delta\beta^z-a^2 &= \gamma\delta(\alpha^x\beta^y+\alpha^y\beta^x)+\delta^2\beta^{x+y}-\gamma\alpha^x \\ &- \gamma\alpha^y-\delta\beta^x-\delta\beta^y+1, \end{aligned} \tag{17}$$

with $a=\pm\gamma^{1/2}\alpha^{(x+y-z)/2}$. This is a unit equation. Let $\mathcal{E}$ be some nondegenerate subequation containing the variable 1. Then any unit in $\mathcal{E}$ can take only finitely many values. If α and β are multiplicatively independent, it then follows that either $\mathcal{E}$ contains $a^2=\alpha^{x+y-z}$, or one of the other units. In the first case, $x+y-z=O(1)$, so $a=O(1)$. In the second case, one checks using the fact that α and β are multiplicatively independent, that $x=O(1)$; hence, only finitely many possibilities.

From now on, we assume that a is bounded for infinitely many solutions. Thus, infinitely many of these solutions will therefore have the same value for a. Now rewrite equation (13) (keeping in mind again that $a^2\gamma\alpha^z=\gamma^2\alpha^{x+y}$ as we did for (17)), as

$$\begin{aligned} a^2+1 &= a^2\delta\beta^z+\delta\beta^x+\delta\beta^y-\delta^2\beta^{x+y} \\ &+ \gamma\alpha^x+\gamma\alpha^y-\gamma\delta\alpha^x\beta^y-\gamma\delta\alpha^y\beta^x. \end{aligned} \tag{18}$$

This is again a unit equation. In order to discuss its degeneracies, we distinguish several cases.

Assume first that α and β are multiplicatively independent. Then there must be a nondegenerate subequation containing the left side ($a^2+1\neq 0$) and some member from the right hand side. There are only finitely many such subequations, and each one of them has only finitely many solutions. In each one of the cases, we get that $x=O(1)$; hence, only finitely many possibilities.

Assume now that α and β are multiplicatively dependent. In this case, there exists $\rho>1$ and coprime integers $i>j$ such that $\alpha=\rho^i$ and $\beta=\pm\rho^j$.

If $j>0$, then again there must be some non-degenerate subequation of equation (18) containing the fixed nonzero number a^2+1 from the left hand side and some variable from the right hand side. This leads to $x=O(1)$; hence, only finitely many possibilities.

If $j=0$, then $\beta=\pm1$, $\alpha>1$ and $\gamma,\ \delta$ are all integers. We may also assume that the class of (x,y,z) in $(\mathbb{Z}/2\mathbb{Z})^3$ is fixed. Thus, the three numbers $\delta\beta^x,\ \delta\beta^y$ and $\delta\beta^z$ are fixed in $\{\pm\delta\}$. We rewrite equation (18) as

$$\begin{aligned} a^2+1 &- a^2\delta\beta^z-\delta\beta^x-\delta\beta^y+\delta^2\beta^{x+y} \\ &= \gamma(1-\delta\beta^y)\alpha^x+\gamma(1-\delta\beta^x)\alpha^y. \end{aligned}$$

The left hand side as well as the coefficients $\gamma(1-\delta\beta^y)$ and $\gamma(1-\delta\beta^x)$ from the right hand side of α^x and α^y, respectively, are fixed. Assume first that these coefficients are zero. Then $\delta\beta^x = \delta\beta^y = 1$ and the left hand side must also be zero. This leads to $a^2(1-\delta\beta^z) = 0$, therefore $\delta\beta^z = 1$, which is not allowed. Thus, at least one of the two coefficients $\gamma(1-\delta\beta^y)$ and $\gamma(1-\delta\beta^x)$ from the right hand side is nonzero. Note that the left hand side is a fixed integer. Thus, if the left hand side is nonzero, then equation (18) is a unit equation with $N = 1$ or 2 according to whether one or none of the coefficients of α^x and α^y from the right hand side vanishes. This leads again to $x = O(1)$; hence, only finitely many possibilities. Assume now that the right hand side is zero. Then

$$\alpha^{y-x} = -\frac{1-\delta\beta^y}{1-\delta\beta^x}, \qquad a^2 = -\frac{(1-\delta\beta^x)(1-\delta\beta^y)}{1-\delta\beta^z}.$$

Since $\alpha > 1$, it follows from the first of the above two equations that the cases $\beta = 1$, or $\beta = -1$ and $x \equiv y \pmod 2$ are impossible. Thus, up to replacing δ by $-\delta$ if needed, we may assume that

$$\alpha^{y-x} = -\frac{(1-\delta)}{(1+\delta)}.$$

Since $y > x$ and α is an integer, we get that $1+\delta \mid 1-\delta$. Thus, $1+\delta \mid 2$ leading to $1+\delta = -2,\ -1,\ 1,\ 2$. The cases $\delta = 1+\delta = 1,\ 2$ lead to $\delta = 0$, which is not allowed, and $\alpha = 0$, which is not allowed either. The cases $1+\delta = -2,\ -1$ give $\alpha^{y-x} = 2,\ 3$, respectively. Thus, $\alpha = 2,\ 3$, respectively, and $y = x+1$. Now

$$a^2 = -\frac{(1-\delta\beta^x)(1-\delta\beta^y)}{(1-\delta\beta^z)} = -\frac{1-\delta^2}{1\pm\delta} \in \{-4,-3,2,1\},$$

so the only possibility is that $a = 1$. This happens if $\delta = -2$ and $a^2 = -(1+\delta)$, therefore $1-\delta\beta^z = 1-\delta$, so z is even. On the other hand, $1 = a = \gamma^{1/2}\alpha^{(x+y-z)/2}$ and γ and α are positive integers, therefore $\gamma = 1$ and $z = x+y = 2x+1$ is odd. This contradiction shows that it is not possible that the left hand side of equation (18) is zero and not both of the coefficients $\gamma(1-\delta\beta^y)$ and $\gamma(1-\delta\beta^x)$ of α^y and α^x, respectively, from its right hand side be zero. Hence, if $j = 0$, then there are only finitely many possibilities for $x,\ y$ and z.

Finally, assume that $j < 0$. Then $j = -1$, $i = 1$, so $\beta = \pm\alpha^{-1}$. Rewrite equation (18) as

$$\begin{aligned} a^2+1 &- a^2\delta\beta^z - \delta\beta^x - \delta\beta^y + \delta^2\beta^{x+y} + \gamma\delta(\alpha^x\beta^y + \alpha^y\beta^x) \\ &= \gamma(\alpha^x + \alpha^y). \end{aligned}$$

Its right hand side is $\gg \alpha^y$. Its left hand side is in absolute value $\ll \alpha^{y-x}$, since $\beta = \pm\alpha^{-1}$. Thus, $\alpha^{y-x} \gg \alpha^y$, leading to $\alpha^x \ll 1$, therefore $x = O(1)$; hence, finitely many possibilities.

Having analyzed all the possible scenarios and having arrived to only finitely many possibilities in each case, we conclude that $a = O(1)$ leads to only finitely many possibilities. Thus, it must be the case that $a \to \infty$ as $z \to \infty$. Furthermore, in case α and β are multiplicatively independent, we have $a > |\alpha|^{\kappa_1 z}$ when $z > z_0$, where $\kappa_1 > 0$ is some constant. □

We saw that $\delta\beta^z \neq 1$. For future use, we also record that $\delta\beta^y \neq 1$ and $\delta\beta^x \neq 1$. Indeed, if say $\delta\beta^x = 1$, then $\beta = \pm 1$ and $a \mid \gcd(\gamma\alpha^z + (\delta\beta^z - 1), \gamma\alpha^x)$. Since $\delta\beta^z - 1 = O(1)$ is nonzero, it follows easily that a is bounded, which is a contradiction. The similar contradiction that $b = O(1)$ is obtained if one assumes that $\delta\beta^y = 1$.

5 The case α and β multiplicatively independent

In this section we will finish the proof of the theorem in the case when α and β are multiplicatively independent. This will be done by applying Theorem 1 of [11], which follows from the general result from [6] (see also [3], [4], [10], or [12]). We will indicate the proof to see that we get an additional piece of information which is not stated explicitly, although well-known, in [11, Theorem 1]. Then we show that the assumption of α and β being multiplicatively independent leads to a contradiction. As a first independent step we show that $\min\{y - x, y - 2x, z - 2x\} = O(1)$ in this case. Afterwards, the contradiction is derived.

5.1 An application of the Subspace theorem

The three relations (2) yield

$$(u_x - 1)(u_y - 1)(u_z - 1) = (abc)^2. \tag{19}$$

Note that

$$(u_x - 1)(u_y - 1)(u_z - 1) = \gamma^3\alpha^{x+y+z}(1 + \eta),$$

where

$$\eta = \prod_{t\in\{x,y,z\}} \left(\gamma_1 \left(\frac{\beta}{\alpha}\right)^t + \delta_1 \left(\frac{1}{\alpha}\right)^t\right),$$

with $\gamma_1 = \delta/\gamma$ and $\delta_1 = -1/\gamma$. Thus,

$$abc = \gamma^{3/2}\alpha^{(x+y+z)/2}(1 + \eta)^{1/2} = \gamma^{3/2}\alpha^{(x+y+z)/2} \sum_{k\geq 0} \binom{1/2}{k} \eta^k.$$

Furthermore, using the binomial formulae, for each k we have

$$\eta^k = \sum_{(\mathbf{i},\mathbf{j})\in\Gamma_k} c_{(\mathbf{i},\mathbf{j})}\alpha^{-i_1x - i_2y - i_3z}\beta^{j_1x + j_2y + j_3z},$$

where Γ_k is the set of all sextuples $(\mathbf{i},\mathbf{j})$ with $\mathbf{i}=(i_1,i_2,i_3)$, $\mathbf{j}=(j_1,j_2,j_3)$ fulfilling $i_1+i_2+i_3=k$, and $0\le j_\ell\le i_\ell$ for all $\ell=1,2,3$, while $c_{(\mathbf{i},\mathbf{j})}$ are certain coefficients in $\mathbb{K}$ indexed over the members of Γ_k.

Since $x,\ y$ and z have the same order of magnitude, the arguments from [11] show that there exists a finite set Λ of sextuples $(\mathbf{i},\mathbf{j})$ (note that if $(\mathbf{i},\mathbf{j})$ is given, then k is the sum of the entries in $\mathbf{i}$), and nonzero coefficients $d_{(\mathbf{i},\mathbf{j})}\in\overline{\mathbb{Q}}$ for $(\mathbf{i},\mathbf{j})\in\Lambda$, such that infinitely many of the solutions $(a,b,c;x,y,z)$ have the property that

$$abc=\alpha^{(x+y+z)/2}\sum_{(\mathbf{i},\mathbf{j})\in\Lambda} d_{(\mathbf{i},\mathbf{j})}\alpha^{-i_1x-i_2y-i_3z}\beta^{j_1x+j_2y+j_3z}. \tag{20}$$

From now on, we work only with such solutions. We insert abc given by formula (20) into formula (19) and we end up with

$$(u_x-1)(u_y-1)(u_z-1)=\alpha^{x+y+z}\left(\sum_{(\mathbf{i},\mathbf{j})\in\Lambda} d_{(\mathbf{i},\mathbf{j})}\alpha^{-i_1x-i_2y-i_3z}\beta^{j_1x+j_2y+j_3z}\right)^2 \tag{21}$$

which upon expansion of both sides above leads to an $\mathcal{S}$-unit equation with infinitely many solutions. We now study this equation.

5.2 $\min\{y-x,y-2x,z-2x\}=O(1)$ when α and β are multiplicatively independent

We order the units appearing on the left had side of the unit equation (21) according to their sizes of their absolute values.

5.2.1 The case $|\beta|>1$.

It is then easy to see that

$$\begin{aligned}(u_x-1)(u_y-1)(u_z-1) &= \gamma^3\alpha^{x+y+z}+\gamma^2\delta\alpha^{z+y}\beta^x+\gamma^2\delta\alpha^{z+x}\beta^y\\ &+ \gamma^2\delta\alpha^{x+y}\beta^z+\gamma\delta^2\alpha^z\beta^{x+y}+\text{smaller units}.\end{aligned} \tag{22}$$

We claim that for large z, we have

$$\alpha^{z+y}|\beta|^x>\alpha^{z+x}|\beta|^y>\alpha^{x+y}|\beta|^z>\alpha^z|\beta|^{x+y}.$$

Indeed, the ratios of any two consecutive expressions above are

$$\left(\frac{\alpha}{|\beta|}\right)^{y-x},\ \left(\frac{\alpha}{|\beta|}\right)^{z-y},\ \left(\frac{\alpha}{|\beta|}\right)^{x+y-z}.$$

The first two expressions are certainly > 1 and they remain bounded only when $y - x = O(1)$ and $z - y = O(1)$, and the fact that the third one tends to infinity as $z \to \infty$ is a consequence of Lemma 4 and of the fact that $\alpha^{x+y-z} \gg a^2 \geq \alpha^{\kappa_1 z}$.

We now insert the right hand side of (22) in (21) and use Lemma 2 (see also the remarks made below Lemma 2). We may assume that α^{x+y+z} cancels from both sides of equation (21). Indeed, if not, then $(\mathbf{0}, \mathbf{0}) \notin \Lambda$, and the largest unit present in the right hand side is $\leq \alpha^{y+z-x}|\beta|^{2x}$. Let $\mathcal{E}$ be some nondegenerate subequation containing α^{x+y+z}. If $\mathcal{E}$ contains some unit from the right hand side of (21), we deduce that the ratio of α^{x+y+z} to $\alpha^{y+z-x}|\beta|^{2x}$ is bounded; hence, $(\alpha/|\beta|)^{2x} = O(1)$, leading to $x = O(1)$; thus, only finitely many possibilities. If on the other hand $\mathcal{E}$ contains some other unit from the left hand side of equation (21), then the ratio of α^{x+y+z} to $\alpha^{y+z}|\beta|^x$ is bounded. Thus, again $(\alpha/|\beta|)^x = O(1)$, which leads to only finitely many possibilities. From now on, we assume that α^{x+y+z} cancels from both sides of equation (21), so in particular that $(\mathbf{0}, \mathbf{0}) \in \Lambda$.

Let $\mathcal{E}$ be some nondegenerate subequation containing $\alpha^{z+y}\beta^x$.

If $\mathcal{E}$ contains either $\alpha^z\beta^{x+y}$ or one of the smaller units, then the ratio of $\alpha^{z+y}\beta^x$ to $\alpha^z\beta^{z+y}$ stays bounded. This gives $(\alpha/|\beta|)^y = O(1)$, therefore $y = O(1)$; thus, only finitely many possibilities.

If $\mathcal{E}$ contains either $\alpha^{z+x}\beta^y$, or $\alpha^{x+y}\beta^z$, we then get that $(\alpha/|\beta|)^{y-x} = O(1)$, which is what we are after.

If $\mathcal{E}$ does not contain any unit from the left hand side of (21), then it must contain one from the right hand side. Hence, the ratio of

$$\alpha^{y+z}\beta^x \qquad \text{to} \qquad \alpha^{x+y+z}\frac{\beta^{j_1x+j_2y+j_3z}}{\alpha^{i_1x+i_2y+i_3z}}$$

is bounded for some $(\mathbf{i}, \mathbf{j}) \in \Lambda$ with $i_1 + i_1 + i_3 = k \neq 0$. Thus,

$$\alpha^{(i_1-1)x+i_2y+i_3z} \ll |\beta|^{(j_1-1)x+j_2y+j_3z}. \tag{23}$$

Since $j_\ell \leq i_\ell$ for $\ell = 1, 2, 3$, it follows that $(\alpha/|\beta|)^{(i_1-1)x+i_2y+i_3z} \ll 1$. If $i_2 + i_3 > 0$, we then get $y - x \ll 1$, which is what we want. Thus, $i_2 = i_3 = 0$, and since $k > 0$, we get that $i_1 \geq 1$. If $i_1 \geq 2$, we then get $x = O(1)$, so we get only finitely many possibilities. Thus, infinitely many of the solutions will have $\mathbf{i}_0 = (1, 0, 0)$. If $j_1 = 0$, then estimate (23) shows that $|\beta|^x \asymp 1$, therefore again $x = O(1)$. Hence, $j_1 = 1$ for infinitely many solutions. This shows that for $\mathbf{i}_0 = (1, 0, 0)$ and $\mathbf{j}_0 = (1, 0, 0)$ we have that $(\mathbf{i}_0, \mathbf{j}_0) \in \Lambda$. In particular, $\alpha^{x+y+z}(\beta/\alpha)^{2x}$ appears in the formula for $(abc)^2$. Let $\mathcal{F}$ be some nondegenerate equation that contains this variable.

If $\mathcal{F}$ contains a unit from the left hand side equal to $\alpha^z\beta^{x+y}$ or smaller, we then get that the ratio of

$$\alpha^{x+y+z}\left(\frac{\beta}{\alpha}\right)^{2x} \qquad \text{to} \qquad \alpha^z\beta^{x+y}$$

is $O(1)$. This implies that $(\alpha/|\beta|)^{y-x} \ll 1$, or $y - x = O(1)$, which is what we want.

If $\mathcal{F}$ contains a unit from the left hand side which is in

$$\{\alpha^{y+z}\beta^x,\ \alpha^{z+x}\beta^y,\ \alpha^{x+y}\beta^z\},$$

we then get that the ratio of $\alpha^{y+z-x}\beta^{2x}$ to one of these three units belongs to a fixed finite set of numbers. Thus, one of

$$\left(\frac{\alpha}{\beta}\right)^x, \qquad \left(\frac{\alpha}{\beta}\right)^{y-2x}, \qquad \left(\frac{\alpha}{\beta}\right)^{z-2x}$$

belongs to a fixed finite set of numbers. The first possibility gives $x = O(1)$, so only finitely many possibilities. The second and third show that $y - 2x = O(1)$, or $z - 2x = O(1)$, which is what we wanted.

Assume now that $\mathcal{F}$ does not contain any unit from the left hand side of equation (21). Then it must contain some unit from the right hand side. Thus, there must exist $(\mathbf{i}_1, \mathbf{j}_1) \neq (2\mathbf{i}_0, 2\mathbf{j}_0)$ such that the ratio of $(\beta/\alpha)^{2x}$ to $\beta^{j_1'x+j_2'y+j_3'z}/\alpha^{i_1'x+i_2'y+i_3'z}$ belongs to a finite set of numbers. Here, $\mathbf{i}_1 = (i_1', i_2', i_3')$ and $\mathbf{j}_1 = (j_1', j_2', j_3')$. Put $k = i_1' + i_2' + i_3'$. If $k \geq 3$, then

$$\frac{|\beta|^{j_1'x+j_2'y+j_3'z}}{\alpha^{i_1'x+i_2'y+i_3'z}} \ll \left(\frac{|\beta|}{\alpha}\right)^{3x},$$

and so we get that $(\alpha/|\beta|)^x \ll 1$, showing that $x = O(1)$; hence, again only finitely many possibilities. If $k = 2$, then it is easy to see that units of this shape of maximal absolute value not equal to $(\beta/\alpha)^{2x}$ have maximal value at most $(|\beta|/\alpha)^{x+y}$. So, the ratio of $(\beta/\alpha)^{2x}$ to such a unit is $\gg (\alpha/|\beta|)^{y-x}$. Hence, $(\alpha/|\beta|)^{y-x} \ll 1$, showing that $y - x = O(1)$, which is what we want.

The only elements in $\mathcal{F}$ with $k = 1$ are

$$\frac{1}{\alpha^x}, \quad \frac{1}{\alpha^y}, \quad \frac{1}{\alpha^z}, \quad \left(\frac{\beta}{\alpha}\right)^x, \quad \left(\frac{\beta}{\alpha}\right)^y, \quad \left(\frac{\beta}{\alpha}\right)^z.$$

Thus, the ratio of $(\beta/\alpha)^{2x}$ to one of the above six units belongs to some finite set of numbers. If one of these six units is one of the first four, then we get that one of $\beta^{2x}\alpha^{-x}$, $\beta^{2x}\alpha^{y-x}$, $\beta^{2x}\alpha^{z-x}$, or $(\beta/\alpha)^x$ belongs to a finite list of numbers. Since α and β are multiplicatively independent, we get that $x = O(1)$; hence, there are only finitely many possibilities. Finally, if one of these six units is one of the last two, we then get that one of $(\beta/\alpha)^{2x-y}$ or $(\beta/\alpha)^{2x-z}$ belongs to a fixed finite set of numbers. Thus, $y - 2x = O(1)$ or $z - 2x = O(1)$, as we wanted.

This finishes the case when $|\beta| > 1$.

5.2.2 The case $|\beta| < 1$

Here, we just sketch the main steps since the argument is very similar to the previous one. Instead of (22), we have

$$\begin{aligned}(u_x-1)(u_y-1)(u_z-1) &= \gamma^3\alpha^{x+y+z} - \gamma^2\alpha^{z+y} - \gamma^2\alpha^{z+x} \\ &- \gamma^2\alpha^{x+y} + \gamma\alpha^z + \text{smaller units.} \end{aligned} \tag{24}$$

The main roots are, in decreasing order of their absolute values,

$$\alpha^{x+y+z},\ \alpha^{y+z},\ \alpha^{z+x},\ \alpha^{x+y},\ \alpha^z,$$

and the ratios between any two consecutive ones is

$$\alpha^x,\ \alpha^{y-x},\ \alpha^{z-y},\ \alpha^{x+y-z},$$

respectively. The last one tends to infinity with z by Lemma 4. The same argument as the one used at the case $|\beta| > 1$ shows that one may assume that the unit α^{x+y+z} cancels from both sides of the unit equation (21), for otherwise we get $x = O(1)$; hence, only finitely many possibilities. Thus, $(\mathbf{0}, \mathbf{0}) \in \Lambda$.

Let $\mathcal{E}$ be again some nondegenerate subequation of (21) containing α^{y+z} in the left hand side. If it contains some other unit from the left hand side which is α^z or smaller in absolute value, we get that $\alpha^y = (\alpha^{y+z})/\alpha^z = O(1)$. Thus, we have only finitely many possibilities. If $\mathcal{E}$ contains one of the units α^{z+x} or α^{x+y} from the left hand side, we then get $\alpha^{y-x} = O(1)$, which is what we want. Suppose now $\mathcal{E}$ contains some unit from the left hand side, say of the form

$$\alpha^{x+y+z}\frac{\beta^{j_1x+j_2y+j_3z}}{\alpha^{i_1x+i_2y+i_3z}},$$

where $k = i_1 + i_2 + i_3 > 0$. Then

$$\alpha^{(i_1-1)x+i_2y+i_3z} \ll \beta^{j_1x+j_2y+j_3z}.$$

Since $|\beta| < 1$, the above inequality leads easily to the conclusion that $x = O(1)$, unless $\mathbf{i}_0 = (i_1, i_2, i_3) = (1, 0, 0)$ and $\mathbf{j}_0 = (j_1, j_2, j_3) = (0, 0, 0)$. Thus, $(\mathbf{i}_0, \mathbf{j}_0) \in \Lambda$, which shows that its square appears in the right hand side of equation (21). Let $\mathcal{F}$ be some subequation containing α^{y+z-x} appearing on the right hand side of (21). Assume that $\mathcal{F}$ contains some unit from the left hand side of (21). If this is α^z or some unit of a smaller absolute value, we get that $\alpha^{y-x} \ll O(1)$. Thus, $y - x = O(1)$, which is what we want. If it contains one of $\alpha^{y+z},\ \alpha^{x+z}$, or α^{x+y}, then one of the numbers $\alpha^x,\ \alpha^{y-2x}$ or α^{z-2x} belongs to a finite list. Thus, either $x = O(1)$, which happens for only finitely many possibilities, or $\min\{y - 2x,\ z - 2x\} = O(1)$, which is what we want.

Finally, assume that $\mathcal{F}$ contains some other unit from the right hand side of equation (21) of the form $\alpha^{x+y+z}\beta^{j_1'x+j_2'y+j_3'z}/\alpha^{i_1'x+i_2'y+i_3'z}$. We scale everything by α^{x+y+z}. If $k \geq 3$,

then the largest such unit in absolute value is $1/\alpha^{3x}$. The ratio of $1/\alpha^{2x}$ to this unit is $\gg \alpha^x$, so if this ratio is in a finite set of numbers, we then get $x = O(1)$; hence, only finitely many possibilities. If $k = 2$, then the largest such unit in absolute value which is not $1/\alpha^{2x}$ is $\leq 1/\alpha^{x+y}$. The ratio of $1/\alpha^{2x}$ to such a unit is $\gg \alpha^{y-x}$. So, if this ratio is in a finite set, we get $y - x = O(1)$, as desired. Finally, the only possibilities when $k = 1$ are

$$\frac{1}{\alpha^x}, \quad \frac{1}{\alpha^y}, \quad \frac{1}{\alpha^z}, \quad \left(\frac{\beta}{\alpha}\right)^x, \quad \left(\frac{\beta}{\alpha}\right)^y, \quad \left(\frac{\beta}{\alpha}\right)^z.$$

If $\mathcal{F}$ contains one of these units, we then get that one of

$$\alpha^x, \ \alpha^{y-x}, \ \alpha^{z-x}, \ (\alpha\beta)^x, \ \alpha^{y-2x}\beta^{-y}, \ \alpha^{z-2x}\beta^{-z}$$

belongs to a finite list. In the first case, we get $x = O(1)$. In the next two, we get $y - x = O(1)$, as desired. Finally, since α and β are multiplicatively independent, in the last three cases we get $x = O(1)$; hence, finitely many possibilities also.

In conclusion, we proved that both when $|\beta| > 1$ and $|\beta| < 1$, assuming that α and β are multiplicatively independent, infinitely many of the solutions will have one of $y - x$, $y - 2x$, or $z - 2x$ bounded.

5.3 Proof of the theorem for α and β multiplicatively independent

Suppose first that $y - x = \lambda$ is a fixed number for infinitely many of our solutions. Then

$$a \mid \gamma\alpha^x + \delta\beta^x - 1 \qquad \text{and} \qquad a \mid \gamma\alpha^{x+\lambda} + \delta\beta^{x+\lambda} - 1.$$

Multiplying the first equation relation above by α^λ and subtracting them, we get that

$$a \mid \delta\beta^x(\alpha^\lambda - \beta^\lambda) - (\alpha^\lambda - 1), \tag{25}$$

and, as in the proof of Lemma 3, the right hand side above is nonzero for $z > z_0$. Note further that $\alpha^\lambda - \beta^\lambda \neq 0$ because $\lambda \neq 0$ and α/β is not a root of 1. Put $\zeta = \delta^{-1}(\alpha^\lambda - 1)/(\alpha^\lambda - \beta^\lambda)$. Note that $\zeta \neq 0$. Relation (25) shows that

$$a \mid \kappa_4(\beta^x - \zeta),$$

where we can take κ_4 to be some fixed positive integer which is divisible by the norm of $|\alpha^\lambda - \beta^\lambda|$ with respect to $\mathbb{K}$. The same argument (interchanging α with β) shows that

$$a \mid \kappa_4(\alpha^x - \eta),$$

where $\eta = \gamma^{-1}(\beta^\lambda - 1)/(\beta^\lambda - \alpha^\lambda)$. The fact that $\eta \neq 0$ follows because $\beta \neq \pm 1$ and $\lambda \neq 0$. Furthermore, both $\alpha^x - \eta$ and $\beta^x - \zeta$ are nonzero. Hence,

$$a \ll N_{\mathbb{K}}\left(\gcd(\alpha^x - \eta, \beta^x - \zeta)\right),$$

where the last expression is to be interpreted as the norm of the ideal greatest common divisor of the two algebraic numbers in $\mathbb{K}$ (see also [20]). Since α and β are multiplicatively independent, the Main Theorem from [5, p. 205] shows that $a = \exp(o(x))$ as $x \to \infty$. This contradicts Lemma 4 for large values of x.

Suppose now that $y - 2x = \lambda$ for some fixed value of λ. We will get the contradiction by a similar argument as in the first case. It follows

$$a \mid \gamma\alpha^x + (\delta\beta^x - 1) \mid (\gamma\alpha^x)^2 - (\delta\beta^x - 1)^2.$$

Thus,

$$a \mid \gamma^2\alpha^{2x} - \delta^2\beta^{2x} + 2\delta\beta^x - 1 \qquad \text{and} \qquad a \mid \gamma\alpha^{2x+\lambda} + \delta\beta^{2x+\lambda} - 1.$$

Multiplying the first relation above by α^λ, the second by γ, and subtracting them, we get

$$a \mid \beta^{2x}\delta(\gamma\beta^\lambda + \delta\alpha^\lambda) - 2\delta\alpha^\lambda\beta^x + \alpha^\lambda - \gamma.$$

The last expression above is nonzero for large x. Indeed, this expression is a polynomial of degree at most 2 in β^x. If it were zero, then it must happen that all three coefficients $\delta(\gamma\beta^\lambda + \delta\alpha^\lambda)$, $-2\delta\alpha^\lambda$ and $\alpha^\lambda - \gamma$ are zero, which is not the case since $\delta\alpha \neq 0$. Thus,

$$a \mid \kappa_4 P(\beta^x),$$

where $P(\beta^x)$ is a nonzero monic polynomial of degree at most 2. Interchanging β to α in the previous argument, we get that

$$a \mid \kappa_4 Q(\alpha^x),$$

where $Q(X) \in \mathbb{K}[X]$ is some nonzero polynomial of degree at most 2. Hence, at the level of ideals,

$$a \mid \kappa_4 \prod_{\substack{\zeta,\eta \\ P(\zeta)=0,\ Q(\eta)=0}} N_{\mathbb{L}}\left(\gcd(\beta^x - \zeta, \alpha^x - \eta)\right),$$

where $\mathbb{L}$ is the splitting field over $\mathbb{K}$ of $P(X)Q(X)$ and where the roots ζ and η of $P(X)$ and $Q(X)$ in $\mathbb{L}$, respectively, are counted with their multiplicities. If $\zeta\eta \neq 0$, then $N_{\mathbb{K}}(\gcd(\beta^x - \zeta, \alpha^x - \eta)) = |\alpha|^{o(x)}$ as $x \to \infty$ by [6, Main Theorem, p. 205]. It remains to deal with the case when one of ζ or η is zero. Assume say that $\zeta = 0$. Let π be any prime ideal dividing β in $\mathbb{K}$. All we need to understand is an upper bound for $\mu_\pi(a)$, where for a number $\omega \in \mathbb{K}$ we use $\mu_\pi(\omega)$ for the exponent of π in the factorization of ω in prime ideals inside $\mathbb{K}$. If π divides also α, then π does not divide $u_x - 1$ for large x. Thus, $\mu_\pi(a) = 0$ in this case. If π does not divide α, then

$$\mu_\pi(u_x - 1) = \mu_\pi(\gamma\alpha^x + \delta\beta^x - 1) \leq \min\{x, \mu_\pi(\gamma\alpha^x - 1)\}.$$

By linear forms in π-adic logarithms (see, for example, [21]),

$$\mu_\pi(\gamma\alpha^x - 1) \ll \log x.$$

Thus, for large x, $\mu_\pi(a) \le \mu_\pi(u_x - 1) \ll \log x$. A similar argument applies to the ideals dividing α. This argument shows that the roots $\zeta\eta = 0$ contribute a factor of size $|\alpha|^{O(\log x)} = |\alpha|^{o(x)}$ as $x \to \infty$ in a. Consequently,

$$a \le |\alpha|^{o(x)}$$

holds as $x \to \infty$, contradicting again Lemma 4.

The same argument works also in the case $z - 2x = O(1)$, the role of a being played by b. We give no further details.

6 The case α and β multiplicatively dependent

We begin with some remarks about the case when α and β are multiplicatively dependent. Since they are also either rational or quadratic integers, there exist $\rho > 1$, coprime integers $i > 0$ and j, and $\eta \in \{\pm 1\}$, such that $\alpha = \rho^i$ and $\beta = \eta\rho^j$. If $j \ge 0$, then ρ is a rational integer. Otherwise, $i = 1,\ j = -1$, and ρ is a quadratic unit.

Observe now that if $j \ge 0$, then

$$u_n - 1 = \gamma(\rho^n)^i + \eta^n\delta(\rho^n)^j - 1$$

is a polynomial in ρ^n when $\eta = 1$, and one of two polynomials when $\eta = -1$ according to whether n is even or odd. When $j = -1$, then

$$u_n = \rho^{-n}(\gamma(\rho^n)^2 - \rho^n + \eta^n\delta)$$

is associated (because ρ^{-n} is a unit) to one (if $\eta = 1$), or one of the two (if $\eta = -1$) polynomials of degree 2 in ρ^n with coefficients in $\mathbb{K}$. The following result is very important in what follows.

Lemma 5. *All solutions (x, y, z) of equation (2) are contained in the union of finitely many lines in $\mathbb{Z}^3$.*

Proof. We let b_1 and c_1 be the largest divisors of b and c, respectively, which are free of primes dividing ρ. Note that both b/b_1 and c/c_1 are $O(1)$. Indeed, if $j > 0$, then $\rho > 1 \in \mathbb{Z}$ and $u_n - 1$ is coprime to ρ for all n sufficiently large. If $j < 0$, then ρ is a unit, so $b_1 = b$ and $c_1 = c$. Finally, if $j = 0$, then, since $\delta\beta^z \ne 1$ and $\delta\beta^y \ne 1$, we get that $\delta\beta^z - 1 = O(1)$ and $\delta\beta^y - 1 = O(1)$ are both nonzero.

This justifies that $b/b_1 = O(1)$ and $c/c_1 = O(1)$.

We now fix the class of (x, y, z) modulo $(\mathbb{Z}/2\mathbb{Z})^3$. For $j \geq 0$, we may write

$$\begin{aligned} bc &= u_z - 1 = \gamma P(\rho^z) = \gamma \prod_{i=1}^{\ell} (\rho^z - \mu_i)^{\sigma_i}, \\ ac &= u_y - 1 = \gamma Q(\rho^y) = \gamma \prod_{j=1}^{\ell'} (\rho^y - \mu'_j)^{\sigma'_\ell}. \end{aligned}$$

In the above formulae, $\mu_1, \ldots, \mu_\ell$ are all the distinct roots of $P(X)$ having multiplicities $\sigma_1, \ldots, \sigma_\ell$, respectively. Similarly, $\mu_1, \ldots, \mu_{\ell'}$ are the distinct roots of $Q(X)$ of multiplicities $\sigma'_1, \ldots, \sigma'_{\ell'}$, respectively. Note that $\mu_1, \ldots, \mu_\ell, \mu'_1, \ldots, \mu'_{\ell'}$ are all nonzero. Note also that $P(X)$ and $Q(X)$ have degrees i. When $j < 0$, then we write

$$bc = u_z - 1 = \gamma \rho^{-z} P(\rho^z), \qquad \text{and} \qquad ac = u_y - 1 = \gamma \rho^{-y} Q(\rho^y),$$

where now $P(X)$ and $Q(X)$ are quadratic polynomials. We keep the notations $\mu_i,\ \sigma_i$ and $\mu'_j,\ \sigma'_j$ with $1 \leq i \leq \ell,\ 1 \leq j \leq \ell'$ for the distinct roots with their corresponding multiplicities of $P(X)$ and $Q(X)$, respectively.

In all cases, we put d for the common degree of $P(X)$ and $Q(X)$.

We now write $\sigma = \max\{\sigma_i, \sigma'_j : 1 \leq i \leq \ell,\ 1 \leq j \leq \ell'\}$, $\mathbb{L}$ for the splitting field of $P(X)Q(X)$ over $\mathbb{K}$, and κ_5 for a positive integer divisible by the denominators of γ, μ_i and μ'_j for all $1 \leq i \leq \ell$ and $1 \leq j \leq \ell'$. We then get that

$$\begin{aligned} c_1 \ &| \ \gcd(u_z - 1, u_y - 1) \mid \gcd(\gamma P(\rho^z), \gamma Q(\rho^y)) \\ &| \ \kappa_5^{d^3+1} \gamma \prod_{\substack{1 \leq i \leq s \\ 1 \leq j \leq t}} \gcd\left(\rho^z - \mu_i, \rho^y - \mu'_j\right)^{\sigma}. \end{aligned} \tag{26}$$

The last product above is to be interpreted as a product of ideals in $\mathbb{L}$.

Now let $T > 2$ be a large positive integer. Consider the set of numbers $\mathcal{T} = \{pz+qy : 1 \leq p \leq T,\ 1 \leq q \leq T\}$. Clearly, all numbers in $\mathcal{T}$ are $\leq 2zT$ for large z. Since there are T^2 pairs of positive integers $(p, q) \in [1, T]^2$, it follows, by the pigeon hole principle, that there there exist $(p, q) \neq (p', q')$ such that $|pz+qy-(p'z+q'y)| \leq 2Tz/(T^2-1) < 3z/T$. Write $u = p - p'$ and $v = q - q'$ and assume that $uz + vy \geq 0$ (otherwise, we replace the pair (u, v) by the pair $(-u, -v)$). For $1 \leq i \leq \ell$ and $1 \leq j \leq \ell'$, put $c_{1,i,j}$ for the ideal $\gcd(c_1, \rho^z - \mu_i, \rho^y - \mu'_j)$ in $\mathbb{L}$. Since

$$\rho^z \equiv \mu_i \pmod{c_{1,i,j}} \qquad \text{and} \qquad \rho^y \equiv \mu'_j \pmod{c_{1,i,j}},$$

and ρ is invertible modulo c_1, we get that $\rho^{uz+vy} \equiv \mu_i^u \mu_j'^v \pmod{c_{1,i,j}}$. We thus get, using relation (26), that

$$c_1 \mid \kappa_5^{T(d^3+1)} \gamma \prod_{\substack{1 \leq i \leq \ell \\ 1 \leq j \leq \ell'}} \left(\rho^{uz+vy} - \mu_i^u \mu_j'^v\right). \tag{27}$$

Assume that the right hand side above is nonzero. Then, taking norms in $\mathbb{L}$ and using the fact that $0 \le uz + vy \ll z/T$, we get that

$$c_1 \le \exp(O(z/T + T)).$$

The constant implied by the above O depends on the sequence $(u_n)_{n\ge 0}$. Since $c_1 \gg c \gg \alpha^{z/2}$, we get that

$$\alpha^{z/2} \le \exp(O(z/T + T)),$$

therefore $z \ll z/T + T$. This inequality is false if we first choose $T > 2\kappa_6^{-1}$, where κ_6 is the constant implied by the above O, and then make z large. The contradiction comes from the fact that we have assumed that the right hand side of (27) is nonzero for $T = \lfloor \kappa_6^{-1} \rfloor + 1$ once z is large. If the right hand side of (27) is zero with this value for T, then $\rho^{uz+vy} = \mu_i^u \mu_j'^v$ for some i, j, u, v, and since ρ is not a root of 1, we get that $uz + vy$ is uniquely determined once i, j, u, v have been fixed.

We now repeat the argument but with x instead of y and with b instead of c. The similar argument leads to the conclusion that unless some equality of the form $\rho^{u'z+v'y} = \mu_i^{u'} \mu_j''^{v'}$ holds with some integers u', v' of absolute values at most T' and not both zero, then $b \le \exp(O(z/T' + T'))$. Here, $\mu_1'', \ldots, \mu_{\ell''}''$ are the roots of the polynomial $R(X)$ such that $u_x - 1$ is associated to $\gamma R(\rho^x)$ in the same way as $u_z - 1$ and $u_y - 1$ were associated to $\gamma P(\rho^z)$ and $\gamma Q(\rho^y)$, respectively. Since $b \gg \alpha^{(1-\kappa_0)z}$ for some constant $\kappa_0 \in (0, 1)$, we get again that $z \ll z/T' + T'$, which is a contradiction if T' is first chosen to be sufficiently large, and then z is allowed to be large. In conclusion, there must exist a relation of the form $\rho^{u'z+v'x} = \mu_i^{u'} \mu_j''^{v'}$, with exponents $u',\ v'$ of sizes $O(1)$, which are not both zero, leading again to the fact that $u'z + v'x = O(1)$. Since we also have $uz + vy = O(1)$, we get that (x, y, z) belongs to one of finitely many effectively computable lines in $\mathbb{Z}^3$. □

Since we have infinitely many solutions (x, y, z) and only finitely many possibilities for the lines in $\mathbb{Z}^3$ on which they might lie, it follows that infinitely many of the x, y and z are of the form

$$x = d_1 t + e_1, \qquad y = d_2 t + e_2, \qquad z = d_3 t + e_3,$$

where $d_1, d_2, d_3, e_1, e_2, e_3$ are fixed integers with the first three positive and t is a positive integer which may be arbitrarily large. Note that $d_3 \ge d_2 \ge d_1 > 0$. We may also fix the parity of t, therefore the signs of $\beta^x,\ \beta^y,\ \beta^z$ are all determined by η and the parities of $e_1,\ e_2$ and e_3. We now distinguish the following cases.

6.1 The case $j > 0$

This is the easiest case. We have

$$\begin{aligned} ab &= u_x - 1 = (\gamma\alpha^{ie_1})(\rho^t)^{id_1} + \zeta_1(\delta\rho^{je_1})(\rho^t)^{jd_1} - 1, \\ ac &= u_y - 1 = (\gamma\alpha^{ie_2})(\rho^t)^{id_2} + \zeta_2(\delta\rho^{je_2})(\rho^t)^{jd_2} - 1, \\ bc &= u_z - 1 = (\gamma\alpha^{ie_3})(\rho^t)^{id_3} + \zeta_3(\delta\rho^{je_3})(\rho^t)^{jd_3} - 1, \end{aligned}$$

where $\zeta_i = \eta^{e_i} \in \{\pm 1\}$ for $i = 1, 2, 3$. Multiplying the three relations above we get a polynomial with rational coefficients in ρ^t which is a perfect square for infinitely many values of t. Since 0 is not a root of this polynomial (in fact, its constant term is -1), it follows easily that this polynomial must be the perfect square of a polynomial with rational coefficients (see, for example, [15, Criterion 1]). However, this is impossible because its constant term is -1, which is not a perfect square.

6.2 The case $j = 0$

In this case, $i = 1$ and we have

$$\begin{aligned} ab &= u_x - 1 = \gamma_1(\rho^t)^{d_1} + \delta_1, \\ ac &= u_y - 1 = \gamma_2(\rho^t)^{d_2} + \delta_2, \\ bc &= u_z - 1 = \gamma_3(\rho^t)^{d_3} + \delta_3, \end{aligned}$$

where $\delta_1, \delta_2, \delta_3 \in \{-\delta - 1, \delta - 1\}$ are nonzero and $\gamma_i = \gamma\rho^{e_i}$ for $i = 1, 2, 3$. Let us put $P_i(X) = \gamma_i X^{d_i} + \delta_i$. Then

$$a \mid \gcd(P_1(\rho^t), P_2(\rho^t)),\ b \mid \gcd(P_1(\rho^t), P_3(\rho^t)),\ c \mid \gcd(P_2(\rho^t), P_3(\rho^t)).$$

We now look at $\gcd(P_i(X), P_j(X))$ for $i \neq j$. The roots of $P_i(X)$ in $\mathbb{C}$ are $e^{2\pi i\mu/d_i}\eta_i$, for $\mu = 0, 1, \ldots, d_i - 1$, where η_i is any fixed determination of $(-\delta_i/\gamma_i)^{1/d_i}$. It now follows easily that $\gcd(P_i(X), P_j(X))$ is a polynomial of degree at most $\gcd(d_i, d_j)$. In particular, $\gcd(P_3(X), P_1(X))\cdot \gcd(P_3(X), P_2(X))$ is a polynomial of degree at most $\gcd(d_3, d_3) + \gcd(d_3, d_2)$. Since

$$P_3(\rho^t) = bc \mid \gcd(P_1(\rho^t), P_3(\rho^t))\gcd(P_2(\rho^t), P_3(\rho^t))$$

holds for infinitely many positive integers t, we get that $d_3 \leq \gcd(d_3, d_1) + \gcd(d_3, d_2)$. Since $d_1 \leq d_2 \leq d_3$, the above inequality shows that either $d_3 = d_2$, or $d_1 = d_2 = d_3/2$. We treat only the case $d_1 = d_2$, since the case when $d_2 = d_3$ is similar. Since $d_1 = d_2$ and $y > x$, we get that $e_2 > e_1$. Putting $d = d_1$, we get that $P_1(X)$ is associated to $X^d + \delta_1/\gamma_1$ and $P_2(X)$ is associated to $X^d + \delta_2/\gamma_2$. They have a common root if and only if $\delta_1/\gamma_1 = \delta_2/\gamma_2$. This leads to $\rho^{e_2 - e_1} = \delta_2/\delta_1$. If $\delta_2 = \delta_1$, then $e_2 = e_1$, therefore $x = y$, which is a contradiction. This shows that $\delta_2 \neq \delta_1$, therefore δ_2/δ_1 equals either

$(\delta-1)/(-\delta-1)$, or $(-\delta-1)/(\delta-1)$. Changing δ to $-\delta$, if necessary, we may assume that

$$\rho^{e_2-e_1}=-\frac{\delta-1}{\delta+1}.$$

Since ρ is an integer, we get that $1+\delta \mid \delta-1$, therefore $1+\delta \mid 2$. Thus, $1+\delta=-2,-1,1,2$. The cases $1+\delta=-2,\ -1,\ 2$ give $\rho^{e_2-e_1}=-2,\ -3,\ 0$, respectively, which are impossible because ρ is positive, while the case $1+\delta=1$ gives $\delta=0$, which is not allowed. This completes the analysis of the case when $j=0$.

6.3 The case $j=-1$

This is by far the most technical one. In this case, we have that

$$\begin{aligned} u_x-1 &= \gamma\rho^{x+e_1}((\rho^t)^{2d_1}-\gamma_1(\rho^t)^{d_1}+\delta_1),\\ u_y-1 &= \gamma\rho^{y+e_2}((\rho^t)^{2d_2}-\gamma_2(\rho^t)^{d_2}+\delta_2),\\ u_z-1 &= \gamma\rho^{z+e_3}((\rho^t)^{2d_3}-\gamma_3(\rho^t)^{d_3}+\delta_3), \end{aligned}$$

where $\gamma_i=\gamma^{-1}\rho^{-e_i}$, $\delta_i=\eta_i\delta\gamma^{-1}\rho^{-2e_i}$ and $\eta_i=\eta^{e_i}\in\{\pm 1\}$ for $i=1,2,3$. We put

$$P_i(X)=X^{2d_i}-\gamma_i X^{d_i}+\delta_i=Q_i(X^{d_i})\qquad \text{for all } i=1,2,3,$$

where $Q_i(X)=X^2-\gamma_i X+\delta_i$ for $i=1,2,3$. Note that $P(\rho^t)=\prod_{i=1}^3 P_i(\rho^t)$ is associated to a perfect square in $\mathbb{K}$ for infinitely many t. Since $P(X)=\prod_{i=1}^t P_i(X)$ does not have zero as a root, it follows, again by [15, Criterion 1], that $P(X)$ is a square of a polynomial in $\mathbb{K}[X]$. In particular, all roots of $P(X)$ have even multiplicities.

We now fix $i\in\{1,2,3\}$ and take a closer look at $P_i(X)$. Let $z_{i,1}$ and $z_{i,2}$ be the roots of $Q_i(X)$. Since $P_i(X)=Q_i(X^{d_i})$, it follows that all roots of $P_i(X)$ are $e^{2\pi i\ell/d_i}z_{i,j}^{1/d_i}$ for $\ell=0,1,\ldots,d_i-1$ and $j=1,2$, where $z_{i,1}^{1/d_i}$ and $z_{i,2}^{1/d_i}$ are two fixed determinations of these complex nonzero numbers. Thus, if $P_i(X)$ has a double root, then it must be the case that $e^{2\pi i\ell/d_i}z_{i,1}^{1/d_i}=e^{2\pi i\ell'/d_i}z_{i,2}^{1/d_i}$ for some $\ell,\ell'\in\{0,1,\ldots,d_i-1\}$. Upon exponentiating this last relation to the power d_i, we get $z_{i,1}=z_{i,2}$. Thus, $Q_i(X)$ has a double root. This happens if and only if $\gamma_i^2-4\delta_i=0$, which leads to $\eta^{e_i}\gamma\delta=1/4$. Furthermore, if this is the case, then $z_{i,1}=z_{i,2}=\gamma_i/2$ is an algebraic integer and $P_i(X)=(X^{d_i}-\gamma_i/2)^2$ is the square of a polynomial whose coefficients are algebraic integers in $\mathbb{K}$.

6.3.1 The case of double roots

Assume that $P_i(X)$ has a double root for some $i\in\{1,2,3\}$. Then writing $\{1,2,3\}=\{i,j,k\}$, we get, from the fact that $P(X)$ and $P_i(X)$ are both squares of other polynomials with coefficients in $\mathbb{K}$, that $P_j(X)P_\ell(X)$ is a square of a polynomial with coefficients in $\mathbb{K}$. If $P_j(X)$ has a double root, then again $z_{j,1}=z_{j,2}=\gamma_j/2$ and

$P_j(X) = (X^{d_j} - \gamma_j/2)^2$. This leads to the fact that $P_\ell(X)$ is also the square of a polynomial with coefficients in $\mathbb{K}$, therefore $P_\ell(X) = (X^{d_\ell} - \gamma_\ell/2)^2$.

Put $R(X) = \prod_{i=1}^{3}(X^{d_i} - \gamma_i/2)$. Thus, $R(X)$ is monic and $P(X) = R^2(X)$. For a fixed t even, we have that abc is associated in $\mathbb{K}$ to $\gamma^{1/2}R(\rho^t)$, where $\gamma' = \gamma^{1/2}$. Indeed, note that $abc = \gamma^3\rho^{x+y+z+e_1+e_2+e_3} \cdot R^2(\rho^t)$, and

$$x + y + z + e_1 + e_2 + e_3 = t(d_1 + d_2 + d_3) + 2(e_1 + e_2 + e_3)$$

is even, therefore γ' must be a member of $\mathbb{K}$. Since bc is associated to $\gamma^2 P_3(\rho^t) = \gamma^2((\rho^t)^{d_3} - \gamma_3/2)^2$, we have that a is associated to $H(\rho^t)$, where

$$H(X) = \gamma'\gamma^{-2}\frac{(X^{d_1} - \gamma_1/2)(X^{d_2} - \gamma_2/2)}{(X^{d_3} - \gamma_3/2)}.$$

We now show that $H(X)$ is a polynomial. Assume that this is not so and let $H(X) = F(X)/G(X)$, where $G(X)$ is of positive degree and $F(X)$ and $G(X)$ are coprime. Then the algebraic integer $G(\rho^t)$ in $\mathbb{K}$ divides the resultant $\mathrm{Res}_X(F(X), G(X))$ evaluated at $X = \rho^t$, which is a nonzero algebraic integer in $\mathbb{K}$. Thus, $G(\rho^t)$ is associated to some element from a finite list in $\mathbb{K}$. However, since $G(X)$ is of positive degree and does not have zero as a root, this resulting Diophantine equation has only finitely many positive integer solutions t. In fact, by the classical theory of Diophantine equations (see [19], for example), this Diophantine equation can be immediately reduced to a unit equation in three terms in $\mathbb{K}[(\gamma_3/2)^{1/d_3}]$. This contradiction shows that $H(X)$ is a polynomial, therefore that $X^{d_3} - \gamma_3/2$ divides $(X^{d_1} - \gamma_1/2)(X^{d_2} - \gamma_2/2)$. The polynomials $X^{d_3} - \gamma_3/2$ and $X^{d_i} - \gamma_i/2$ can have at most $\gcd(d_3, d_i)$ roots in common for $i = 1, 2$. Thus, $d_3 \le \gcd(d_3, d_1) + \gcd(d_3, d_1)$. Since $d_3 \ge d_2 \ge d_1$, it follows that either $d_3 = d_2$, or $d_1 = d_2 = d_3/2$. If $d_3 = d_2$, then by putting $d = d_3$ and using the fact that $X^d - \gamma_3/2$ and $X^d - \gamma_2/2$ have a root in common, we also get $\gamma_3 = \gamma_2$, therefore $\rho^{e_2} = \rho^{e_3}$. Thus, $z = y$ which is not allowed. Finally, if $d_1 = d_2$, then using the fact that also $X^{d_1} - \gamma_1/2$ and $X^{d_2} - \gamma_2/2$ have a root in common (because a becomes arbitrarily large), we get that $\gamma_1 = \gamma_2$, therefore $e_1 = e_2$, leading to $x = y$, which is again not allowed.

We now return to the situation where $P_i(X) = (X^{d_i} - \gamma_i/2)^2$ but $P_j(X)$ does not have a double root. Then $P_\ell(X)$ does not have a double root either, and since $P_j(X)P_\ell(X)$ is a square, we get that $P_j(X) = P_\ell(X)$. By identifying degrees and coefficients, we get $d_j = d_\ell$ and $\gamma_j = \gamma_\ell$. The last equation implies that $\rho^{e_j} = \rho^{e_\ell}$; hence, $e_j = e_j$. Since $(d_j, e_j) = (d_\ell, e_\ell)$, we get again that the two of the three variables $\{x, y, z\}$ corresponding to j and ℓ are equal, which is impossible.

6.3.2 Bounding the number of common roots

From now on, we can assume that all three polynomials $P_1(X), P_2(X)$ and $P_3(X)$ have only simple roots. We look at

$$P_3(X) = (X^{d_3} - z_{3,1})(X^{d_3} - z_{3,2}),$$

and count the number of common roots that $P_3(X)$ can have with $P_i(X)$ for some $i = 1, 2$. Let

$$P_i(X) = (X^{d_i} - z_{i,1})(X^{d_i} - z_{i,2}).$$

Note that both $P_3(X)$ and $P_i(X)$ are product of two binomial polynomials. Our aim is to show that $P_3(X)$ has $\leq 2\gcd(d_3, d_1)$ roots in common with each of $P_i(X)$ for $i = 1, 2$.

Assume say that $z_{3,1}/z_{3,2}$ is not a root of 1. Suppose that $z_{i,1}/z_{i,2}$ is not a root of 1 either. Then, since all roots of $X^{d_3} - z_{3,1}$ differ one from another multiplicatively by roots of unity, it follows that if $X^{d_3} - z_{3,1}$ has a root in common with $X^{d_i} - z_{i,j}$, then it will not have a root in common with $X^{d_i} - z_{i,\ell}$, where $\{j, \ell\} = \{1, 2\}$. Thus, in this case there exists at most one $j \in \{1, 2\}$ such that $X^{d_3} - z_{3,1}$ has a common root with $X^{d_i} - z_{i,j}$, and clearly the number of such roots is $\leq \gcd(d_3, d_i)$. Hence, $X^{d_3} - z_{3,1}$ has at most $\gcd(d_3, d_i)$ common roots with $P_i(X)$. The same is true for $X^{d_3} - z_{3,2}$. Hence, in this case the number of common roots of $P_3(X)$ and $P_i(X)$ is $\leq 2\gcd(d_3, d_i)$.

Assume now that still $z_{3,1}/z_{3,2}$ is not a root of 1, but that $z_{i,1}/z_{i,2}$ is a root of 1. If each of $X^{d_3} - z_{3,i}$ for $i = 1, 2$ has common roots with at most one of the two binomials $X^{d_i} - z_{i,j}$ for $j = 1, 2$, then the above argument shows again that the number of common roots of $P_3(X)$ and $P_i(X)$ is at most $2\gcd(d_3, d_i)$. If say $X^{d_3} - z_{3,1}$ has common roots with both $X^{d_i} - z_{i,1}$ and $X^{d_i} - z_{i,2}$, then it has at most $\gcd(d_3, d_i)$ common roots with each one of them, while $X^{d_3} - z_{3,2}$ does not have common roots neither with $X^{d_i} - z_{i,1}$, nor with $X^{d_i} - d_{i,2}$, since otherwise $z_{3,1}/z_{3,2}$ will end up being a root of 1, which is not the case. Hence, again $P_3(X)$ and $P_i(X)$ have at most $2\gcd(d_3, d_i)$ roots in common.

Assume next that $z_{3,1}/z_{3,2}$ is a root of 1, but that $z_{i,1}/z_{i,2}$ is not. If both $X^{d_3} - z_{3,1}$ and $X^{d_3} - z_{3,2}$ have common roots with $P_i(X)$, then these common roots will be roots of $X^{d_i} - z_{i,j}$ for the same value of j. Thus, each of $X^{d_3} - z_{3,1}$ and $X^{d_3} - z_{3,2}$ will have at most $\gcd(d_3, d_i)$ common roots with $X^{d_i} - z_{i,j}$ (and none common with $X^{d_i} - z_{i,\ell}$, where ℓ is such that $\{j, \ell\} = \{1, 2\}$), so again $P_3(X)$ and $P_i(X)$ have at most $2\gcd(d_3, d_i)$ roots in common. Of course, if only one of $X^{d_3} - z_{3,j}$ for $j = 1, 2$ has common roots with $P_i(X)$, then again it will have common roots with only one of $X^{d_i} - z_{i,\ell}$ for $\ell = 1, 2$, and the number of such is $\leq \gcd(d_3, d_i)$, so in this case $P_3(X)$ and $P_i(X)$ have at most $\gcd(d_3, d_i) < 2\gcd(d_3, d_i)$ common roots.

So far, we have always obtained that $P_3(X)$ and $P_i(X)$ have at most $2\gcd(d_i, d_3)$ roots in common.

Assume now finally that both $z_{3,1}/z_{3,2}$ and $z_{i,1}/z_{i,2}$ are roots of 1.

Note that $(z_{i,1}\gamma\rho^{e_i}, z_{i,2}\gamma\rho^{e_i})$ are the roots of $X^2 - X + \eta^{e_i}\gamma\delta$, and $\gamma\delta \in \mathbb{Q}^*$ because γ and δ are conjugates in $\mathbb{K}$. Thus, while $z_{i,1},\ z_{i,2}$ might belong to a quadratic field over $\mathbb{K}$ (hence, a field of degree 4 over $\mathbb{Q}$), their ratio belongs to a quadratic field. Thus, if $z_{i,1}/z_{i,2} \neq 1$ is a root of 1, then its order is one of $2, 3, 4$, or 6. Note next that the order cannot be 2 (i.e., $z_{i,1} = -z_{i,2}$), because the coefficient of X in the quadratic polynomial $X^2 - X + \eta^{e_i}\gamma\delta$ is not zero. Hence, $z_{i,1}/z_{i,2}$ is a root of unity of order $3, 4$, or 6. One checks easily that $z_{i,1}/z_{i,2}$ is a root of 1 of orders $3, 4, 6$, respectively, if and

only if $\eta^{e_i}\gamma\delta = 1,\ 1/2$, or $1/3$, respectively. Since we are discussing the case when both $z_{3,1}/z_{3,2}$ and $z_{i,1}/z_{i,2}$ are roots on unity, we deduct that either $\eta = 1$, or $\eta = -1$ and $e_i \equiv e_3 \pmod 2$, and in any case these two roots of unity have the same order. Let this order be $k \in \{3, 4, 6\}$, and put $\varepsilon = e^{2\pi i/k}$.

If each of $X^{d_3} - z_{3,1}$ and $X^{d_3} - z_{3,2}$ has common roots with at most one of two polynomials $X^{d_i} - z_{i,1}$ and $X^{d_i} - z_{i,2}$, then the previous argument shows that $P_3(X)$ and $P_i(X)$ have at most $2\gcd(d_3, d_i)$ roots in common. Further, if at most one of the two polynomials $X^{d_3} - z_{3,1}$ and $X^{d_3} - z_{3,2}$ has common roots with $P_i(X)$, then again the previous argument shows that the number of common roots of $P_3(X)$ and $P_i(X)$ is at most $2\gcd(d_3, d_i)$.

We now look at the remaining cases. Here, we shall show that the number of common roots of $P_3(X)$ and $P_i(X)$ is $< d_3$.

We start by noting that up to relabeling the roots of $P_i(X)$, we may assume that $z_{i,1} = z_i$, that $z_{i,2} = z_i\varepsilon$, and that $X^{d_3} - z_{3,1}$ has a root η in common with $X^{d_i} - z_i$, and another root η' in common with $X^{d_i} - z_i\varepsilon$. Certainly, $z_{3,2} = z_{3,1}\varepsilon^{\pm 1}$, and $X^{d_3} - z_{3,2}$ has a root in common with at least one of $X^{d_i} - z_i$ or $X^{d_i} - z_i\varepsilon$.

Since $X^{d_3} - z_{3,1}$ has a root in common with $X^{d_i} - z_i$, we get that there is a number ν such that $\nu^{d_3} = z_{3,1}$ and $\nu^{d_i} = z_i$. Thus,

$$P_i(X) = (X^{d_i} - \nu^{d_i})(X^{d_i} - \nu^{d_i}\varepsilon).$$

Since $X^{d_3} - \nu^{d_3}$ has also a root in common with $X^{d_i} - \nu^{d_i}\varepsilon$, it follows that for some integers j and ℓ we have

$$\nu e^{2\pi ij/d_3} = \nu e^{2\pi i/(kd_i) + 2\pi i\ell/d_i}.$$

Thus,

$$\frac{1}{kd_i} \in \frac{\ell}{d_i} - \frac{j}{d_3} + \mathbb{Z},$$

implying that $\mathrm{lcm}[d_3, d_i]$ is a multiple of kd_i. Thus, $kd_i \le \mathrm{lcm}[d_3, d_i] = d_3d_i/\gcd(d_3, d_i)$, giving $\gcd(d_3, d_i) \le d_3/k$.

Suppose first that $X^{d_3} - z_{3,2}$ does not have a common root with both of $X^{d_i} - z_i$ and $X^{d_i} - z_i\varepsilon$. Then $P_3(X)$ and $P_i(X)$ have at most $3\gcd(d_3, d_i) \le 3d_3/k$ roots in common. Note that $3d_3/k \le d_3$. Thus, $P_3(X)$ and $P_i(X)$ have at most d_3 roots in common. Let us show that in fact the inequality is strict. From the above arguments, the inequality is strict unless $k = 3$ and $\gcd(d_3, d_i) = d_3/3$. Put $\gcd(d_3, d_i) = \lambda$. Then $d_3 = 3\lambda$ and $d_i \in \{\lambda, 2\lambda\}$. If $d_i = \lambda$, then $P_i(X)$ has a totality of $2\lambda < d_3$ roots, and we obtain a contradiction. Thus, $d_i = 2\lambda$. Hence,

$$P_3(X) = (X^{3\lambda} - \nu^{3\lambda})(X^{3\lambda} - \nu^{3\lambda}\varepsilon^{\pm 1}), \quad P_i(X) = (X^{2\lambda} - \nu^{2\lambda})(X^{2\lambda} - \nu^{2\lambda}\varepsilon).$$

However, it is now easy to see that $X^{3\lambda} - \nu^{3\lambda}\varepsilon^{\pm 1}$ cannot have a common root with $P_i(X)$. Indeed, any such common root x will satisfy $x^{3\lambda} = \nu^{3\lambda}\varepsilon^{\pm 1}$ and either $x^{2\lambda} = \nu^{2\lambda}$

(leading to $\nu^{6\lambda}\varepsilon^{\pm 2} = x^{6\lambda} = \nu^{6\lambda}$, which is false since $\varepsilon^{\pm 2} \neq 1$), or $x^{2\lambda} = \nu^{2\lambda}\varepsilon$ (leading to $\nu^{6\lambda}\varepsilon^{\pm 2} = x^{6\lambda} = \nu^{6\lambda}\varepsilon^3$, which is again false since $\varepsilon^3 = 1$ and $\varepsilon^{\pm 2} \neq 1$).

So, it remains to treat the case when also $X^{d_3} - z_{1,3}\varepsilon^{\pm 1}$ has a root in common with both $X^{d_i} - z_i$ and $X^{d_i} - z_i\varepsilon$. With the previous notations, since $X^{d_3} - \nu^{d_3}\varepsilon^{\pm 1}$ and $X^{d_i} - \nu^{d_i}$ have a root in common, we get that for some integers j and ℓ we have $\nu e^{\pm 2\pi i/(kd_3) + 2\pi ij/d_3} = \nu e^{2\pi i\ell/d_i}$. This leads to

$$\pm\frac{1}{kd_3} \in \frac{\ell}{d_i} - \frac{j}{d_3} + \mathbb{Z},$$

so $\mathrm{lcm}[d_3, d_i]$ is a multiple of kd_3. Thus, $kd_3 \leq \mathrm{lcm}[d_3, d_i]$, leading to $\gcd(d_3, d_i) \leq d_i/k$. In particular, $d_i \neq d_3$. Write $\lambda = \gcd(d_3, d_i)$. Then $d_i \geq k\lambda$, therefore $d_3 \geq (k+1)\lambda$. Thus, $\lambda \leq d_3/(k+1)$. Since $P_3(X)$ and $P_i(X)$ have at most 4λ roots in common anyway, we get that the number of common roots of these two polynomials is $\leq 4d_3/(k+1) \leq d_3$. Equality is obtained if and only if $k = 3$ and $d_3 = 4\lambda$. Clearly, d_i cannot be λ (otherwise $P_i(X)$ and $P_3(X)$ will have at most $2d_i \leq 2\lambda < d_3$ roots in common), and $d_i \neq 2\lambda$, for otherwise $\lambda = \gcd(d_3, d_i) = 2\lambda$, which is a contradiction. So, it must be the case that $d_i = 3\lambda$. Hence,

$$P_3(X) = (X^{4\lambda} - \nu^{4\lambda})(X^{4\lambda} - \nu^{4\lambda}\varepsilon^{\pm 1}), \quad P_i(X) = (X^{3\lambda} - \nu^{3\lambda})(X^{3\lambda} - \nu^{3\lambda}\varepsilon).$$

Note now that the second factor of $P_i(X)$ above cannot have a common root x with the first factor of $P_3(X)$ above, for if not, we would have $\nu^{12\lambda} = x^{12\lambda} = \nu^{12\lambda}\varepsilon^4$, therefore $\varepsilon^4 = 1$, which is false.

Having covered all the possibilities, we get that $P_3(X)$ has $< d_3$ common roots with $P_i(X)$. If this is true for both $i, j \in \{1, 2\}$, it follows that there is a root of $P_3(X)$ which is not a root of $P_1(X)P_2(X)$, and this is a contradiction because $P_1(X)P_2(X)P_3(X)$ has the property that all its roots are double.

So, there could be at most one $i \in \{1, 2\}$ such that $P_3(X)$ has common $< d_3$ common roots with $P_i(X)$, and for $j \notin \{i, 3\}$, $P_3(X)$ and $P_j(X)$ have at most $2\gcd(d_3, d_j)$ roots in common. If $\gcd(d_3, d_j) \neq d_3$, it follows that $\gcd(d_3, d_j) \leq d_3/2$, so $P_3(X)$ has $< 2d_3$ roots in common with $P_1(X)P_2(X)$, which is false. So, it must be the case that $\gcd(d_3, d_j) = d_3$, so $d_j = d_3$. Write $d = d_3$. Thus,

$$P_3(X) = (X^d - z_{3,1})(X^d - z_{3,2}), \qquad P_j(X) = (X^d - z_{j,1})(X^d - z_{j,2}).$$

But it is clear that if the above polynomials have more than d roots in common, then they will have all roots in common so they will coincide. In particular, $d_3 = d_j$ and $\gamma_3 = \gamma_j$, leading to $e_3 = e_j$, so we get again the contradiction that two of the positive integer unknowns x, y and z are equal. Hence, $P_3(X)$ and $P_j(X)$ have at most d_3 roots in common, therefore $P_3(X)$ and $P_1(X)P_2(X)$ have less than $2d_3$ roots in common, which is false.

In conclusion, it must be the case that $P_3(X)$ has $\leq 2\gcd(d_3, d_i)$ roots in common with each of $P_i(X)$ for $i = 1, 2$. Thus, $2d_3 \leq 2\gcd(d_3, d_1) + 2\gcd(d_3, d_2)$, therefore

either $d_2 = d_3$, or $d_1 = d_2 = d_3/2$. Assume that $d_1 = d_2 = d_3/2$. Then $P_3(X)$ has at most d_3 roots in common with each of $P_1(X)$ and $P_2(X)$. Since all its roots are common to either $P_1(X)$ or $P_2(X)$, we get that $P_3(X)$ and $P_1(X)P_2(X)$ are monic and have the same roots which are all simple for each of these two polynomials. Hence, $P_3(X) = P_1(X)P_2(X)$. Evaluating this in $X = \rho^t$ with large t, we get that $a = O(1)$, which is a contradiction.

6.3.3 The case $d_1 < d_2 = d_3$

Let $d = d_2 = d_3$. Then the two polynomials

$$P_3(X) = (X^d - z_{3,1})(X^d - z_{3,2}), \qquad P_2(X) = (X^d - z_{2,1})(X^d - z_{2,3})$$

cannot have more than d root in common, for otherwise, by an argument already used before, we would get that they coincide, therefore $z = y$, which is a contradiction. Thus, $P_3(X)$ and $P_2(X)$ have exactly d roots in common, therefore $P_3(X)$ and $P_1(X)$ also have d roots in common. Since the number of such roots is $\leq 2\gcd(d_3, d_1)$, we get that either $d_1 = d$, or $d_1 = d/2$. Assume that $d_1 = d/2$. Then $P_1(X)$ divides $P_3(X)$. Furthermore, up to relabeling the roots of $Q_2(X)$, it follows that we may assume that $\gcd(P_3(X), P_2(X)) = X^d - z_{2,1}$. Then $P_1(X)P_2(X)P_3(X) = P_1(X)^2(X^d - z_{2,1})^2(X^d - z_{2,2})$, and since this must be the square of a polynomial with coefficients in $\mathbb{K}$, we get that $X^d - z_{2,2}$ is a square of a polynomial with coefficients in $\mathbb{K}$, and this is false again.

6.3.4 The case $d = d_1 = d_2 = d_3$

It now follows immediately that $Q_1(X)Q_2(X)Q_3(X)$ must be a perfect square of a polynomial of degree 3 with coefficients in $\mathbb{K}[X]$. Furthermore, $Q_i(X)$ and $Q_j(X)$ have precisely one root in common for all $i \neq j \in \{1, 2, 3\}$. We now analyze this last situation.

Assume first that either $\eta = 1$, or $\eta = -1$ but that $e_1,\ e_2,\ e_3$ are all congruent modulo 2. Let us write u and v for the roots of $X^2 - X + \eta^e\gamma\delta$, where the value of e modulo 2 is congruent to e_i $(i = 1, 2, 3)$ in case $\eta = -1$. It then follows that $Q_i(X)$ has roots $u\gamma^{-1}\rho^{-e_i}$ and $v\gamma^{-1}\rho^{-e_i}$. Note that since $Q_i(X) \in \mathbb{K}[X]$ for all $i \in \{1, 2, 3\}$, and any two of them have precisely one root in common, it follows that $u,\ v \in \mathbb{K}$. Furthermore, since $u/v \neq \pm 1$, and $\mathbb{K}$ is real, it follows, up to interchanging u and v, that we may assume $|u| > |v|$. Since the root $u\gamma^{-1}\rho^{-e_i}$ is also a root of $Q_j(X)$ for some $j \in \{1, 2, 3\}\backslash\{i\}$, we get that either $u\gamma^{-1}\rho^{-e_i} = u\gamma^{-1}\rho^{-e_j}$, leading to $e_i = e_j$, therefore two of the positive integer unknowns $x,\ y$ and z are equal, which is impossible, or for each i there is $j \neq i$ such that $u\gamma^{-1}\rho^{-e_i} = v\gamma^{-1}\rho^{-e_j}$. Thus, $u/v = \rho^{e_i - e_j}$, and since $|u| > |v|$ and $\rho > 1$, we get that $e_i > e_j$. Thus, for each $i \in \{1, 2, 3\}$, there is $j \neq i$ in the same set such that $e_i > e_j$. This is of course impossible because there must be some index i such that $e_i = \min\{e_j : j \in \{1, 2, 3\}\}$.

Finally, we assume that $\eta = -1$ and that not all e_i are congruent modulo 2 for $i = 1, 2, 3$. Thus, there are two of them, say i and j such that $e_i \equiv e_j \pmod 2$, and the third one ℓ is such that $e_\ell \not\equiv e_i \pmod 2$. Let $e \equiv e_i \pmod 2$, and we assume that u and v are the roots of $X^2 - X + (-1)^e \gamma\delta$, and that u_1 and v_1 are the roots of $X^2 - X - (-1)^e \gamma\delta$. An argument used previously shows that u, v, u_1, v_1 are all in $\mathbb{K}$. In particular, they are real. Then the pairs of roots of $Q_i(X)$, $Q_j(X)$ and $Q_\ell(X)$ are $(u\gamma^{-1}\rho^{-e_i}, v\gamma^{-1}\rho^{-e_i})$, $(u\gamma^{-1}\rho^{-e_j}, v\gamma^{-1}\rho^{-e_j})$, and $(u_1\gamma^{-1}\rho^{-e_\ell}, v_1\gamma^{-1}\rho^{-e_\ell})$, respectively. Up to interchanging u and v, we may assume that $u\gamma^{-1}\rho^{-e_i}$ is also a root of $Q_j(X)$. If $u\gamma^{-1}\rho^{-e_i} = u\gamma^{-1}\rho^{-e_j}$, we then get again $e_i = e_j$, which leads again to the conclusion that two of the three positive integer unknowns x, y and z coincide, which is false. Thus, $u\gamma^{-1}\rho^{-e_i} = v\gamma^{-1}\rho^{-e_j}$, so $u/v = \rho^{e_i - e_j}$. In particular, $(-1)^e\delta\gamma = uv = v^2(u/v) = v^2\rho^{e_i - e_j}$ is a positive number. Now each of the roots of $Q_\ell(X)$ is also a root of $Q_i(X)$ or $Q_j(X)$. In particular, $u_1\gamma^{-1}\rho^{-e_\ell} = w_1\gamma^{-1}\rho^{-e_m}$ and $v_1\gamma^{-1}\rho^{-e_\ell} = w_2\gamma^{-1}\rho^{-e_n}$, where w_1, $w_2 \in \{u, v\}$, and m, $n \in \{i, j\}$. Hence, $(-1)^{e+1}\delta\gamma = u_1v_1 = w_1w_2\rho^{2e_\ell - e_m - e_n}$, but this last number is positive since $\rho > 1$ and $w_1w_2 \in \{u^2, v^2, uv\}$. This contradicts the fact that $(-1)^e\gamma\delta > 0$, and completes the proof of Theorem 1.

References

[1] Y. Bugeaud – P. Corvaja – U. Zannier, *An upper bound for the G.C.D. of $a^n - 1$ and $b^n - 1$*, Math. Z. **243** (2003), 79–84.

[2] Y. Bugeaud – A. Dujella, *On a problem of Diophantus for higher powers*, Math. Proc. Cambridge Philos. Soc. **135** (2005), 1–10.

[3] Y. Bugeaud – F. Luca, *On the period of the continued fraction expansion of square root of $2^{2n+1} + 1$*, Indag. Math., NS **16** (2005), 21–35.

[4] P. Corvaja – U. Zannier, *Diophantine equations with power sums and Universal Hilbert Sets*, Indag. Math., NS **9** (1998), 317-332.

[5] P. Corvaja – U. Zannier, *A lower bound for the height of a rational function at S-unit points*, Monatsh. Math. **144** (2005), 203-224.

[6] P. Corvaja – U. Zannier, *S-unit points on analytic hypersurfaces*, Ann. Sci. École Norm. Sup. (4) **38** (2005), 76–92.

[7] A. Dujella, *There are only finitely many Diophantine quintuples*, J. reine angew. Math. **566** (2004), 183–214.

[8] A. Dujella, *Diophantine m-tuples*, webpage available under http://web.math.hr/∼duje/dtuples.html

[9] C. Fuchs, *An upper bound for the G.C.D. of two linear recurring sequences*, Math. Slovaca **53** (2003), 21–42.

[10] C. Fuchs, *Diophantine problems with linear recurrences via the Subspace Theorem*, Integers: Electronic Journal of Combinatorial Number Theory **5** (2005), #A08.

[11] C. Fuchs, *Polynomial-exponential equations involving multirecurrences*, Studia Sci. Math. Hungar., to appear.

[12] C. Fuchs – A. Scremin, *Polynomial-exponential equations involving several linear recurrences*, Publ. Math. Debrecen **65** (2004), 149–172.

[13] F. Luca, *On shifted products which are powers*, Glas. Mat. Ser. III **40** (2005), 13–20.

[14] F. Luca, *On the greatest common divisor of $u-1$ and $v-1$ with u and v near $\mathcal{S}$-units*, Monatsh. Math. **146** (2005), 239–256.

[15] F. Luca – T. N. Shorey, *Diophantine equations with products of consecutive terms in Lucas sequences, II*, Acta Arith., to appear.

[16] F. Luca – L. Szalay, *Fibonacci Diophantine triples*, Preprint, 2007.

[17] H. P. Schlickewei – W. M. Schmidt, *Linear equations in members of recurrence sequences*, Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) **20** (1993), 219–246.

[18] W. M. Schmidt, *Linear Recurrence Sequences and Polynomial-Exponential Equations*, In: "Diophantine Approximation, Proc. of the C.I.M.E. Conference, Cetraro (Italy) 2000", F. Amoroso – U. Zannier (eds.), Springer-Verlag, LN **1819**, 2003, pp. 171–247.

[19] T. N. Shorey – R. Tijdeman, "Exponential Diophantine Equations", Cambridge Univ. Press, Cambridge, 1986.

[20] J. Silverman, *Generalized greatest common divisors, divisibility sequences, and Vojta's conjecture for blowups*, Monats. Math. **145** (2005), 333–350.

[21] K. R. Yu, *p-adic logarithmic forms and group varieties, II*, Acta Arith. **89** (1999), 337–378.

[22] U. Zannier, "Some applications of Diophantine Approximation to Diophantine Equations (with special emphasis on the Schmidt Subspace Theorem)", Forum, Udine, 2003.

[23] U. Zannier, *Diophantine equations with linear recurrences. An overview of some recent progress*, J. Théor. Nombres Bordeaux **17** (2005), 423-435.

Clemens Fuchs
Department of Mathematics, ETH Zürich, Rämistrasse 101, 8092 Zürich, Switzerland
E-mail: clemens.fuchs@math.ethz.ch

Florian Luca
Instituto de Matemáticas, Universidad Nacional Autónoma de México, C.P. 58180, Morelia, Michoacán, México
E-mail: fluca@matmor.unam.mx

Laszlo Szalay
Department of Mathematics and Statistics, University of West Hungary, 9400, Sopron, Bajcsy-Zs. út 4, Hungary
E-mail: laszalay@ktk.nyme.hu

dc_871_14

dc_871_14

Florian Luca, László Szalay

Fibonacci diophantine triples

Glas. Mat., III. Ser., 43 (2008), 253-264.

dc_871_14

Fibonacci diophantine triples

Florian Luca, László Szalay

Abstract

In this paper, we show that there are no three distinct positive integers $a,\ b,\ c$ such that $ab+1,\ ac+1,\ bc+1$ are all three Fibonacci numbers.

1 Introduction

A *Diophantine m-tuple* is a set of $\{a_1, \ldots, a_m\}$ of positive rational numbers or integers such that $a_i a_j + 1$ is a square for all $1 \leq i < j \leq m$. Diophantus found the rational quadruple $\{1/16, 33/16, 17/4, 105/16\}$, while Fermat found the integer quadruple $\{1, 3, 8, 120\}$. Infinitely many Diophantine quadruples of integers are known and it is conjectured that there is no Diophantine quintuples. This was almost proved by Dujella [5], who showed that there can be at most finitely many Diophantine quintuples and all of them are, at least in theory, effectively computable. In the rational case, it is not known that the size m of the Diophantine m-tuples must be bounded and a few examples with $m = 6$ are known by the work of Gibbs [8]. We also note that some generalization of this problem for squares replaced by higher powers (of fixed, or variable exponents) were treated by many authors (see [1], [2], [9], [13] and [10]).

In the paper [7], the following variant of this problem was treated. Let r and s be nonzero integers such that $\Delta = r^2 + 4s \neq 0$. Let $(u_n)_{n\geq 0}$ be a binary recurrence sequence of integers satisfying the recurrence

$$u_{n+2} = ru_{n+1} + su_n \qquad \text{for all } n \geq 0.$$

It is well-known that if we write α and β for the two roots of the *characteristic equation* $x^2 - rx - s = 0$, then there exist constants $\gamma,\ \delta \in \mathbb{K} = \mathbb{Q}[\alpha]$ such that

$$u_n = \gamma\alpha^n + \delta\beta^n \qquad \text{holds for all } n \geq 0. \tag{1}$$

Assume further that the sequence $(u_n)_{n\geq 0}$ is *nondegenerate*, which means that $\gamma\delta \neq 0$ and α/β is not root of unity. We shall also make the convention that $|\alpha| \geq |\beta|$.

A Diophantine triple with values in the set $\mathcal{U} = \{u_n : n \geq 0\}$ is a set of three distinct positive integers $\{a, b, c\}$ such that $ab+1,\ ac+1,\ bc+1$ are all in $\mathcal{U}$. Note that if $u_n = 2^n + 1$ for all $n \geq 0$, then there are infinitely many such triples (namely, take $a,\ b,\ c$ to be any distinct powers of two). The main result in [7] shows that the above

example is representative for the sequences $(u_n)_{n\geq 0}$ with real roots for which there exist infinitely many Diophantine triples with values in $\mathcal{U}$. The precise result proved there is the following.

Theorem 1. *Assume that $(u_n)_{n\geq 0}$ is a nondegenerate binary recurrence sequence with $\Delta > 0$ such that there exist infinitely many sextuples of nonnegative integers*

$$(a, b, c; x, y, z)$$

with $1 \leq a < b < c$ such that

$$ab + 1 = u_x, \qquad ac + 1 = u_y, \qquad bc + 1 = u_z. \tag{2}$$

Then $\beta \in \{\pm 1\}$, $\delta \in \{\pm 1\}$, $\alpha,\ \gamma \in \mathbb{Z}$. Furthermore, for all but finitely many of the sextuples $(a, b, c; x, y, z)$ as above one has $\delta\beta^z = \delta\beta^y = 1$ and one of the following holds:

(i) $\delta\beta^x = 1$. In this case, one of δ or $\delta\alpha$ is a perfect square;

(ii) $\delta\beta^x = -1$. In this case, $x \in \{0, 1\}$.

No finiteness result was proved for the case when $\Delta < 0$. The case $\delta\beta^z = 1$ is not hard to handle. When $\delta\beta^z \neq 1$, results from Diophantine approximations relying on the Subspace Theorem, as well as on the finiteness of the number of solutions of nondegenerate unit equations with variables in a finitely generated multiplicative group and bounds for the greatest common divisor of values of rational functions at units points in the number fields setting, allow one to reduce the problem to elementary considerations concerning polynomials.

The Fibonacci sequence $(F_n)_{n\geq 0}$ is the binary recurrent sequence given by $(r, s) = (1, 1)$, $F_0 = 0$ and $F_1 = 1$. It has $\alpha = (1 + \sqrt{5})/2$ and $\beta = (1 - \sqrt{5})/2$. According to Theorem 1, there should be only finitely many triples of distinct positive integers $\{a, b, c\}$ such that $ab + 1,\ ac + 1,\ bc + 1$ are all three Fibonacci numbers. Our main result here is that in fact there are no such triples.

Theorem 2. *There do not exist positive integers $a < b < c$ such that*

$$ab + 1 = F_x, \qquad ac + 1 = F_y, \qquad bc + 1 = F_z, \tag{3}$$

where $x < y < z$ are positive integers.

Let us remark that since the values $n = 1,\ 2,\ 3$ and 5 are the only positive integers n such that $F_n = k^2 + 1$ holds with some suitable integer k (see [6]), it follows from Theorem 2 that all the solutions of equation (4) under the more relaxed condition $0 < a \leq b \leq c$ are

$$(a, b, c; x, y, z) = \begin{cases} (1, 1, F_t - 1; 3, t, t), & t \geq 3; \\ (2, 2, (F_t - 1)/2; 5, t, t), & t \geq 4,\ t \not\equiv 0 \pmod 3; \end{cases}$$

Note also that there are at least two *rational* solutions $0 < a < b < c$, namely

$$(a, b, c; x, y, z) = (2/3, 3, 18; 4, 7, 10)\,, \quad (9/2, 22/3, 12; 9, 10, 11)\,.$$

It would be interesting to decide whether equation (3) has only finitely many rational solutions $(a, b, c; x, y, z)$ with $0 < a < b < c$, and in the affirmative case whether the above two are the only ones.

2 Proof of Theorem 2

2.1 Preliminary results

In the sequel, we suppose that $1 \le a < b < c$ and $4 \le x < y < z$. We write $(L_n)_{n\ge 0}$ for the companion sequence of the Fibonacci numbers given by $L_0 = 2,\ L_1 = 1$ and $L_{n+2} = L_{n+1} + L_n$ for all $n \ge 0$. It is well-known (see, for example, Ron Knott's excellent web-site on Fibonacci numbers [11], or Koshy's monograph [12]), that the formulae

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \qquad \text{and} \qquad L_n = \alpha^n + \beta^n$$

hold for all $n \ge 0$, where $\alpha = (1 + \sqrt{5})/2$ and $\beta = (1 - \sqrt{5})/2$.

We shall need the following statements.

Lemma 3. *The following divisibilities hold:*

(i) $\gcd(F_u, F_v) = F_{\gcd(u,v)}$*;*

(ii) $$\gcd(L_u, L_v) = \begin{cases} L_{\gcd(u,v)}, & \text{if } \frac{u}{\gcd(u,v)} \equiv \frac{v}{\gcd(u,v)} \equiv 1 \pmod 2; \\ 1 \text{ or } 2, & \text{otherwise;} \end{cases}$$

(iii) $$\gcd(F_u, L_v) = \begin{cases} L_{\gcd(u,v)}, & \text{if } \frac{u}{\gcd(u,v)} \not\equiv \frac{v}{\gcd(u,v)} \equiv 1 \pmod 2; \\ 1 \text{ or } 2, & \text{otherwise.} \end{cases}$$

Proof. This is well-known (see, for instance, the proof of Theorem VII. in [3]). □

Lemma 4. *The following formulae hold:*

$$F_u - 1 = \begin{cases} F_{\frac{u-1}{2}}\, L_{\frac{u+1}{2}}, & \text{if } u \equiv 1 \pmod 4; \\ F_{\frac{u+1}{2}}\, L_{\frac{u-1}{2}}, & \text{if } u \equiv 3 \pmod 4; \\ F_{\frac{u-2}{2}}\, L_{\frac{u+2}{2}}, & \text{if } u \equiv 2 \pmod 4; \\ F_{\frac{u+2}{2}}\, L_{\frac{u-2}{2}}, & \text{if } u \equiv 0 \pmod 4. \end{cases}$$

Proof. This too is well-known (see, for example, Lemma 2 in [14]). □

Lemma 5. *Let u_0 be a positive integer. Put*

$$\varepsilon_i = \log_\alpha \left(1 + (-1)^{i-1} \left(\frac{|\beta|}{\alpha}\right)^{u_0}\right), \qquad \delta_i = \log_\alpha \left(\frac{1 + (-1)^{i-1} \left(\frac{|\beta|}{\alpha}\right)^{u_0}}{\sqrt{5}}\right)$$

for $i = 1,\ 2$, respectively. Here, $\log_\alpha$ is the logarithm in base α. Then for all integers $u \geq u_0$, the two inequalities

$$\alpha^{u+\varepsilon_2} \leq L_u \leq \alpha^{u+\varepsilon_1} \tag{4}$$

and

$$\alpha^{u+\delta_2} \leq F_u \leq \alpha^{u+\delta_1} \tag{5}$$

hold.

Proof. Let $c_0 = 1$, or $\sqrt{5}$, according to whether $u_n = L_n$ or $u_n = F_n$, respectively. Obviously,

$$\left.\begin{matrix} L_u \\ F_u \end{matrix}\right\} \leq \frac{\alpha^u + |\beta|^{u_0}}{c_0} \leq \frac{\alpha^u \left(1 + \frac{|\beta|^{u_0}}{\alpha^u}\right)}{c_0} \leq \alpha^u \left(\frac{1 + \left(\frac{|\beta|}{\alpha}\right)^{u_0}}{c_0}\right),$$

which prove the upper bounds from the formulae (4) and (5), respectively. Similarly,

$$\left.\begin{matrix} L_u \\ F_u \end{matrix}\right\} \geq \frac{\alpha^u - |\beta|^{u_0}}{c_0} \geq \frac{\alpha^u \left(1 - \frac{|\beta|^{u_0}}{\alpha^u}\right)}{c_0} \geq \alpha^u \left(\frac{1 - \left(\frac{|\beta|}{\alpha}\right)^{u_0}}{c_0}\right)$$

lead to the lower bounds from the formulae (4) and (5), respectively. □

Lemma 6. *Suppose that $a > 0$ and $b \geq 0$ are real numbers, and that u_0 is a positive integer. Then for all integers $u \geq u_0$, the inequality*

$$a\alpha^u + b \leq \alpha^{u+\kappa}$$

holds, where $\kappa = \log_\alpha \left(a + \frac{b}{\alpha^{u_0}}\right)$.

Proof. This is obvious. □

Lemma 7. *Assume that $a,\ b,\ z$ are integers. Furthermore, suppose that all the expressions appearing inside the* gcd*'s below are also integers. Then the following hold:*

(i) If $a \neq b$, then $\gcd\left(\frac{z+a}{2}, \frac{z+b}{4}\right) \leq \left|\frac{a-b}{2}\right|$. *Otherwise,* $\gcd\left(\frac{z+a}{2}, \frac{z+b}{4}\right) = \frac{z+b}{4}$;

(ii) If $3a \neq b$, then $\gcd\left(\frac{z+a}{2}, \frac{3z+b}{8}\right) \leq \left|\frac{3a-b}{2}\right|$. *Otherwise,* $\gcd\left(\frac{z+a}{2}, \frac{3z+b}{8}\right) = \frac{z+a}{8}$.

Proof. This is an easy applications of the Euclidean algorithm. □

Lemma 8. *Assume that $z \geq 8$ is an integer. Then the following hold:*

(i) If z is odd, then $L_{\frac{z-1}{2}} < \sqrt{2F_z}$;

(ii) If z is even, then $L_{\frac{z-2}{2}} < \sqrt{F_z}$.

Proof. For (i), note that

$$L^2_{\frac{z-1}{2}} = L_{z-1} + 2(-1)^{z-1} \leq L_{z-1} + 2 = F_{z-2} + F_z + 2,$$

and the right hand side above is easily seen to be smaller than $2F_z$ when $z \geq 8$. For (ii), we similarly have

$$L^2_{\frac{z-2}{2}} \leq L_{z-2} + 2 = F_{z-3} + F_{z-1} + 2 < F_z,$$

where the last inequality is equivalent to $F_{z-3} + 2 < F_{z-2}$, or $2 < F_{z-4}$, which is fulfilled for $z \geq 8$. □

Lemma 9. *All positive integer solutions of the system* (3) *satisfy $z \leq 2y$.*

Proof. The last two equations of system (3) imply that c divides both $F_y - 1$ and $F_z - 1$. Consequently,

$$c \mid \gcd(F_y - 1, F_z - 1). \tag{6}$$

Obviously, $F_z = bc + 1 < c^2$; hence, $\sqrt{F_z} < c$. From (6), we obtain $\sqrt{F_z} < F_y$. Clearly,

$$\sqrt{\frac{\alpha^z - 1}{\sqrt{5}}} < \sqrt{F_z} < F_y < \frac{\alpha^y + 1}{\sqrt{5}}. \tag{7}$$

Since $y \geq 5$ entails $\alpha^y + 1 < \sqrt[4]{5}\,\alpha^y$, we get $\alpha^z - 1 < \alpha^{2y}$, which easily leads to the conclusion that $2y \geq z$. □

2.2 The Proof of Theorem 2

By Lemma 9, we have

$$\sqrt{F_z} < \gcd(F_z - 1, F_y - 1). \tag{8}$$

Applying Lemma 4, we obtain

$$\gcd(F_z - 1, F_y - 1) = \gcd\left(F_{\frac{z-i}{2}}\, L_{\frac{z+i}{2}}\ ,\ F_{\frac{y-j}{2}}\, L_{\frac{y+j}{2}}\right) \leq \tag{9}$$

$$\leq \gcd\left(F_{\frac{z-i}{2}}\ ,\ F_{\frac{y-j}{2}}\right) \gcd\left(F_{\frac{z-i}{2}}\ ,\ L_{\frac{y+j}{2}}\right) \gcd\left(L_{\frac{z+i}{2}}\ ,\ F_{\frac{y-j}{2}}\right) \gcd\left(L_{\frac{z+i}{2}}\ ,\ L_{\frac{y+j}{2}}\right),$$

where $i, j \in \{\pm 1, \pm 2\}$. The values i and j depend on the residue classes of z and y modulo 4, respectively. In what follows, we let $d_1,\ d_2,\ d_3$ and d_4 denote suitable positive integers which will be defined shortly.

Lemma 3 yields

$$m_1 = F_{\gcd\left(\frac{z-i}{2}, \frac{y-j}{2}\right)} = F_{\frac{z-i}{2d_1}}. \tag{10}$$

The second factor m_2 on the right hand of (9) can be 1, 2, or

$$m_2 = L_{\gcd\left(\frac{z-i}{2}, \frac{y+j}{2}\right)} = L_{\frac{z-i}{2d_2}}. \tag{11}$$

The third factor m_3 is again 1, 2, or

$$m_3 = L_{\gcd\left(\frac{z+i}{2}, \frac{y-j}{2}\right)} = L_{\frac{z+i}{2d_3}}. \tag{12}$$

Finally, if the fourth factor m_4 is neither 1 nor 2, then

$$m_4 = L_{\gcd\left(\frac{z+i}{2}, \frac{y+j}{2}\right)} = L_{\frac{z+i}{2d_4}}. \tag{13}$$

We now distinguish two cases.

Case 1. $z \leq 150$.

In this case, we ran an exhaustive computer search to detect all positive integer solutions of system (3). Observe that we have

$$a = \sqrt{\frac{(F_x - 1)(F_y - 1)}{F_z - 1}}\,, \qquad 4 \leq x < y < z \leq 150.$$

Going through all the eligible values for $x,\ y$ and z, and checking if the above number a is an integer, we found no solution to system (3).

Case 2. $z > 150$.

In this case, Lemma 5 gives $-2 < \delta_1$ for F_z. Hence, $\alpha^{\frac{z-2}{2}} < \sqrt{F_z}$. If $d_k \geq 5$ holds for all $k = 1,\ 2,\ 3,\ 4$, then the subscripts $\frac{z \pm i}{2d_k}$ of the Fibonacci and Lucas numbers appearing in (10)–(13) are at most $\frac{z \pm i}{10}$ each. Lemma 5 now gives that $\varepsilon_2 < 0.5$ and $\delta_2 < -1$ hold for $L_{\frac{z \pm i}{10}}$ and $F_{\frac{z-i}{10}}$, respectively, because $\frac{z \pm i}{10} > 14$. Now formulae (8)–(13) lead to

$$\alpha^{\frac{z-2}{2}} < \sqrt{F_z} < \alpha^{\left(\frac{z-i}{10} - 1\right) + \left(\frac{z-i}{10} + 0.5\right) + \left(\frac{z+i}{10} + 0.5\right) + \left(\frac{z+i}{10} + 0.5\right)}, \tag{14}$$

which implies that

$$\frac{z-2}{2} < \frac{2z}{5} + 0.5,$$

contradicting the fact that $z > 150$.

From now on, we analyze those cases when at least one of the numbers d_k for $k = 1,\ 2,\ 3,\ 4$, which we will denote by d, is less than five.

First assume that $d = 4$. Then either $\frac{z+\eta_1 i}{8} = \frac{y+\eta_2 j}{2}$, or $\frac{z+\eta_1 i}{8} = \frac{y+\eta_2 j}{6}$, where $\eta_1,\ \eta_2 \in \{\pm 1\}$.

If the first equality holds, then Lemma 9 leads to $z = 4y + 4\eta_2 j - \eta_1 i \leq 2y$. Thus, $z \leq 2y \leq \eta_1 i - 4\eta_2 j \leq 10$, contradicting the fact that $z > 150$.

The second equality leads to $y = \frac{3z+3\eta_1 i-4\eta_2 j}{4}$. In this case,

$$\frac{y+\eta_2' j}{2} = \frac{3z + 3\eta_1 i + tj}{8}, \tag{15}$$

where $t = 4(\eta_2' - \eta_2) \in \{\pm 8, 0\}$ for $\eta_2' \in \{\pm 1\}$. Applying Lemma 7, we get

$$\begin{aligned} \gcd\left(\frac{z+\eta_1' i}{2}, \frac{y+\eta_2' j}{2}\right) &= \gcd\left(\frac{z+\eta_1' i}{2}, \frac{3z+3\eta_1 i+tj}{8}\right) \\ &\leq \left|\frac{3(\eta_1' - \eta_1)i - tj}{2}\right| \leq 14, \end{aligned} \tag{16}$$

for all $(\eta_1', \eta_2') \neq (\eta_1, \eta_2) \in \{\pm 1\}^2$. For the last inequality above, we used Lemma 7 together with the fact that $3(\eta_1' - \eta_1) - tj \neq 0$. Indeed, if $3(\eta_1 - \eta_1') - tj = 0$, then $3 \mid tj$, and since $t \in \{\pm 8, 0\}$, $j \in \{\pm 1, \pm 2\}$, we get that $t = 0$, therefore $\eta_2 = \eta_2'$. Since also $3(\eta_1 - \eta_1') = tj = 0$, we get $\eta_1 = \eta_1'$, therefore $(\eta_1', \eta_2') = (\eta_1, \eta_2)$, which is not allowed.

Continuing with the case $d = 4$, since $F_{14} < L_{14} = 843$ and $\frac{z\pm i}{8} > 18$, we get that $\varepsilon_2 < 0.25$ and $\delta_2 < 0.25$, where these values correspond to $L_{\frac{z\pm i}{8}}$ and $F_{\frac{z\pm i}{8}}$, respectively. It now follows that

$$\alpha^{\frac{z-2}{2}} < \alpha^{\frac{z\pm i}{8}+0.25} L_{14}^3 \leq 843^3 \alpha^{\frac{z+2}{8}+0.25}.$$

Thus, $z < 4 + 8\log_\alpha 843 < 116$, which completes the analysis for this case.

Consider now the case $d = 3$. The only possibility is $\frac{z+\eta_1 i}{6} = \frac{y+\eta_2 j}{2}$ for some $\eta_1, \eta_2 \in \{\pm 1\}$. Together with Lemma 9, we get $z = 3y + 3\eta_2 j - \eta_1 i \leq 2y$. Consequently, $\frac{z}{2} \leq y \leq \eta_1 i - 3\eta_2 j \leq 8$, which is impossible.

Assume next that $d = 2$. Then $\frac{z+\eta_1 i}{4} = \frac{y+\eta_2 j}{2}$ for some $\eta_1, \eta_2 \in \{\pm 1\}$. We get that $y = \frac{z+\eta_1 i-2\eta_2 j}{2}$. Thus, $\frac{y+\eta_2' j}{2} = \frac{z+\eta_1 i+tj}{4}$ with $t = 2(\eta_2' - \eta_2) \in \{\pm 4, 0\}$. By Lemma 7, we have

$$\begin{aligned} \gcd\left(\frac{z+\eta_1' i}{2}, \frac{y+\eta_2' j}{2}\right) &= \gcd\left(\frac{z+\eta_1' i}{2}, \frac{z+\eta_1 i+tj}{4}\right) \\ &\leq |(\eta_1' - \eta_1)i - tj| \leq 12. \end{aligned}$$

The argument works assuming that the last number above is not zero for $(\eta_1', \eta_2') \neq (\eta_1, \eta_2) \in \{\pm 1\}^2$. Assume that it is. Then $(\eta_1' - \eta_1)i = tj$. Clearly, tj is always a multiple of 4. If it is zero, then $t = 0$, so $\eta_2' = \eta_2$. Then also $(\eta_1 - \eta_1')i = tj = 0$,

therefore $\eta_1' = \eta_1$. Hence, $(\eta_1', \eta_2') = (\eta_1, \eta_2)$, which is not allowed. Assume now that $t \neq 0$. Then $(\eta_1 - \eta_1')i \neq 0$, so $\eta_1' = -\eta_1$. Also, $t \neq 0$, therefore $\eta_2 = -\eta_2'$. We get that $2\eta_1 i = -4\eta_2 j$, therefore $\eta_1 i = -2\eta_j$. Thus, $i = \pm 1$ and $j = \pm 2$. In particular, z is odd and y is even. Now $(z + \eta_1 i)/2$ is divisible by a larger power of 2 than $(y + \eta_2 j)/2$. A quick inspection of formulae (10)–(13) defining m_1, m_2, m_3 and m_4 together with Lemma 3 (ii) and (iii), shows that the only interesting cases are when $k = 1$ or 2 (since $m_3 \mid 2$ and $m_4 \mid 2$). Thus, $(\eta_1, \eta_2) = (-1, -1)$ or $(-1, 1)$. Hence, $(\eta_1', \eta_2') = (1, 1)$ or $(1, -1)$, and here we have that $m_3 \mid 2$ and $m_4 \mid 2$ anyway. This takes care of the case when $(\eta_1' - \eta_1)i - tj = 0$.

Continuing with $d = 2$, since $\frac{z \pm i}{4} \geq 37$, Lemma 5 yields $\varepsilon_2, \delta_2 < 0.1$. We then get the estimate

$$\alpha^{\frac{z-2}{2}} < \alpha^{\frac{z \pm i}{4} + 0.1} L_{12}^3 \leq 322^3 \alpha^{\frac{z+2}{4} + 0.1},$$

leading to $z < 6.4 + 12 \log_\alpha 322 < 150.5$, which is a contradiction.

	(z, y) (4)	(i, j)	possible equalities	consequence
1	$(1, 1)$	$(1, -1)$	$\frac{z-1}{2} = \frac{y+1}{2}$	$z = y + 2$ † : $x \equiv y \pmod 4$
2	$(1, 2)$	$(1, -2)$	$\frac{z-1}{2} = \frac{y+2}{2}$	$z = y + 3$ † : d_2 must be even
		$(-1, -2)$	$\frac{z+1}{2} = \frac{y+2}{2}$	$z = y + 1$ † : $z \equiv y - 1 \pmod 4$
3	$(1, 3)$	$(1, -1)$	$\frac{z-1}{2} = \frac{y+1}{2}$	$z = y + 2$ † : d_1 must be even
4	$(1, 0)$	$(1, -2)$	$\frac{z-1}{2} = \frac{y+2}{2}$	$z = y + 3$ † : $x \equiv y + 1 \pmod 4$
		$(-1, -2)$	$\frac{z+1}{2} = \frac{y+2}{2}$	$z = y + 1$ **is possible** $(d_3 = 1)$
5	$(3, 1)$	$(1, -1)$	$\frac{z-1}{2} = \frac{y+1}{2}$	$z = y + 2$ **is possible** $(d_4 = 1)$
6	$(3, 2)$	$(-1, -2)$	$\frac{z+1}{2} = \frac{y+2}{2}$	$z = y + 1$ † : d_2 must be even
		$(1, -2)$	$\frac{z-1}{2} = \frac{y+2}{2}$	$z = y + 3$ † : $x \equiv y + 1 \pmod 4$
7	$(3, 3)$	$(1, -1)$	$\frac{z-1}{2} = \frac{y+1}{2}$	$z = y + 2$ † : $x \equiv y \pmod 4$
8	$(3, 0)$	$(-1, -2)$	$\frac{z+1}{2} = \frac{y+2}{2}$	$z = y + 1$ † : $x \equiv y - 1 \pmod 4$
		$(1, -2)$	$\frac{z-1}{2} = \frac{y+2}{2}$	$z = y + 3$ **is possible** $(d_3 = 1)$
9	$(2, 1)$	$(2, 1)$	$\frac{z-2}{2} = \frac{y-1}{2}$	$z = y + 1$ † : d_1 must be even
		$(2, -1)$	$\frac{z-2}{2} = \frac{y+1}{2}$	$z = y + 3$ † : $x \equiv y + 1 \pmod 4$
10	$(2, 2)$	$(2, -2)$	$\frac{z-2}{2} = \frac{y+2}{2}$	$z = y + 4$ † : d_2 must be even
11	$(2, 3)$	$(2, -1)$	$\frac{z-2}{2} = \frac{y+1}{2}$	$z = y + 3$ † : d_1 must be even
		$(2, 1)$	$\frac{z-2}{2} = \frac{y-1}{2}$	$z = y + 1$ † : $x \equiv y - 1 \pmod 4$
12	$(2, 0)$	$(2, -2)$	$\frac{z-2}{2} = \frac{y+2}{2}$	$z = y + 4$ † : $x \equiv y + 2 \pmod 4$
13	$(0, 1)$	$(2, 1)$	$\frac{z-2}{2} = \frac{y-1}{2}$	$z = y + 1$ † : $x \equiv y - 1 \pmod 4$
		$(2, -1)$	$\frac{z-2}{2} = \frac{y+1}{2}$	$z = y + 3$ **is possible** $(d_4 = 1)$
14	$(0, 2)$	$(2, -2)$	$\frac{z-2}{2} = \frac{y+2}{2}$	$z = y + 4$ † : $x \equiv y + 2 \pmod 4$
15	$(0, 3)$	$(2, -1)$	$\frac{z-2}{2} = \frac{y+1}{2}$	$z = y + 3$ † : $x \equiv y + 1 \pmod 4$
		$(2, 1)$	$\frac{z-2}{2} = \frac{y-1}{2}$	$z = y + 1$ **is possible** $(d_4 = 1)$
16	$(0, 0)$	$(2, -2)$	$\frac{z-2}{2} = \frac{y+2}{2}$	$z = y + 4$ **is possible** $(d_3 = 1)$

Table 1. The case $d = 1$.

Finally, we assume that $d = 1$. The equality $\frac{z\pm i}{2} = \frac{y\pm j}{2}$ leads to $z = y \mp i \pm j$. Obviously, here $\mp i \pm j$ must be positive, otherwise we would get $z \le y$. Note that in the application of Lemma 4, both z and y are classified according to their congruence classes modulo 4. The following table summarizes the critical cases of $d = 1$. Only 6 layouts in Table 1 below need further investigations (the sign † abbreviates a contradiction).

In what follows, we consider separately the 6 exceptional cases. The common treatment of all these cases is to go back to the system (3). In all exceptional cases we have $z = y + s$, where $s \in \{1, 2, 3, 4\}$. Hence,

$$\left\{ \begin{array}{lcl} ab+1 & = & F_x, \\ ac+1 & = & F_{z-s}, \\ bc+1 & = & F_z, \end{array} \right. \tag{17}$$

and, as previously, $c \mid \gcd(F_{z-s} - 1, F_z - 1)$.

Table 1, Row 4. $z \equiv 1,\ y \equiv 0 \pmod 4$, $z = y + 1$ and

$$F_{z-1} - 1 = F_{\frac{z+1}{2}} L_{\frac{z-3}{2}}, \qquad F_z - 1 = F_{\frac{z-1}{2}} L_{\frac{z+1}{2}}.$$

Clearly,

$$\gcd\left(F_{\frac{z+1}{2}}, F_{\frac{z-1}{2}}\right) = 1, \quad \gcd\left(L_{\frac{z-3}{2}}, L_{\frac{z+1}{2}}\right) = 1, \quad \gcd\left(F_{\frac{z+1}{2}}, L_{\frac{z+1}{2}}\right) = 1,\ 2,$$

while

$$\gcd(L_{\frac{z-3}{2}}, F_{\frac{z-1}{2}}) = \left\{ \begin{array}{l} L_{\gcd\left(\frac{z-3}{2}, \frac{z-1}{2}\right)} = L_1 = 1 \\ 1 \text{ or } 2 \end{array} \right\} \le 2.$$

Therefore $c \le 4$, and we arrived at a contradiction because $F_z = bc+1 \le 13$ contradicts $z > 150$.

Table 1, Row 5. $z \equiv 3,\ y \equiv 1 \pmod 4$, $z = y + 2$ and

$$F_{z-2} - 1 = F_{\frac{z-3}{2}} L_{\frac{z-1}{2}}, \qquad F_z - 1 = F_{\frac{z+1}{2}} L_{\frac{z-1}{2}}.$$

Since

$$\gcd\left(F_{\frac{z-3}{2}}, F_{\frac{z+1}{2}}\right) = 1,$$

we get $c \mid \gcd(F_{z-2} - 1, F_z - 1) = L_{\frac{z-1}{2}}$. Consequently, by the proof of Lemma 9,

$$L_{\frac{z-1}{2}} = c_1 c > c_1 \sqrt{F_z}.$$

By Lemma 8, we now have

$$c_1 < \frac{L_{\frac{z-1}{2}}}{\sqrt{F_z}} < 2.$$

Hence, $c_1 = 1$, therefore $c = L_{\frac{z-1}{2}}$. In view of equation (17), we get $a = F_{\frac{z-3}{2}},\ b = F_{\frac{z+1}{2}}$, and so

$$F_x = F_{\frac{z-3}{2}} F_{\frac{z+1}{2}} + 1 = F_{\frac{z-1}{2}}^2 + (-1)^{\frac{z-1}{2}} + 1 = F_{\frac{z-1}{2}}^2. \tag{18}$$

By the work of Cohn [4], we get that (18) is not possible for $z > 150$.

Table 1, Row 8. $z \equiv 3,\ y \equiv 0 \pmod 4$, $z = y + 3$ and

$$F_{z-3} - 1 = F_{\frac{z-1}{2}} L_{\frac{z-5}{2}}, \qquad F_z - 1 = F_{\frac{z+1}{2}} L_{\frac{z-1}{2}}.$$

It follows easily, by Lemma 3, that

$$\gcd\left(F_{\frac{z-1}{2}}, F_{\frac{z+1}{2}}\right) = 1, \quad \gcd\left(L_{\frac{z-5}{2}}, L_{\frac{z-1}{2}}\right) = 1, \quad \gcd\left(F_{\frac{z-1}{2}}, L_{\frac{z-1}{2}}\right) = 1,\ 2,$$

and

$$\gcd\left(L_{\frac{z-5}{2}}, F_{\frac{z+1}{2}}\right) = \left\{ \begin{array}{l} L_{\gcd\left(\frac{z+1}{2}, \frac{z-5}{2}\right)} \le L_3 = 4 \\ 1 \text{ or } 2 \end{array} \right\} \le 4.$$

Thus, $c \mid \gcd(F_{z-3} - 1, F_z - 1) \le 8$. However, the inequalities $a < b < c \le 8$ contradict the fact that $z > 150$.

Table 1, Row 13. $z \equiv 0,\ y \equiv 1 \pmod 4$, $z = y + 3$ and

$$F_{z-3} - 1 = F_{\frac{z-4}{2}} L_{\frac{z-2}{2}}, \qquad F_z - 1 = F_{\frac{z+2}{2}} L_{\frac{z-2}{2}}. \tag{19}$$

Since

$$\gcd\left(F_{\frac{z-4}{2}}, F_{\frac{z+2}{2}}\right) = F_{\gcd\left(\frac{z-4}{2}, \frac{z+2}{2}\right)} \le F_3 = 2,$$

we have $c \mid \gcd(F_{z-2} - 1, F_z - 1) = L_{\frac{z-1}{2}}$, or $c \mid \gcd(F_{z-2} - 1, F_z - 1) = 2L_{\frac{z-1}{2}}$.

In the first case, we get

$$L_{\frac{z-2}{2}} = c_2 c > c_2 \sqrt{F_z},$$

and applying Lemma 8 we arrive at

$$c_2 < \frac{L_{\frac{z-1}{2}}}{\sqrt{F_z}} < 1,$$

which is a contradiction.

In the second case, put

$$2L_{\frac{z-2}{2}} = c_3 c > c_3 \sqrt{F_z}.$$

Again by Lemma 8, we obtain

$$c_3 < \frac{2L_{\frac{z-1}{2}}}{\sqrt{F_z}} < 2.$$

Thus, $c_3 = 1$, therefore $c = 2L_{\frac{z-1}{2}}$. System (17) and relations (19) lead to $2a = F_{\frac{z-4}{2}}$, $2b = F_{\frac{z+2}{2}}$, and

$$F_x = \frac{1}{4} F_{\frac{z-4}{2}} F_{\frac{z+2}{2}} + 1.$$

On the one hand, since $z > 150$, by Lemma 5, we get

$$\alpha^{x-1.67} > F_x > \frac{1}{4}\alpha^{\frac{z-4}{2}-1.68}\alpha^{\frac{z+2}{2}-1.68} > \alpha^{z-1-3.36-2.89},$$

therefore $x > z - 5.48$. On the other hand, by combining Lemma 5 and Lemma 6 with $\kappa < 0.01$, we get

$$\alpha^{x-1.68} < F_x < \frac{1}{4}\alpha^{\frac{z-4}{2}-1.67}\alpha^{\frac{z+2}{2}-1.67} + 1 < \alpha^{z-1-3.34-2.88+0.01},$$

leading to $x < z - 5.53$. But the interval $(z - 5.48, z - 5.53)$ does not contain any integer, which takes care of this case.

Table 1, Row 15. $z \equiv 0,\ y \equiv 3 \pmod 4$, $z = y + 1$ and

$$F_{z-1} - 1 = F_{\frac{z}{2}} L_{\frac{z-2}{2}}, \qquad F_z - 1 = F_{\frac{z+2}{2}} L_{\frac{z-2}{2}}.$$

Since

$$\gcd(F_{\frac{z}{2}}, F_{\frac{z+2}{2}}) = 1,$$

we get $c \mid \gcd(F_{z-1} - 1, F_z - 1) = L_{\frac{z-2}{2}}$. Consequently, by the proof of Lemma 9, it follows that

$$L_{\frac{z-2}{2}} = c_4 c > c_4\sqrt{F_z}.$$

Now Lemma 8 leads to the contradiction

$$c_4 < \frac{L_{\frac{z-2}{2}}}{\sqrt{F_z}} < 1.$$

Table 1, Row 16. $z \equiv 0,\ y \equiv 0 \pmod 4$, $z = y + 4$ and

$$F_{z-4} - 1 = F_{\frac{z-2}{2}} L_{\frac{z-6}{2}}, \qquad F_z - 1 = F_{\frac{z+2}{2}} L_{\frac{z-2}{2}}.$$

Obviously,

$$\gcd(F_{\frac{z-2}{2}}, F_{\frac{z+2}{2}}) = 1, \qquad \gcd(L_{\frac{z-6}{2}}, L_{\frac{z-2}{2}}) = 1, \qquad \gcd(F_{\frac{z-2}{2}}, L_{\frac{z-2}{2}}) = 1,\ 2,$$

while

$$\gcd(L_{\frac{z-6}{2}}, F_{\frac{z+2}{2}}) = \left\{ \begin{array}{l} L_{\gcd\left(\frac{z-6}{2}, \frac{z+2}{2}\right)} \le L_4 = 7 \\ 1 \text{ or } 2 \end{array} \right\} \le 7.$$

Thus, $c \leq 14$, which leads to a contradiction with $z > 150$.

The proof of the Theorem 2 is now complete.

Acknowledgments. During the preparation of this paper, F. L. was supported in part by Grants SEP-CONACyT 79685 and PAPIIT 100508, and L. S. was supported in part by a János Bolyai Scholarship of HAS and the Hungarian National Foundation for Scientific Research Grants No. T 048945 MAT and K 61800 FT2.

References

[1] Y. Bugeaud and A. Dujella, 'On a problem of Diophantus for higher powers', Math. Proc. Cambridge Philos. Soc. **135** (2003), 1–10.

[2] Y. Bugeaud and K. Gyarmati, 'On generalizations of a problem of Diophantus', Illinois J. Math. **48** (2004), 1105–1115.

[3] R. D. Carmichael, 'On the numerical factors of the arithmetic function $\alpha^n \pm \beta^n$ ', Annals Math., 2nd Ser., **15** No. 1/4. (1913-1914), 30–48.

[4] J. H. E. Cohn, 'On square Fibonacci numbers', J. London Math. Soc., **39** (1964), 537-540.

[5] A. Dujella, 'There are only finitely many Diophantine quintuples', *J. reine angew. Math.* **566** (2004), 183–214.

[6] R. Finkelstein, 'On Fibonacci numbers which are one more then a square', *J. reine angew. Math.* **262/263** (1973), 171–182.

[7] C. Fuchs, F. Luca and L. Szalay, 'Diophantine triples with values in binary recurrences', *Preprint*, 2007.

[8] P. Gibbs, 'Some rational Diophantine sextuples', *Glas. Mat. Ser. III* **41(61)** (2006), 195–203.

[9] K. Gyarmati, A. Sarkozy and C. L. Stewart, 'On shifted products which are powers', Mathematika **49** (2002), 227–230.

[10] K. Gyarmati and C. L. Stewart, 'On powers in shifted products', Glas. Mat. Ser. III **42** (2007), 273–279.

[11] R. Knott, *Fibonacci Numbers and the Golden Section*, http://www.mcs.surrey.ac.uk/Personal/R.Knott/Fibonacci/.

[12] T. Koshy, *Fibonacci and Lucas numbers with applications*, Wiley-Interscience, New York, 2001.

[13] F. Luca, 'On shifted products which are powers', Glas. Mat. Ser. III **40** (2005), 13–20.

[14] F. Luca and L. Szalay, 'Fibonacci numbers of the form $p^a \pm p^b + 1$', *Fibonacci Quart.*, to appear.

dc_871_14

dc_871_14

Nurettin Irmak, László Szalay

Diophantine triples and reduced quadruples with the Lucas sequence of recurrence $u_n = Au_{n-1} - u_{n-2}$

Elfogadva: Glasnik Matematicki, 2013.

Diophantine triples and reduced quadruples with the Lucas sequence of recurrence $u_n = Au_{n-1} - u_{n-2}$

Nurettin Irmak, László Szalay

Abstract

In this study, we show that there is no positive integer triple $\{a, b, c\}$ such that all of $ab + 1,\ ac + 1$ and $bc + 1$ are in the sequence $\{u_n\}_{n\geq 0}$ satisfies the recurrence $u_n = Au_{n-1} - u_{n-2}$ with the initial values $u_0 = 0,\ u_1 = 1$. Further, we investigate the analogous question for the quadruples $\{a, b, c, d\}$ with $abc+1 = u_x$, $bcd + 1 = u_y$, $cda + 1 = u_z$ and $dab + 1 = u_t$, and deduce the non-existence of such quadruples.

1 Introduction

A Diophantine m-tuple is a set $\{a_1, a_2, \ldots, a_m\}$ of positive integers such that $a_i a_j + 1$ is a square for all $1 \leq i < j \leq m$. This problem and its variations have a rich history. Diophantus investigated first, although rational quadruples, and found the set $\{1/16, 33/16, 68/16, 105/16\}$. Fermat was the first who could give an integer quadruple, namely the set $\{1, 3, 8, 120\}$.

It is widely known that infinitely many integer Diophantine quadruples exist. For instance, Hoggatt and Bergum [5] proved that for any positive integer k, the set

$$\{F_{2k},\ F_{2k+2},\ F_{2k+4},\ 4F_{2k+1}F_{2k+2}F_{2k+3}\}$$

is always quadruple. A widely believed conjecture states that no quintuple exists. The famous theorem of Dujella [3] states that there are only finitely many quintuples.

A variant of the problem is obtained if one replaces the squares by the terms of a given binary recurrence. For details, see the articles [4], [6], [7] and [1]. The first cited paper investigates a general case and provides sufficient and necessary conditions to have only finitely diophantine triples with terms of the binary recurrent sequence. But the arguments in [4] give no hint how to find the triples themselves. The other papers describe methods to determine all Diophantine triples for Fibonacci, Lucas and balancing numbers, respectively.

In this paper, we follow the treatment of the above results, but there is an essential difference, namely the binary recurrence we investigate here contains a positive integer parameter A. Therefore, we must include new, additional ideas in order to prove our theorems.

Assume that A is a given positive integer. Define the sequence $\{u_n\}$ by

$$u_n = Au_{n-1} - u_{n-2}$$

with the initial conditions $u_0 = 0$, $u_1 = 1$. The Binet formula

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$$

gives u_n explicitly, where $\alpha = (A + \sqrt{A^2 - 4})/2$ and $\beta = (A - \sqrt{A^2 - 4})/2$. Obviously, $\alpha + \beta = A$ and $\alpha\beta = 1$. Further the condition $A \geq 3$ entails that the zeros of the characteristic polynomial $x^2 - Ax + 1$ are real, have $\alpha > 1$ and $\beta \in (0, 1)$ and moreover α increases and β decreases when A increases. We define $\{v_n\}_{n\geq 0}$ as the associated sequence of $\{u_n\}_{n\geq 0}$. The recurrence relation for $\{u_n\}_{n\geq 0}$ and $\{v_n\}_{n\geq 0}$ coincide, but the initial conditions in the second case are $v_0 = 2$ and $v_1 = A$. It is well-known that

$$v_n = \alpha^n + \beta^n.$$

The main results of this work are the following.

Theorem 1. *Suppose that $A \neq 2$ is a positive integer. Then there do not exist integers $1 \leq a < b < c$ such that*

$$\begin{aligned} ab + 1 &= u_x, \\ ac + 1 &= u_y, \\ bc + 1 &= u_z \end{aligned} \tag{1}$$

hold with the natural numbers $1 \leq x < y < z$.

Note that $A = 2$ gives that the sequence $\{u_n\}_{n\geq 0}$ is the sequence of all natural numbers and in this case, trivially, system (1) is satisfied by arbitrary a, b and c. Clearly, it will also be true for (2).

Theorem 2. *If $A \neq 2$ is a positive integer then the system*

$$\begin{aligned} abc + 1 &= u_x, \\ bcd + 1 &= u_y, \\ cda + 1 &= u_z, \\ dab + 1 &= u_t \end{aligned} \tag{2}$$

is not solvable in the integers $1 \leq a < b < c < d$ and $1 \leq x < t < z < y$.

Observe, that although the last three equations of (2) would generalize system (1) by one more unknown d, here we have the additional equation $abc + 1 = u_x$.

Note that the case $A = 1$ provides the periodic sequence

$$u_n = 0, 1, 1, 0, -1, -1, \ldots.$$

Hence, neither (1) nor (2) cannot be fulfilled with $A = 1$. Thus, in the sequel, we assume $A \geq 3$.

In the next part, we gather the auxiliary results which are needed in the proofs of the theorems.

2 Preliminary Results

Lemma 3. *Assume that n and m are arbitrary non-negative integers. Then the following identities hold.*

1. $\gcd(u_n, u_m) = u_{\gcd(n,m)}$,
2. $\gcd(u_n, v_m) = 1$ *or* 2 *or* $v_{\gcd(n,m)}$, *especially* $\gcd(u_n, v_n) = 1$ *or* 2,
3. $(u_n - 1)(u_n + 1) = u_{n-1}u_{n+1}$,
4. $u_{2n+1} - 1 = u_n v_{n+1}$,
5. $2u_{n+m} = u_n v_m + v_n u_m$.

Proof. The first two identities are known from [2]. Paper [9] contains (3), the remaining identities can be proved by using Binet formula. For instance,

$$\begin{aligned} u_n v_{n+1} &= \left(\frac{\alpha^n - \beta^n}{\alpha - \beta}\right)\left(\alpha^{n+1} + \beta^{n+1}\right) \\ &= \frac{\alpha^{2n+1} - \beta^{2n+1}}{\alpha - \beta} - (\alpha\beta)^n = u_{2n+1} - 1. \end{aligned}$$

□

Lemma 4. *Suppose that $A \geq 3$. Then for all integers $n \geq 3$, the inequalities*

$$\alpha^{n-1} < u_n < \alpha^{n-0.83} \tag{3}$$

and

$$\alpha^n < v_n < \alpha^{n+0.004} \tag{4}$$

hold.

Proof. Using the Binet formula of the sequence $\{u_n\}_{n\geq 0}$, we obtain

$$\alpha^{n-1} < \frac{\alpha^n - \beta^n}{\alpha - \beta} = u_n = \frac{\alpha^n}{\alpha - \beta}\left(1 - \left(\frac{\beta}{\alpha}\right)^n\right) < \alpha^{n-\log_\alpha(\alpha-\beta)}. \tag{5}$$

To justify the right hand side, we show that the function

$$f(\alpha) = \log_\alpha\left(\alpha - \frac{1}{\alpha}\right) = \frac{\log(\alpha^2-1)}{\log\alpha} - 1$$

is strictly increasing for $\alpha > 1$. Indeed, $f'(\alpha) > 0$ is a consequence of the arguments

$$(\alpha^2-1)\log(\alpha^2-1) < (\alpha^2-1)\log\alpha^2 < 2\alpha^2\log\alpha.$$

Replacing α by the worst case $(3+\sqrt{5})/2$ (it corresponds to the smallest possibility for A which is $A = 3$) in the exponent of the rightmost term of (5), it leads to $u_n < \alpha^{n-0.83}$.

The lower bound in (4) for v_n is trivial. To have an upper bound, we evaluate

$$v_n \leq \alpha^n\left(1 + \frac{1}{\alpha^6}\right) < 1.0032 \cdot \alpha^n < \alpha^{n+0.004}.$$

□

Remark 5. *Since the estimate of the right hand side of (3) does not depend on the condition $n \geq 3$, we conclude that it remains valid for any $n \in \mathbb{N}$. A similar observation is true for the left hand side of (4).*

Lemma 6. *Suppose $A \geq 3$. Then $\log_\alpha(2(A^2-2)) < 3.1$.*

Proof. Let $g(\alpha) = \log(\alpha + 1/\alpha)/\log\alpha$ and $h(\alpha) = \log_\alpha(2)$. It is easy to see that the functions $g(\alpha)$ and $h(\alpha)$ are strictly decreasing when $\alpha > 1$. Thus, the largest possible value $\alpha = (3+\sqrt{5})/2$ belonging to the case $A = 3$, together with

$$\log_\alpha(A^2-2) < 2\log_\alpha A = 2g(\alpha)$$

shows the statement. □

Lemma 7. *Assume that $n \geq 3$ and $A \geq 3$ are integers. Then*

$$\gcd(u_n - 1, u_{n-2} - 1) \leq 2(A^2-2).$$

Proof. Put $g = \gcd(u_n - 1, u_{n-2} - 1)$. The recurrence relation of the sequence $\{u_n\}_{n\geq 0}$, together with Lemma 3 (1) and (3) yields

$$\begin{aligned} g &= \gcd(u_n - 1, u_n - u_{n-2}) \leq \gcd(u_{n-1}u_{n+1}, u_n - u_{n-2}) \\ &\leq \gcd(u_{n-1}, Au_{n-1} - 2u_{n-2})\gcd(u_{n+1}, 2u_n - Au_{n-1}) \\ &\leq 2\gcd\left(u_{n+1}, (2-A^2)u_n + Au_{n+1}\right) \leq 2(A^2-2). \end{aligned}$$

□

Lemma 8. *Any integer $n \geq 2$ satisfies*

$$\gcd(u_{2n-3} - 1, u_n - 1) < \alpha^{5.7}.$$

Proof. Similarly to the previous Lemma, put $g = \gcd(u_{2n-3} - 1, u_n - 1)$ and apply (4) of Lemma 3. It implies

$$\begin{aligned} g &= \gcd(u_{n-2}v_{n-1}, u_{n-1}u_{n+1}) \\ &\leq \gcd(u_{n-2}, u_{n-1}) \gcd(u_{n-2}, u_{n+1}) \gcd(v_{n-1}, u_{n-1}) \gcd(v_{n-1}, u_{n+1}). \end{aligned}$$

By (5) of Lemma 3, we have $2u_{n+1} = u_{n-1}v_2 + v_{n-1}u_2$, which together with (1) and (2) of Lemma 3 yields

$$g \leq 2u_3 \gcd(v_{n-1}, u_{n-1}v_2 + u_2v_{n-1}) \leq 4u_3v_2 < \alpha^{5.7}.$$

□

Lemma 9. *Any integer $n \geq 2$ satisfies*

$$\gcd(u_{2n-2} - 1, u_n - 1) < \alpha^{6.4}.$$

Proof. Put $g = \gcd(u_{2n-2} - 1, u_n - 1)$.

$$\begin{aligned} g &= \gcd(u_{2n-1}u_{2n-3}, u_{n-1}u_{n+1}) \\ &\leq \gcd(u_{2n-1}, u_{n-1}) \gcd(u_{2n-1}, u_{n+1}) \\ &\quad \times \gcd(u_{2n-3}, u_{n-1}) \gcd(u_{2n-3}, u_{n+1}) \\ &\leq u_1^2 u_3 u_5 < \alpha^{6.4}. \end{aligned}$$

□

Lemma 10. *All positive solutions to system (1) satisfy $z \leq 2y - 1$.*

Proof. Considering the last two equations of system (1) we have

$$c \mid \gcd(u_y - 1, u_z - 1).$$

Moreover $u_z = bc + 1 < c^2$, therefore $\sqrt{u_z} < c$ holds. By (3), we obtain

$$\sqrt{\alpha^{z-1}} < \sqrt{u_z} < c < u_y < \alpha^{y-0.83},$$

which implies $z < 2y - 0.66$, so $z \leq 2y - 1$. □

Lemma 11. *The solutions to system (2) satisfy the inequality $y \leq 2z - 1$.*

Proof. Clearly, $u_y = bcd + 1 < (cd)^2$, so $\sqrt{u_y} < cd$. From system (2), we deduce that

$$cd \mid \gcd(u_y - 1, u_z - 1).$$

By Lemma 4,

$$\sqrt{\alpha^{y-1}} < \sqrt{u_y} < cd < u_z < \alpha^{z-0.83},$$

which leads to $y \leq 2z - 1$. □

3 Proof of Theorem 2

Suppose that $A \geq 3$. Further suppose $1 \leq a < b < c$ and that $1 \leq x < y < z$ satisfy (1). Then, $1 \cdot 2 + 1 \leq ab + 1 = u_x$ implies $x \geq 2$. Now we distinguish two cases.

Case 1. $z \leq 138$.

Firstly, we find upper bound for the coefficient A of the sequence $\{u_n\}_{n\geq 0}$.

Lemma 12. *If $z \leq 138$ and there exist a solution to system (1) then $A \leq A_0$ with a suitable $A_0 \in \mathbb{N}^+$.*

Proof. Clearly, the terms of the sequence $\{u_n\}$ are monic polynomials in A with $\deg(u_n(A)) = n - 1$ $(n \geq 1)$, the first few terms are $u_0(A) = 0,\ u_1(A) = 1$ and

$$u_2(A) = A, \quad u_3(A) = A^2 - 1, \quad u_4(A) = A^3 - 2A, \quad \ldots .$$

If $2 \leq x < y < z \leq 138$ and $1 \leq a < b < c$ satisfy (1) then

$$a = \sqrt{\frac{(u_x(A) - 1)\,(u_y(A) - 1)}{u_z(A) - 1}}$$

must be necessarily integer for some A. Since $u_z(A)$ is monic, then by polynomial division, there uniquely exist polynomials $q(A) \in \mathbb{Z}[A]$ and $r(A) \in \mathbb{Z}[A]$ such that

$$(u_x\,(A) - 1)\,(u_y\,(A) - 1) = q\,(A) \cdot (u_z\,(A) - 1) + r\,(A)\,,$$

where $\deg\,(r\,(A)) < \deg\,(u_z\,(A))$.

Checking the eligible possibilities for x, y and z by computer, $r(A)$ is never the constant zero polynomial. Hence,

$$\frac{(u_x(A) - 1)\,(u_y(A) - 1)}{u_z(A) - 1} = q\,(A) + \frac{r\,(A)}{u_z\,(A) - 1} \tag{6}$$

follows. Again a computer verification shows that there is no positive integer $A \geq 3$ satisfying the equation $r(A) = 0$ with the condition $z \leq 138$. Thus the fraction $r(A)/(u_z(A) - 1)$ never disappears on the right hand side of (6).

If for some A the left hand side of the equation (6) is integer, then by $q\,(A) \in \mathbb{N}$, we deduce that

$$\frac{r\,(A)}{u_z\,(A) - 1}$$

is so. But $\deg\,(r\,(A)) < \deg\,(u_z\,(A))$, so A cannot be large since

$$\lim_{A\to\infty} \frac{r\,(A)}{u_z\,(A) - 1} = 0.$$

Consequently, $|r\,(A)\,| \geq u_z\,(A) - 1$ must hold, which proves $A \leq A_0$ with some positive integer A_0. To obtain the exact upper bound, we run a computer search with the conditions $2 \leq x < y < z \leq 138$, and we found that $A_0 = 2$. □

Then, by Lemma 12 we obtain immediately that there is no solution to the system (1) in the first case.

Case 2. $z > 138$.

Put $P = \gcd(u_z - 1, u_y - 1)$. By (1) and (3) of Lemma 3, we have

$$\begin{aligned} P &= \gcd(u_{z-1}u_{z+1}, u_{y-1}u_{y+1}) \\ &\leq \prod_{i,j\in\{\pm 1\}} \gcd(u_{z-i}, u_{y-j}) = \prod_{i,j\in\{\pm 1\}} u_{\gcd(z-i,y-j)}. \end{aligned} \tag{7}$$

Let us say that $\gcd(z-i, y-j) = \frac{z-i}{t_{ij}}$ for some positive integer t_{ij}.

Suppose that $t_{ij} \geq 8$ holds for all pairs $(i,j) \in \{\pm 1\}^2$. Then Lemma (4) implies that

$$\alpha^{\frac{z-1}{2}} < \sqrt{u_z} < c \leq P \leq u^2_{\frac{z-1}{8}} u^2_{\frac{z+1}{8}} < \alpha^{4\left(\frac{z+1}{8} - 0.83\right)}. \tag{8}$$

If we compare the exponents of α in (8), we arrive at a contradiction.

In what follows, we assume that $t_{ij} \leq 7$ holds for some pair. Let k denote this t_{ij}. Further suppose that

$$\frac{z-i}{k} = \frac{y-j}{\ell}$$

holds for a suitable positive integer ℓ coprime to k.

Suppose for the moment that $\ell > k$. Then $z - i < y - j$ implies $z = y + 1$ via $y < z$. Thus,

$$\begin{aligned} P &= \gcd(u_y - 1, u_{y+1} - 1) = \gcd(u_{y+1}u_{y-1}, u_y u_{y+2}) \\ &= \gcd(u_{y-1}, u_{y+2}) \leq u_3 < \alpha^{2.2}. \end{aligned}$$

Hence, by the first part of (8), we have

$$\alpha^{\frac{z-1}{2}} < \alpha^{2.2},$$

which leads to the contradiction $z < 5.4$.

Assume now that $\ell = k$. Necessarily we have $k = \ell = 1$. Since $z - i = y - j$, we obtain $z = y + 2$. By Lemma 7,

$$\alpha^{\frac{z-1}{2}} < \sqrt{u_z} < c \leq P = \gcd(u_z - 1, u_{z-2} - 1) < 2(A^2 - 2).$$

Using Lemma 6, we obtain a contradiction again from

$$z < 2\log_\alpha\left(2(A^2 - 2)\right) + 1 < 7.2.$$

In the sequel, we assume $\ell < k$. First we analyze the case when $2 \leq k/\ell$. Here,

$$z = \frac{k}{\ell}(y - j) + i \geq 2(y - 1) - 1 = 2y - 3,$$

which, together with Lemma (10) implies the following three possibilities.

- When $z = 2y - 1$ holds, then we have

$$\alpha^{y-1.17} = \frac{\alpha^{2y-2}}{\alpha^{y-0.83}} < \frac{u_{2y-1}}{u_y} = \frac{bc+1}{ac+1} < \frac{b}{a}.$$

  Subsequently,

$$a^2\alpha^{y-1.17} < ab = u_x - 1 < u_x < \alpha^{x-0.83}$$

  holds according to Remark 5. Thus,

$$a^2 < \alpha^{x-y+0.34} \leq \alpha^{-0.66}$$

  again a contradiction.

- Assume that $z = 2y - 2$. Then, by Lemma 9, it follows that

$$\alpha^{\frac{z-1}{2}} < P = \gcd(u_y - 1, u_{2y-2} - 1) < \alpha^{6.4},$$

  which is not possible since $z \geq 139$.

- If $z = 2y - 3$ then, according to Lemma 8,

$$\alpha^{\frac{z-1}{2}} < P = \gcd(u_y - 1, u_{2y-3} - 1) < \alpha^{5.7}$$

  holds, which is obviously impossible.

Finally assume that $k/\ell < 2$. Note that this condition implies $k \geq 3$. Taking any pair $(i_0, j_0) \neq (i, j)$, we have

$$z - i_0 = \frac{k}{\ell}(y - j) + i - i_0.$$

Now the main goal is to calculate the best upper bound for $P_0 = \gcd(z - i_0, y - j_0)$. Starting with

$$\begin{aligned} P_0 &= \gcd\left(\frac{k}{\ell}(y-j) + i - i_0, y - j_0\right) \\ &\leq \gcd(k(y-j) + \ell(i-i_0), k(y-j_0)) = |k(j_0 - j) + \ell(i - i_0)|, \end{aligned}$$

we need to consider the last expression. The three cases

$$j \neq j_0,\ i \neq i_0, \qquad j \neq j_0,\ i = i_0, \qquad j = j_0,\ i \neq i_0, \tag{9}$$

give $2(k + \ell)$, $2k$, 2ℓ, respectively. Then using the inequality (7), we get

$$\begin{aligned} \alpha^{\frac{z-1}{2}} \leq P &= \gcd(u_y - 1, u_z - 1) < \prod_{i,j \in \{\pm 1\}} u_{\gcd(z-i, y-j)} \\ &\leq \alpha^{\frac{z+1}{k} + 2(k+\ell) + 2k + 2\ell - 4 \cdot 0.83}. \end{aligned}$$

Going through the eligible pairs

$$(k,\ell) = (3,2),\ (4,3),\ (5,3),\ (5,4),\ (6,5),\ (7,4),\ (7,5),\ (7,6), \tag{10}$$

the previous argument provides the upper bounds

$$z < 105.1,\ 101.8,\ 98,\ 111.3,\ 124.1,\ 115.8,\ 127,\ 138.2,$$

respectively. The assertion of the second part of the proof contradicts any of these upper bounds. Thus, the proof of Theorem 2 is complete.

4 The proof of Theorem 3

Apart from the second equation, system (2) turns to a triple if we take $a = 1$. Therefore, we may suppose that $2 \le a < b < c < d$ and with $1 \le x < z < v < y$ they satisfy system (2). Since $2 \times 3 \times 4 + 1 \le abc + 1 = u_x$, then $2 \le x < t < z < y$ hold. We again split the proof into two parts.

Case 3. $y \le 138$.

Repeating the treatment of Lemma 12 we prove the impossibility of the existence of quadruples satisfies (2) with $y \le 138$.

Lemma 13. *System (2) has no solution with $A \ge 3$ and $y \le 138$.*

Proof. Follow the approach of the proof of Lemma 12. Considering the integer

$$a = \sqrt[3]{\frac{(u_x(A)-1)(u_t(A)-1)(u_z(A)-1)}{(u_y(A)-1)^2}},$$

and the polynomial division

$$(u_x(A)-1)(u_t(A)-1)(u_z(A)-1) = q(A)(u_y(A)-1)^2 + r(A),$$

we found $A \le 2$ if $y \le 138$ is assumed.

Case 4. $y > 138$.

The results of Lemma 10 and 11 coincide if we interchange the role of y and z. Since only the two largest variables (y and z) are used in the second part of the proof of Theorem 1, we can make a step by step copy of that to show the remaining part of Theorem 2. The only difference is to consider here cd instead of c:

$$\sqrt{u_y} < cd \le \gcd\left(u_y - 1,\ u_z - 1\right) \le \prod_{i,j\in\{\pm 1\}} u_{\gcd(y-i,z-j)}.$$

Therefore the proof is complete. □

Acknowledgements This paper was written when the first author visited University of West Hungary. He thanks the Institute of Mathematics for the kind hospitality.

References

[1] M. Alp, N. Irmak and L. Szalay, *Balancing Diophantine Triples,* Acta Univ. Sapientiae **4** (2012), 11–19.

[2] R. D. Carmichael, *On the Numeric Factors of the Arithmetic Forms* $\alpha^n \pm \beta^n$*,* The Annals of Mathematics, Second Series **15(1/4)** (1913-1914), 30–48.

[3] A. Dujella, *There are only finitely many Diophantine quintuples,* J. Reine Angew. Math. **566** (2004), 183–214.

[4] C. Fuchs, F. Luca and L. Szalay, *Diophantine triples with values in binary recurrences,* Ann. Scuola Norm. Sup. Pisa. Cl. Sci. III **5** (2008), 579–608.

[5] V. E. Hoggat and G. E. Bergum, *A problem of Fermat and Fibonacci sequence,* Fibonacci Quart. **15** (1977), 323–330.

[6] F. Luca and L. Szalay, *Fibonacci Diophantine Triples,* Glasnik Math. **43(63)** (2008), 253–264.

[7] F. Luca and L. Szalay, *Lucas Diophantine Triples,* INTEGERS **9** (2009), 441–457.

[8] G. K. Panda and S. S. Rout, *A Class of recurrent Sequences Exhibiting Some Exciting Properties of Balancing Numbers,* World Acad. of Sci., Eng. and Tech. **61** (2012), 164–166.

[9] L. Szalay, *Diophantine equations with binary recurrences associated to Brocard-Ramanujan problem,* Portugal. Math. **69** (2012), 213–220.

dc_871_14

László Szalay, Volker Ziegler

On an S-unit variant of Diophantine m-tuples

Publ. Math. Debrecen, 83 (2013), 97-121.

On an S-unit variant of Diophantine m-tuples

László Szalay, Volker Ziegler

Abstract

Let S be a fixed set of primes and let $a_1, \dots, a_m$ be positive distinct integers. We call the m-tuple $(a_1, \dots, a_m)$ S-Diophantine, if for all $i \neq j$ the integers $a_i a_j + 1 = s_{i,j}$ are S-integers. In this paper we show that if $|S| = 2$, then under some technical restrictions no S-Diophantine quadruple exists.

1 Introduction

An m-tuple $(a_1, \dots, a_m)$ of positive distinct integers is called Diophantine if

$$a_i a_j + 1 = \square \tag{1}$$

for $i \neq j$. Diophantine m-tuples have been studied since ancient times by several authors. Most notable is Dujella's result [5] that no Diophantine six-tuple exists and that there are only finitely many quintuples. It is widely believed that there exist no quintuples at all.

Not only Diophantine m-tuples have been considered, but also various variants. For instance, Bugeaud and Dujella [1] examined m-tuples, where $\square$ in (1) is replaced by k-th power, Dujella and Fuchs [6] investigated a polynomial version, and Fuchs, Luca and Szalay [8] replaced $\square$ by terms of given binary recurrence sequences. For a complete overview we suggest Dujella's web page on Diophantine tuples [4].

In this paper we mean to consider an S-unit version of Diophantine m-tuples. Let S be a fixed set of primes. Then we call an m-tuple $(a_1, \dots, a_m)$, with positive integers $0 < a_1 < \cdots < a_m$ an S-Diophantine m-tuple, if for all $1 \leq i < j \leq n$ we have $a_i a_j + 1 = s_{i,j}$ to be an S-unit. A closely related problem was studied by Győry, Sárközy and Tijdeman [9], who considered the largest prime factor of the products

$$\prod_{a \in A, b \in B} (ab + 1),$$

where A and B are fixed sets. This problem goes back to Erdős and Turán [7], who considered the number of prime factors in the product

$$\prod_{a \in A, b \in B} (a + b).$$

In particular, Győry, Sárközy and Tijdeman conjectured that for positive integers $a < b < c$ the number of prime factor of

$$(ab+1)(ac+1)(bc+1)$$

tends to infinity as $c \to \infty$. This conjecture has been proved by Corvaja and Zannier [3], which means in our context that there exist only finitely many S-Diophantine triples for a fixed set of primes S. Since they used Schmidt's subspace theorem (see e.g. [13][Theorem 1E, p. 178]), this result is ineffective. On the other hand Stewart and Tijdeman [14] proved an effective result, i.e. they showed that for a fixed set of primes there are only finitely many S-Diophantine quadruples which are effectively computable.

In this paper we consider the following problem. Fix the size of S, but not S itself. Does there exist an integer m such that no Diophantine m-tuple exists? In the case of $|S| = 2$ we conjecture that one can choose $m = 4$. Unfortunately, we were able to proof this conjecture only under some technical restrictions. Using the notation $\mathrm{ord}_p(q)$ for the multiplicative order of q modulo p, the main theorem in this paper is the following.

Theorem 1. *Let $S = \{p, q\}$ be a set of two primes with $p < q$ and assume that $p^2 \nmid q^{\mathrm{ord}_p(q)} - 1$, $q^2 \nmid p^{\mathrm{ord}_q(p)} - 1$, further that $q < p^\xi$ holds with some $\xi > 1$. Then there exists a constant $C = C(\xi)$ such that for all such $p, q > C$ no S-Diophantine quadruple exists. In particular we can choose*

$$C = C(\xi) = \Psi(9; 2.142 \cdot 10^{22}\xi^3),$$

where $\Psi(k; x)$ denotes the largest solution $y > 0$ to the equation $x = \frac{y}{(\log y)^k}$.

Remark 1. In case of $\xi = 2$ we obtain $C = C(2) = 1.023 \cdot 10^{41}$.

Let p be a large prime. Then there exists some $b \in \mathbb{Z}$, $1 < b < p$ such that $q = b + p$ is also prime. Put $g = \mathrm{ord}_p(q)$ and $g' = \mathrm{ord}_q(p)$. Then we have

$$q^g \equiv b^g + gpb^{g-1} \mod p^2 \quad \text{and} \quad p^{g'} \equiv \pm\left(b^{g'} - g'qb^{g'-1}\right) \mod q^2.$$

Let us assume that $q^g \equiv 1 \mod p^2$ or $p^{g'} \equiv 1 \mod q^2$, then we replace q by $q' = ap + b$ and obtain

$$q'^g \equiv b^g + gapb^{g-1} \mod p^2 \quad \text{and} \quad p^{g'} \equiv \pm(b^{g'} - g'aqb^{g'-1}) \mod q^2.$$

Since $b^g \equiv 1 + Ap \mod p^2$ for some A or $b^{g'} \equiv 1 + Bq \mod q^2$ and $p \nmid g$ with $q \nmid g'$ we deduce that if q' satisfies the assumptions of Theorem 1 then we have $a \not\equiv s_1 \mod p$ and $a \not\equiv s_2 \mod q$ for some s_1, s_2. Hence, $a \equiv r \mod pq$ for some $r \in (\mathbb{Z}_{pq})^*$. For technical reasons we also exclude the case $a \equiv 1 \mod q$ and we therefore assume that $(p-1)(q-2)$ possiblities for choosing a are left. I.e. a pair of primes (p, q') with

$$q' = b + ap = b + (r + kpq)p = b + rp + kp^2q$$

satisfies the assumptions of Theorem 1. Furthermore $b+pr$ and p^2q are coprime provided $r \not\equiv 1 \mod q$ and we may apply Dirichlet's prime number theorem. We have

$$\begin{aligned}&\sharp\left\{q' \in \mathbb{P} \,:\, (p,q') \in \mathbb{P}^2,\, p^2 \nmid q^{\mathrm{ord}_p(q)}-1,\, q^2 \nmid p^{\mathrm{ord}_q(p)}-1,\, q' \le x\right\}\\ \gg &\frac{x}{\log x}\frac{(p-1)(q-2)}{\phi(p^2q)} \gg \frac{x}{p\log x}\end{aligned}$$

primes $q' < x$ such that the pair (p, q') satisfies the assumptions of Theorem 1. Now, we choose $x = p^{1+\delta}$ for some $\delta > 0$ and we deduce that there exists a prime $q' < p^{1+\delta}$ such that the assumptions of Theorem 1 are fulfilled provided p is large. In particular, we obtain

Corollary 1. *There are infinitely many pairs p, q such that no non-trivial S-Diophantine quadruples exist.*

As mentioned above we conjecture that even more is true:

Conjecture 1. *There exist at most finitely many (respectively no) pairs of primes (p, q) such that $\{p, q\}$-Diophantine quadruples exist.*

2 Plan of the paper

In the next section we provide some useful lemmas that will be used frequently through the rest of the paper. These lemmas contain divisibility properties for the possible solutions in an explicit version of Stewart's and Tijdeman's result [14]. In our case we only have two primes to consider and we can therefore sharpen their result by using lower bounds for linear forms of logarithms in two variables due to Laurent, Mignotte and Nesterenko [11]. Moreover, we show that, assuming (a, b, c, d) is a Diophantine S-tuple, it yields three S-unit equations. In two subsequent sections we will consider two of these S-unit equations and will obtain restrictions for the exponents appearing in the S-units according to the assumptions of Theorem 1. These restrictions are in many cases contradictory and only finally 3 cases remain to handle. In the last section we consider the third S-unit equation and show that its possible solutions are not consistent with the restrictions found in the other sections.

3 Preliminaries

At the beginning of this section we introduce and fix the following notations and assumptions for the rest of the paper. Let $(a, b, c, d) \in \mathbb{Z}^4$ be an S-Diophantine quadruple

with $S = \{p, q\}$ and $p < q$. We assume $0 < a < b < c < d$ and write

$$\begin{aligned} ab + 1 &= s_1, & ac + 1 &= s_2, \\ ad + 1 &= s_3, & bc + 1 &= s_4, \\ bd + 1 &= s_5, & cd + 1 &= s_6, \end{aligned}$$

where $s_i = p^{\alpha_i} q^{\beta_i}$ are S-units for $i = 1, \ldots, 6$. Moreover, we note that

$$\begin{aligned} abcd =& s_2 s_5 - ac - bd - 1 = s_2 s_5 - s_2 - s_5 + 1 \\ =& s_3 s_4 - ad - bc - 1 = s_3 s_4 - s_3 - s_4 + 1 \end{aligned}$$

and therefore we obtain the unit equation

$$s_2 s_5 - s_3 s_4 = s_2 + s_5 - s_3 - s_4. \tag{2}$$

Similarly we also get the unit equations

$$s_1 s_6 - s_3 s_4 = s_1 + s_6 - s_3 - s_4 \qquad \text{and} \tag{3}$$

$$s_2 s_5 - s_1 s_6 = s_2 + s_5 - s_1 - s_6. \tag{4}$$

The solution of these unit equations, under some conditions, plays a crucial role in the proof. Since our proof heavily depends on computing p-adic and q-adic valuations, therefore the following lemma provides a useful tool.

Lemma 1. *Let p and q be odd primes and assume that $q^c \| p^{\mathrm{ord}_q(p)} - 1$ and $q^z | p^x - 1$. Then $x \geq \mathrm{ord}_q(p) q^{z-c}$, moreover if $q^c \| p^{\mathrm{ord}_q(p)} - 1$ and $q^z | p^x + 1$ then $x \geq \frac{\mathrm{ord}_q(p)}{2} q^{z-c}$.*

Proof. The lemma is elementary and some related versions can be found in [2, Section 2.1.4]. For completeness we give a sketch of the proof.

First, note that by the assumption above we have

$$p^{\mathrm{ord}_q(p)} \equiv 1 + aq^c \mod q^{c+1}$$

holds for some a relatively prime to q. Now let us assume $p^x \equiv 1 + aq^m \mod q^{m+2}$ with $q \nmid a$ and $m \geq c \geq 1$. Taking the q-th power we obtain

$$p^{xq} \equiv 1 + aq^{m+1} + q^{2m+1} B \equiv 1 + aq^{m+1} \mod q^{m+2},$$

since $m \geq 1$. Clearly, B denotes some appropriate integer. Similarly, we see that $q^{m+1} \nmid p^{xk} - 1$ follows if $q \nmid k$. Now, by induction, the first statement of the lemma is obvious.

Note that the smallest positive solution to $p^z \equiv -1 \mod p^c$ is at least $\frac{\mathrm{ord}_q(p)}{2}$. Therefore $p^{\mathrm{ord}_q(p)/2} \equiv -1 + aq^c \mod q^{c+1}$ holds for some a. Indeed, squaring both sides, it shows that $q^c \| p^{\mathrm{ord}_q(p)} - 1$. Now the proof runs along similar lines as in the case above. □

Next we consider the case when the S-units on the right side fulfill some divisibility properties.

Lemma 2. *Assume that $\{a, b, c\}$ is an S-Diophantine triple with $a < b < c$. If $ac+1 = s$ and $bc + 1 = t$ then $s \nmid t$.*

Proof. Let us assume $s|t$. Then

$$\mathbb{Z} \ni m = \frac{bc+1}{ac+1} = \frac{b}{a} + \frac{a-b}{a^2c+a} = \frac{b}{a} + \frac{\theta}{a^2}$$

with $|\theta| < 1$. Therefore m is an integer if and only if $\theta = 0$. Thus $a = b$ leads to a contradiction. □

Remark 2. Note that the lemma above shows that for $|S| = 1$ there does not exist an S-Diophantine triple.

We can immediately see that $s_2 \nmid s_4$, $s_3 \nmid s_5$, $s_5 \nmid s_6$ and $s_3 \nmid s_6$, in particular none of the equations $\alpha_2 = \alpha_4$, $\alpha_3 = \alpha_5$, $\alpha_5 = \alpha_6$, $\alpha_3 = \alpha_6$, $\beta_2 = \beta_4$, $\beta_3 = \beta_5$, $\beta_5 = \beta_6$ and $\beta_3 = \beta_6$ hold.

Lemma 3. *We have*

$$\begin{aligned}
a| \gcd &\left(\frac{s_2 - s_1}{\gcd(s_2, s_1)}, \frac{s_3 - s_1}{\gcd(s_3, s_1)}, \frac{s_3 - s_2}{\gcd(s_3, s_2)} \right), \\
b| \gcd &\left(\frac{s_4 - s_1}{\gcd(s_4, s_1)}, \frac{s_5 - s_1}{\gcd(s_5, s_1)}, \frac{s_5 - s_4}{\gcd(s_5, s_4)} \right), \\
c| \gcd &\left(\frac{s_4 - s_2}{\gcd(s_4, s_2)}, \frac{s_6 - s_2}{\gcd(s_6, s_2)}, \frac{s_6 - s_4}{\gcd(s_6, s_4)} \right), \\
d| \gcd &\left(\frac{s_5 - s_3}{\gcd(s_5, s_3)}, \frac{s_6 - s_3}{\gcd(s_6, s_3)}, \frac{s_6 - s_5}{\gcd(s_6, s_5)} \right).
\end{aligned}$$

Proof. We prove only the divisibility property for a since the other cases run completely analogously. First note that $a|a(c-b) = s_2 - s_1$. Since $\gcd(a, s_1) = 1$ and $\gcd(a, s_2) = 1$ we deduce $a|\frac{s_2-s_1}{\gcd(s_2,s_1)}$. Similarly we get the other relations $a|\frac{s_3-s_1}{\gcd(s_3,s_1)}$ and $a|\frac{s_3-s_2}{\gcd(s_3,s_2)}$, hence the proof of the lemma is complete. □

The next lemma is a useful consequence of Lemma 3.

Lemma 4. *If $\gcd(s_4, s_2) \gcd(s_4, s_1) \geq s_4$ then no S-Diophantine quadruple exists.*

Proof. Assume $(a, b, c, d) \in \mathbb{Z}^4$ is an S-Diophantine quadruple. By the lemma above we have $b \leq \frac{s_4}{\gcd(s_4,s_1)} - 1$ and $c \leq \frac{s_4}{\gcd(s_4,s_2)} - 1$. It yields

$$s_4 = bc + 1 < \frac{s_4^2}{\gcd(s_4, s_1) \gcd(s_4, s_2)}.$$

□

Now we prove a lemma which is very helpful in the last two sections of the paper, after collecting enough information on the exponents α_i and β_i, $i = 1, 2 \ldots, 6$.

Lemma 5. *Let the notations be as above and assume that $q > p \geq 5$. Put $\delta = \max\{0, \alpha_4 - \alpha_1 - \alpha_2\}$ and $\epsilon = \max\{0, \beta_4 - \beta_1 - \beta_2\}$. Then we have*

$$p^\delta q^\epsilon a^2 = p^{\alpha_1+\alpha_2+\delta-\alpha_4} q^{\beta_1+\beta_2+\epsilon-\beta_4} - r,$$

with $0 < r < 2p^\delta q^\epsilon$ and $r \in \mathbb{Z}$. If we additionally assume that

$$p^{\alpha_4-\alpha_2} q^{\beta_4-\beta_2} > p^\delta q^\epsilon \quad \text{or} \quad \delta = \epsilon = 0$$

then

$$p^{\alpha_4} q^{\beta_4} - 2p^{\alpha_1+\alpha_2+2\delta-\alpha_4} q^{\beta_1+\beta_2+2\epsilon-\beta_4} < p^{\alpha_2+\delta} q^{\beta_2+\epsilon} < p^{\alpha_4} q^{\beta_4}.$$

The essential part in the proof of the Lemma is the computation of a good approximation of the quantity a^2. To quantify our approximations we will use the so called L-notation (cf. [10]). This allows us to keep track of how large the constants of the usual O-terms get. The L-notation is defined as follows. For two functions $g(t)$ and $h(|t|)$ we write $g(t) = L(h(|t|))$ if $|g(t)| \leq h(|t|)$. In view of applications the estimate

$$\frac{1}{x-1} = \frac{1}{x} + L\left(\frac{1.25}{x^2}\right) = \frac{1}{x} + \frac{1}{x^2} + L\left(\frac{1.25}{x^3}\right)$$

for $|x| \geq 5$ becomes useful. We obtain it by a formal Laurent expansion of $\frac{1}{x-1}$ at infinity.

Proof of Lemma 5. We compute

$$\begin{aligned} a^2 =& \frac{(s_1-1)(s_2-1)}{s_4-1} \\ &= \frac{s_1 s_2}{s_4} - \frac{s_1+s_2}{s_4} + \frac{1}{s_4} + \frac{s_1 s_2}{s_4^2} + L\left(1.25\frac{s_1+s_2+1+s_1 s_2/s_4}{s_4^2}\right) \end{aligned}$$

and therefore we obtain

$$\begin{aligned} p^\delta q^\epsilon a^2 = & p^{\alpha_1+\alpha_2+\delta-\alpha_4} q^{\beta_1+\beta_2+\epsilon-\beta_4} - p^{\alpha_1+\delta-\alpha_4} q^{\beta_1+\epsilon-\beta_4} - p^{\alpha_2+\delta-\alpha_4} q^{\beta_2+\epsilon-\beta_4} \\ & + p^{\delta-\alpha_4} q^{\epsilon-\beta_4} + p^{\alpha_1+\alpha_2+\delta-2\alpha_4} q^{\beta_1+\beta_2+\epsilon-2\beta_4} + L\left(\frac{3.93}{p^{2\alpha_4-\alpha_2-\delta} q^{2\beta_4-\beta_2-\epsilon}}\right). \end{aligned} \tag{5}$$

It implies

$$p^\delta q^\epsilon a^2 = p^{\alpha_1+\alpha_2+\delta-\alpha_4} q^{\beta_1+\beta_2+\epsilon-\beta_4} - r$$

with $0 < r < 2p^\delta q^\epsilon$ and $r \in \mathbb{Z}$. Note that the Diophantine problems

$$\frac{s_1+s_2}{s_4} + \frac{3.93 s_2}{s_4^2} - \frac{1}{s_4} - \frac{s_1 s_2}{s_4^2} > 2, \qquad s_1 \geq 5, s_4 \geq 35$$

and

$$\frac{s_1+s_2}{s_4}-\frac{3.93s_2}{s_4^2}-\frac{1}{s_4}-\frac{s_1s_2}{s_4^2}<0, \qquad s_1\geq 5, s_4\geq 35$$

have no integer solutions. On the other hand, if $r\geq 1$ we deduce that

$$1<p^{\alpha_1+\delta-\alpha_4}q^{\beta_1+\epsilon-\beta_4}+p^{\alpha_2+\delta-\alpha_4}q^{\beta_2+\epsilon-\beta_4}$$

since $1/s_4+s_1s_2/s_4^2>3.93s_2/s_4^2$. In the case of $\delta=\epsilon=0$ we obtain

$$1-p^{\alpha_1-\alpha_4}q^{\beta_1-\beta_4}<p^{\alpha_2-\alpha_4}q^{\beta_2-\beta_4}<1$$

and

$$1-p^{\alpha_1+\delta-\alpha_4}q^{\beta_1+\epsilon-\beta_4}<p^{\alpha_2+\delta-\alpha_4}q^{\beta_2+\epsilon-\beta_4}<p^{\alpha_2+\delta-\delta-\alpha_2}q^{\beta_2+\epsilon-\epsilon-\beta_2}=1$$

otherwise. Some simple computations yield now the second part of the lemma. □

Next, we mean to find appropriate lower bounds for b and c. When $ac+1$ and $bc+1$ are perfect powers of p we may apply Lemma 2. Therefore q divides either $ac+1$ or $bc+1$, and we have $(c-1)c+1\geq bc+1\geq q$. Hence $c>\sqrt{q}$. Knowing that $p\leq ab+1<b^2$ we derive $b>\sqrt{p}$ and therefore we established

Lemma 6. *We have $b>\sqrt{p}$ and $c>\sqrt{q}$.*

The rest of this section is devoted to bring the result due to Stewart and Tijdeman [14] in a more accurate form according to our intentions. In particular, we need suitable upper bounds for d.

Lemma 7. *Let $S=\{p,q\}$, and suppose that (a,b,c,d) is an S-Diophantine quadruple with $a<b<c<d$. Assuming that $10^{10}<p<q$ we have*

$$\frac{\log d}{(\log\log d)^4}<7.969\cdot 10^{21}(\log p\log q)^3.$$

Proof. In order to keep the constants as small as possible we use the theorems on linear forms of logarithms due to Matveev [12] and Laurent, Mignotte and Nesterenko [11]. First recall Matveev's result.

Theorem 2 (Matveev 2000)**.** *Denote by $\alpha_1,\ldots,\alpha_n$ algebraic numbers, nor 0 neither 1, by $\log\alpha_1,\ldots,\log\alpha_n$ determinations of their logarithms, by D the degree over $\mathbb{Q}$ of the number field $K=\mathbb{Q}(\alpha_1,\ldots,\alpha_n)$, and by $b_1,\ldots,b_n$ rational integers. Furthermore let $\kappa=1$ if K is real and $\kappa=2$ otherwise. Choose*

$$A_i\geq\max\{Dh(\alpha_i),|\log\alpha_i|\}\quad(1\leq i\leq n),$$

where $h(\alpha)$ denotes the absolute logarithmic Weil height of α and

$$B=\max\{1,\max\{|b_j|A_j/A_n:1\leq j\leq n\}\}.$$

Assume that $b_n \neq 0$ *and* $\log \alpha_1, \ldots, \log \alpha_n$ *are linearly independent over* $\mathbb{Z}$. *Then*

$$\log |b_1 \log \alpha_1 + \cdots + b_n \log \alpha_n| \geq -C(n) C_0 W_0 D^2 \Omega,$$

with

$$\Omega = A_1 \cdots A_n,$$
$$C(n) = C(n, \kappa) = \frac{16}{n! \kappa} e^n (2n + 1 + 2\kappa)(n+2)(4(n+1))^{n+1} \left(\frac{1}{2} en\right)^{\kappa},$$
$$C_0 = \log\left(e^{4.4n+7} n^{5.5} D^2 \log(eD)\right), \quad W_0 = \log(1.5 eBD \log(eD)).$$

In the case of linear forms in two logarithms we can use a sharper bound due to Laurent et. al. [11]:

Theorem 3 (Laurent, Mignotte, Nesternko 1995)**.** *Let* α_1 *and* α_2 *be two positive, real, multiplicatively independent elements in a number field of degree* D *over* $\mathbb{Q}$. *For* $i = 1, 2$, *let* $\log \alpha_i$ *be any determination of the logarithm of* α_i, *and let* $A_i > 1$ *be a real number satisfying*

$$\log A_i \geq \max\{h(\alpha_i), |\log \alpha_i|/D, 1/D\}.$$

Further, let b_1 *and* b_2 *be two positive integers. Define*

$$b' = \frac{b_1}{D \log A_2} + \frac{b_2}{D \log A_1} \quad \textit{and} \quad \log b = \max\left\{\log b' + 0.14, 21/D, \frac{1}{2}\right\}.$$

Then

$$|b_2 \log \alpha_2 - b_1 \log \alpha_1| \geq \exp\left(-24.34 D^4 (\log b)^2 \log A_1 \log A_2\right).$$

We use the same linear forms as in [14] and consider

$$T_1 = \frac{c}{b} \cdot \frac{bd+1}{cd+1} = \frac{c}{b} p^{\alpha_5 - \alpha_6} q^{\beta_5 - \beta_6}.$$

Similarly we find (see also Stewart and Tijdeman [14])

$$\log(T_1) = \log\left(1 + \frac{c-b}{dcb+b}\right) \leq \log\left(1 + \frac{1}{2d}\right) < \frac{1}{d}.$$

On the other hand, Matveev's result (Theorem 2) yields a lower bound. We bring up this lower bound now. First, choose $A_1 = \log p, A_2 = \log q$ and $A_3 = \log c > \frac{\log q}{2}$. Obviously we have $0 \leq \alpha_5, \alpha_6 \leq \frac{\log(d^2-d+1)}{\log p} < \frac{2 \log d}{\log p}$ and $0 \leq \beta_5, \beta_6 \leq \frac{2 \log d}{\log q}$. Therefore we obtain $B < \frac{2 \log d}{\log c}$, hence we have

$$1.690182 \cdot 10^{10} \log c \log p \log q \left(2.1 + \log\left(\frac{\log d}{\log c}\right)\right) > \log d. \tag{6}$$

In the case of

$$T_2 = \frac{(bd+1)(ac+1)}{(cd+1)ab}$$

we compute

$$\log(T_2) = \log\left(1 + \frac{db+ac-ab+1}{abcd+ab}\right) < \log\left(1+\frac{2}{ac}\right) < \frac{4}{c},$$

and therefore by Theorem 2

$$1.690182 \cdot 10^{10} \log(ab) \log p \log q \left(2.8 + \log\left(\frac{\log d}{\log(ab)}\right)\right) > \log c - \log 4 \tag{7}$$

follows.

In case of

$$T_3 = \frac{(ab+1)(cd+1)}{(ac+1)(bd+1)}$$

we find

$$\log(T_3) = \log\left(1 + \frac{(d-a)(c-b)}{abcd+db+ac+1}\right) < \log\left(1+\frac{1}{ab}\right) < \frac{2}{ab}.$$

Assume for a moment that $b' + 0.14 \geq 21$. Thus we may apply Theorem 3. First,

$$b' \leq \frac{8 \log d}{\log p \log q},$$

therefore we have

$$24.34 \log p \log q \left(2.08 + \log\left(\frac{\log d}{\log p \log q}\right)\right)^2 > \log(ab) - \log 2. \tag{8}$$

If we even suppose that p, q are large, say $10^{10} < p < q$, by combining the inequalities (6), (7) and (8), and using the lower bounds for b and c derived in Lemma 6, we obtain

$$7.969 \cdot 10^{21} (\log p \log q)^3 (\log\log d)^4 > \log d. \tag{9}$$

Since the bound $\frac{21}{8} \log p \log q > \log d$ is much sharper than (9), we proved the lemma completely. □

The previous result gives us upper bounds for d. On the other hand, we will find by Lemma 1 lower bounds for d. In particular, the following lemma provides bounds for p under some restrictions.

Lemma 8. *Assume* $\max_{i=1,\ldots,6}\{\alpha_i + \beta_i\} > p$. *Then we deduce* $p < C(\xi)$ *with*

$$C(\xi) = \Psi(9; 2.142 \cdot 10^{22} \xi^3),$$

where $\Psi(k; x)$ *denotes the largest solution* $y > 0$ *to the equation* $x = \frac{y}{(\log y)^k}$.

Proof. Note that $C(\xi)$ is increasing with $\xi \geq 1$ and note that $C(1) = 1.02 \cdot 10^{40}$. Therefore we may assume $p, q > 10^{40}$. By $d^2 > cd + 1 > p^{\max_{i=1,\dots,6}\{\alpha_i+\beta_i\}} > p^p$, Lemma 7 and the conditions of the lemma we get

$$c\xi^3(\log p)^6(\log\log d)^4 > \log d > \frac{1}{2}p\log p,$$

where $c = 8.478 \cdot 10^{21}$. Therefore

$$c\xi^3(\log p)^6 > \frac{\log d}{(\log\log d)^4} > \frac{p\log p}{2(\log\log p + \log p)^4} > \frac{p}{2.687842(\log p)^3},$$

since $\frac{\log x}{(\log\log x)^4}$ is increasing if $x > 5.15 \cdot 10^{23}$. Solving the last inequality for p, it gives the required result. □

The following proposition will be frequently used.

Proposition 1. *Assume that one of the equations* (2), (3) *and* (4) *is written in the form*

$$p^{e_1}q^{f_1} - p^{e_2}q^{f_2} = p^{e_3}q^{f_3} + p^{e_4}q^{f_4} - p^{e_5}q^{f_5} - p^{e_6}q^{f_6},$$

further let e be the difference of the third to least exponent and the least exponent of the e_i, with $i = 1, \dots, 6$, and let f be defined in the obvious similar way. Then we deduce $e, f \leq 1$, provided that $p > C(\xi)$. Moreover, the two least exponents are equal.

Proof. Let us consider, say, unit equation (2). We obtain

$$p^{\alpha_2+\alpha_5}q^{\beta_2+\beta_5} - p^{\alpha_3+\alpha_4}q^{\beta_3+\beta_4} = p^{\alpha_5}q^{\beta_5} + p^{\alpha_2}q^{\beta_2} - p^{\alpha_3}q^{\beta_3} - p^{\alpha_4}q^{\beta_4}.$$

Suppose that all exponents α_i with $i = 2, 3, 4, 5$ are distinct. Computing the p-adic valuations on the left and right hand sides we see that

$$v_p\left(p^{\alpha_5}q^{\beta_5} + p^{\alpha_2}q^{\beta_2} - p^{\alpha_3}q^{\beta_3} - p^{\alpha_4}q^{\beta_4}\right) = \min\{\alpha_i\}.$$

Say, the minimum is α_2. But, in this case we have $\alpha_2 < \alpha_2 + \alpha_5$ and $\alpha_2 < \alpha_3 + \alpha_4$, i.e. the p-adic valuation on the left side does not fit to the p-adic valuation on the right. Therefore in any case the two least exponents are equal. Observe, that all other cases can be deduced by the same method.

Now divide the equation by the least occurring powers of p and q, respectively. Consider (2) and assume $\alpha_2 = \alpha_5$ and $\beta_4 = \beta_3$ are the smallest exponents. Then

$$p^{\alpha_2}q^{\beta_2+\beta_5-\beta_3} - p^{\alpha_3+\alpha_4-\alpha_2}q^{\beta_3} - q^{\beta_2-\beta_3}(q^{\beta_5-\beta_2}+1) = -p^{\min\{\alpha_3,\alpha_4\}-\alpha_2}(p^{|\alpha_3-\alpha_4|}+1)$$

holds. Clearly, in all other cases we obtain similar equations. In particular, in any case we obtain that for some x the quantity $1 \pm p^x$ is divided by q^f. Since x is at most $\max\{\alpha_i + \beta_i\}$, due to Lemma 8 we obtain that $x < p$ or $p < C(\xi)$. Hence Lemma 1 yields $f \leq 1$ for large p. By similar arguments we also deduce $e \leq 1$. □

4 Unit equation (2)

In this section we deal with equation (2), and our main result is to deduce some relations for the exponents appearing in (2). In particular, this section is devoted to the proof of the following proposition.

Proposition 2. *Let $C(\xi)$ be defined as in Lemma 8. If $p > C(\xi)$ then one of the seven cases in Table 1 holds.*

Table 1: List of the possible solutions to equation (2)

Case	α	β
1	$\alpha_2 = \alpha_5 \leq 1$	$\beta_3 = \beta_4 \leq 1$
2	$\alpha_2 = \alpha_5 \leq 1$	$\beta_3 = \beta_4 = \beta_2 - 1$
3	$\alpha_3 = \alpha_4 = \alpha_2 - 1$	$\beta_2 = \beta_5 = \beta_3 - 1$
4	$\alpha_3 = \alpha_4 = \alpha_2 - 1$	$\beta_2 = \beta_5 \leq 1$
5	$\alpha_3 = \alpha_4 \leq 1$	$\beta_2 = \beta_5 = \beta_3 - 1$
6	$\alpha_3 = \alpha_4 \leq 1$	$\beta_2 = \beta_5 = \beta_4 - 1 = 0$
7	$\alpha_3 = \alpha_4 \leq 1$	$\beta_2 = \beta_5 \leq 1$

By Proposition 1 we may assume that $\alpha_i = \alpha_j$ is minimal for some distinct $i, j \in \{2, 3, 4, 5\}$, i.e. we have to consider six cases. If $\alpha_i = \alpha_j$ and $\beta_i = \beta_j$ hold we deduce that either $s_i | s_j$ or $s_j | s_i$. Therefore we can exclude, by Lemma 2 the cases $\alpha_2 = \alpha_4$ and $\alpha_3 = \alpha_5$ and also when $\beta_2 = \beta_4$ and $\beta_3 = \beta_5$. So four subcases remain to consider.

Before we discuss them we write down again equation (2) explicitly:

$$p^{\alpha_2+\alpha_5} q^{\beta_2+\beta_5} - p^{\alpha_3+\alpha_4} q^{\beta_3+\beta_4} = p^{\alpha_2} q^{\beta_2} + p^{\alpha_5} q^{\beta_5} - p^{\alpha_3} q^{\beta_3} - p^{\alpha_4} q^{\beta_4}. \tag{10}$$

4.1 The case when $\alpha_2 = \alpha_5$ is minimal

First, observe that $\beta_2 < \beta_5$ and we also note that $\beta_4 < \beta_2$ otherwise $s_2 | s_4$ would contradict Lemma 2. Since a sole minimum cannot exist we deduce that $\beta_3 = \beta_4$. The third smallest exponent of q in equation (10) is either $2\beta_3$ or β_2. Hence, by Proposition 1 we have $\beta_3 = \beta_4 \leq 1$ or $\beta_3 = \beta_4 = \beta_2 - 1$. Note that $\beta_4 = \beta_2$ would yield a contradiction by $s_2 | s_4$.

The third smallest exponent of p in equation (10) is either $2\alpha_2$, α_3 or α_4. Therefore we have either $\alpha_2 = \alpha_5 \leq 1$, $\alpha_2 = \alpha_5 = \alpha_3 - 1$ or $\alpha_2 = \alpha_5 = \alpha_4 - 1$. Note that only the first case may hold since by assumption $\beta_2 > \beta_3 = \beta_4$, consequently $s_2 > s_3$ or $s_2 > s_4$ fulfills because of $p < q$. Therefore we deduce that one of the first two cases in Table 1 holds.

4.2 The case when $\alpha_2 = \alpha_3$ is minimal

Again $\beta_4 < \beta_2$ since $s_2 \nmid s_4$. Thus we have $\beta_4 = \beta_5 < \beta_2 < \beta_3$. Therefore the third smallest exponent of q in equation (10) is β_2, subsequently $\beta_4 = \beta_5 = \beta_2 - 1$.

Similarly, by considering the exponents of p in equation (10), we obtain that $\alpha_2 = \alpha_3 = \alpha_4 - 1$ because $\alpha_4 < \alpha_5$. But together with the relations of the β's we arrived at the contradiction $s_2 > s_4$.

4.3 The case when $\alpha_4 = \alpha_5$ is minimal

We immediately see that $\beta_2 < \beta_4$ and $\beta_4 < \beta_5$, since otherwise $s_2 | s_4$ and $s_4 > s_5$, respectively. Therefore $\beta_2 = \beta_3$ is minimal. Consider the exponents of q in equation (10) to obtain $\beta := \beta_2 = \beta_3 = \beta_4 - 1$. Since we have $\beta_2 = \beta_3$ we deduce $\alpha_2 < \alpha_3$ and therefore Proposition 1 in view of p-exponents yields $\alpha := \alpha_5 = \alpha_4 = \alpha_2 - 1$.

In the virtue of $c | s_4 - s_2$ Lemma 3 yields $c < q$. On the other hand, we have $s_4 = p^\alpha q^{\beta+1} = bc + 1 < c^2 < q^2$, and therefore $\beta = 0$ and $p^\alpha < q$. Consider now s_1. We have

$$qp > p^{\alpha+1} = s_2 = ac + 1 > ab + 1 = p^{\alpha_1} q^{\beta_1}.$$

Therefore we have either $\beta_1 = 0$ and $b < p^\alpha$ or $ab + 1 = q$.

First suppose $\beta_1 = 0$. Then we have

$$\mathbb{Z} \ni \frac{ps_4}{s_2} = \frac{pb}{a} - \frac{1}{a} \cdot \frac{p(b-a)}{ac+1} = \frac{pb}{a} - \frac{1}{a} \cdot \frac{\overbrace{b-a}^{<1}}{p^\alpha}.$$

Since the left hand side is an integer we deduce that the "braced" quantity is zero, hence $b = a$, which is a contradiction.

In the case of $ab + 1 = q$, by assumption $c < q$ and $ab + 1 = q$ we get

$$\mathbb{Z} \ni \frac{s_4}{s_1} = \frac{c}{a} - \frac{1}{a} \cdot \frac{\overbrace{c-a}^{<1}}{ab+1}.$$

But $c = a$ is again a contradiction.

4.4 The case when $\alpha_3 = \alpha_4$ is minimal

We have $\beta_2 < \beta_3, \beta_4$ since otherwise we would have $s_2 \geq s_3, s_4$. Because no sole minimum exists we deduce $\beta_2 = \beta_5$. Applying Proposition 1 we obtain either $\beta_2 = \beta_5 \leq 1$ or $\beta_2 = \beta_5 = \beta_3 - 1$ or $\beta_2 = \beta_5 = \beta_4 - 1$. Now we may assume $\alpha_2 < \alpha_5$ and again applying Proposition 1, it provides either $\alpha_3 = \alpha_4 = \alpha_2 - 1$ or $\alpha_3 = \alpha_4 \leq 1$. The combination of the relations of the α's and β's yields either cases listed in Table 1 or

the case $\alpha := \alpha_3 = \alpha_4 = \alpha_2 - 1$ and $\beta := \beta_2 = \beta_5 = \beta_4 - 1$ or the case $\alpha_3 = \alpha_4 \leq 1$ and $\beta := \beta_2 = \beta_5 = \beta_4 - 1$.

When $\alpha := \alpha_3 = \alpha_4 = \alpha_2 - 1$ and $\beta := \beta_2 = \beta_5 = \beta_4 - 1$, similarly to the subsection above, it leads to a contradiction. Note that only the relations between s_2 and s_4 have been used there.

Therefore it remains to prove $\beta = \beta_2 = 0$ in the last case. By $c|s_4 - s_2$ and Lemma 3 we have $c < q$ and therefore $q^2 > bc + 1 = s_4$. Hence $\beta_4 \leq 1$. But $\beta_4 = 0$ would lead to a negative β_2, hence $\beta_4 = \beta_2 + 1 = 1$.

5 Unit equation (4)

In this section we consider the unit equation (4) more closely, in particular we prove the following proposition.

Proposition 3. *Let $C(\xi)$ be defined as in Lemma 8. If $p > C(\xi)$ then one of the three cases in Table 2 holds.*

Table 2: List of the possible solutions to the system of equations (2) and (4)

Case	α	β
I	$\alpha_3 = \alpha_4 \leq 1$; $\alpha_1 = \alpha_6 \leq 1$	$\beta_2 = \beta_5 \leq 1$
II	$\alpha_2 = \alpha_5 \leq 1$	$\beta_3 = \beta_4 \leq 1$; $\beta_1 = \beta_6 \leq 1$
III	$\alpha_2 = \alpha_5 \leq 1$	$\beta_3 = \beta_4 = \beta_2 - 1$; $\beta_1 = \beta_6 \leq 1$

Since none of the α's take a sole minimum in Proposition 1, and $\alpha_5 = \alpha_6$ induces $s_5|s_6$ (a contradiction to Lemma 2) we are left to five subcases. Note that equation (4) takes the form

$$p^{\alpha_2+\alpha_5}q^{\beta_2+\beta_5} - p^{\alpha_1+\alpha_6}q^{\beta_1+\beta_6} = p^{\alpha_2}q^{\beta_2} + p^{\alpha_5}q^{\beta_5} - p^{\alpha_1}q^{\beta_1} - p^{\alpha_6}q^{\beta_6}. \tag{11}$$

5.1 The case when $\alpha_1 = \alpha_2$ is minimal.

Since $\beta_5 = \beta_6$ implies $s_5|s_6$ and $\beta_1 < \beta_2$ we are left to the two possibilities $\beta_1 = \beta_5$ and $\beta_1 = \beta_6$.

5.1.1 The subcase when $\beta_1 = \beta_5$ is minimal.

Note that $\alpha_1 = \alpha_2 = \alpha_5$ cannot hold since otherwise $s_1 = s_5$ is a contradiction. Therefore we deduce $\alpha_2 < \alpha_5$, but this yields by Proposition 2 and our $\beta_2 = \beta_5 = \beta_1$, again a contradiction.

5.1.2 The subcase when $\beta_1 = \beta_6$ is minimal.

By the assumptions $\beta_1 = \beta_6 < \beta_5$ we deduce $\alpha_5 < \alpha_6$. Hence Proposition 1 yields $\alpha_1 = \alpha_2 = \alpha_5$ or $\alpha_1 = \alpha_2 = \alpha_5 - 1$ for the exponents of p. Since $\alpha_5 \leq \alpha_2 + 1$ we deduce $\beta_2 \leq \beta_5$ and Proposition 1 yields in view of exponents of q that either $\beta_1 = \beta_6 \leq 1$ or $\beta_1 = \beta_6 = \beta_2 - 1$.

Let us assume $\alpha_1 = \alpha_2 = \alpha_5$ and $\beta_1 = \beta_6 \leq 1$. Then only the first two cases of Table 1 hold, i.e. these are cases II and III of Table 2.

Now let us assume $\alpha_1 = \alpha_2 = \alpha_5$ and $1 < \beta_1 = \beta_6 = \beta_2 - 1$. Again only the first two cases of Table 1 hold. In the first case we have $\alpha_3 > \alpha_6$ since $s_3 \nmid s_6$ and obviously $\beta_3 < \beta_6$ and we also have $\alpha_6 > \alpha_5 = \alpha_2$ since otherwise $s_5 | s_6$. Note that $\alpha_3 > \alpha_6$ since otherwise we have a contradiction by $s_3 | s_6$. Therefore Lemma 3 in view of the pairs (s_6, s_3) and (s_6, s_2) yields $d | p^{\beta_6 - \beta_3} - p^{\alpha_3 - \alpha_6}$ thus $d < q^{\beta_6}$, and $c | p^{\alpha_6 - \alpha_2} - q$ thus $c < p^{\alpha_6}$. Therefore $p^{\alpha_6} q^{\beta_6} = cd + 1 < p^{\alpha_6} q^{\beta_6}$ shows a contradiction. In the second case we obtain $\beta_1 = \beta_6 = \beta_2 - 1 = \beta_3 = \beta_4$, hence $s_3 | s_6$ again is a contradiction.

Assume now that $\alpha_1 = \alpha_2 = \alpha_5 - 1$. Since $\alpha_2 \neq \alpha_5$, we may exclude the first two cases of Table 1.

Next we consider the cases 3 and 4 in Table 1 and we may assume $\alpha := \alpha_3 = \alpha_4 = \alpha_1 - 1 = \alpha_2 - 1 = \alpha_5 - 2$. Since $\beta_2 = \beta_5$ we have

$$s_2 = p^{\alpha+1} q^{\beta_2} < p^{\alpha} q^{\beta_3}, p^{\alpha} q^{\beta_4} < p^{\alpha+2} q^{\beta_2} = s_5,$$

and therefore we may suppose $\beta := \beta_2 = \beta_5 = \beta_3 - 1 = \beta_4 - 1$ and $\beta_1 < \beta$. Now Lemma 3 yields in view of the pair (s_3, s_5) that $d | p^2 - q$ and therefore $p^{\alpha+2} q^{\beta} = bd + 1 < p^4$ which is impossible unless $\alpha = 0$, $\beta = 1$ and $\beta_1 = 0$. But the later assumption leads to $ab + 1 = p$, hence $b < p$ and $p^2 q = bd + 1 < p^3$ mean again a contradiction.

Now let us assume that either case 5 or case 6 of Table 1 holds. Write $\alpha := \alpha_1 = \alpha_2 = \alpha_5 - 1$. Since $\alpha_3 = \alpha_4 \leq 1$ and $s_2 < s_3, s_4 < s_5 = p s_2$ we deduce $\beta_3 = \beta_4$. Therefore we have $\beta_1 < \beta_2 = \beta_5 = \beta_3 - 1 = \beta_4 - 1 =: \beta$ and Lemma 3 in view of the pairs (s_4, s_2) and (s_5, s_3) yields $b < c < q$ and $d < p^{\alpha+1-\alpha_4}$. Hence $bd + 1 < q p^{\alpha+1}$ which yields a contradiction unless $\beta = 0$. But $\beta = 0$ yields $\beta_1 < 0$.

We turn now to the case $\alpha := \alpha_1 = \alpha_2 = \alpha_5 - 1$, $\alpha' := \alpha_3 = \alpha_4 \leq 1$, $\beta_1 = \beta_6 = 0$ and $\beta_2 = \beta_5 = 1$ which corresponds to case 7 of Table 1. Since $p^{\alpha} q = s_2 < s_3, s_4 < p^{\alpha+1} q$ and $\alpha_3 = \alpha_4$ we deduce that $\beta_3 = \beta_4 =: \beta$. Next, in view of the pairs $(s_2, s_1), (s_5, s_1), (s_4, s_2)$ and (s_6, s_5) and Lemma 3 we obtain

$$a < q, \quad b < pq, \quad c < q^{\beta - 1}, \quad d \leq p^{\alpha_6 - \alpha - 1} - q.$$

Therefore $pq^{\beta} > bc + 1 = p^{\alpha'} q^{\beta}$, which can only hold if $\alpha' = 0$. We reconsider now the unit equation (11) and solve it for p^{α_6}. We get

$$p^{\alpha_6} = \left(1 - \frac{1}{p^{\alpha}}\right)^{-1} \left(p^{\alpha+1} q^2 - q(p+1) + 1\right) = p^{\alpha+1} q^2 + L(2pq^2). \tag{12}$$

Together with the estimations above, (12) implies

$$d \le q^2 + \frac{2q^2}{p^\alpha} - q.$$

Furthermore, we have

$$q^\beta = bc + 1 < d^2 \le q^4 \left(1 + \frac{4}{p^\alpha} + \frac{4}{p^{2\alpha}}\right) - 2q^3 \left(1 + \frac{2}{p^\alpha}\right) + q^2 + 1 < q^5, \qquad (13)$$

i.e. $\beta \le 4$. Since $s_2 > s_1$ and $s_2 \nmid s_4$ we deduce $\beta \ge 2$. In case of $\beta = 2$ we have $c < q$, i.e. $q^2 = bc + 1 < q^2$ is a contradiction. Therefore we consider the case $\beta = 4$ next. Note that we have $\frac{1}{p^\alpha} < \frac{p}{q^3}$ since $s_3 < s_5$. Using this estimate in (13), it yields

$$q^4 = bc + 1 < d^2 < q^4 + 4pq + \frac{4p^2}{q^2} - 2q^3 + q^2 + 1 < q^4.$$

Therefore we can restrict ourselves to the case $\beta = 3$. Since $s_3 < s_5$ we deduce $\frac{1}{p^\alpha} < \frac{p}{q^2}$ and by the estimations for d we obtain

$$d \le q^2 + 2p - q \le q^2,$$

provided $q \ge 2p$. Recall that $a < q$, hence $q^3 = ad + 1 < q^3$ leads to a contradiction. Consequently, we may assume $q < 2p$. In this case we have

$$q^3 = bc + 1 > ac + 1 > \frac{q^{\alpha+1}}{2^\alpha}$$

which is again a contradiction unless $\alpha \le 2$. Obviously, $\alpha = 0$ is impossible. Thus we consider the case $\alpha = 1$, which provides a contradiction by $q^3 = bc + 1 < bd + 1 = p^2 q$. So only $\alpha = 2$ remains to investigate. Recall (12) to obtain

$$p^{\alpha_6} = p^3 q^2 + L(2pq).$$

It gives $\alpha_6 = 5$. Note that we assume that $p < q < 2p$ and p is large. Hence by the estimate $d < p^{\alpha_6 - \alpha - 1} = p^2$ we have $p^5 = cd + 1 < p^4$. This is a contradiction.

5.2 The case when $\alpha_1 = \alpha_5$ is minimal.

Since the case $\alpha_1 = \alpha_2$ has already treated, we may suppose $\alpha_1 = \alpha_5 < \alpha_2$. But by Proposition 2 we obtain $\beta_2 = \beta_5$, hence $s_2 > s_5$ which is an obvious contradiction.

5.3 The case when $\alpha_1 = \alpha_6$ is minimal.

Note that $\beta_1 < \beta_6$, therefore we distinguish three subcases: $\beta_2 = \beta_5$, $\beta_1 = \beta_5$ and $\beta_1 = \beta_2$.

5.3.1 The subcase when $\beta_2 = \beta_5$ is minimal.

Here $\beta_1 < \beta_6$ and $\alpha_2 < \alpha_5$. Applying Proposition 1, we obtain either $\beta_2 = \beta_5 \leq 1$ or $\beta_2 = \beta_5 = \beta_1$ or $\beta_2 = \beta_5 = \beta_1 - 1$. Meanwhile, for the $\alpha' s$ we have either $\alpha_1 = \alpha_6 \leq 1$ or $\alpha_1 = \alpha_6 = \alpha_2 - 1$. Note that the case $\alpha_1 = \alpha_2$ has already been treated above.

Let us consider the case $\beta' := \beta_2 = \beta_5 \leq 1$ and $\alpha' := \alpha_1 = \alpha_6 \leq 1$ first. By Proposition 2, we deduce that either case I holds or we have $\alpha := \alpha_3 = \alpha_4 = \alpha_2 - 1$. First, let us assume that $\beta_4 \leq \beta_1 + \beta'$. Applying Lemma 4 we see immediately that no solution exists in this case.

Therefore we may suppose $\beta_4 \geq \beta_1 + \beta' + 1$. Now Lemma 5 yields

$$a^2 = p^{1+\alpha'} q^{\beta_1 + \beta' - \beta_4} - r$$

with $0 < r < 2$, where r is not necessarily an integer. By $a \geq 1$ we deduce $\beta_4 = \beta_1 + \beta' + 1$, i.e. $a^2 = \frac{p^{1+\alpha'}}{q} - r$, hence $\alpha' = 1$. In order to apply the inequality stated in Lemma 5, we have to show that

$$p^{\alpha_2 + \delta} q^{\beta_2 + \epsilon} < p^{\alpha_4} q^{\beta_4},$$

which is in our case equivalent to

$$p^{\alpha+1} q^{1+\beta'} < p^{\alpha} q^{\beta_1 + \beta' + 1}.$$

This is true unless $\beta_1 = 0$. Now Lemma 5 gives

$$p^{\alpha} q^{\beta_1 + \beta' + 1} - 2p^2 q < p^{\alpha+1} q^{1+\beta'} < p^{\alpha} q^{\beta_1 + \beta' + 1}$$

or

$$q^{\beta_1} - 2\frac{1}{p^{\alpha-2} q^{\beta'}} < p < q^{\beta_1}. \tag{14}$$

Unless $\beta' = 0$ and $\alpha \leq 1$ or $\beta' = 1$ and $\alpha = 0$ we have $q^{\beta_1} - 2 < p < q^{\beta_1}$ which is a contradiction to p is an odd prime. But $\alpha = 1$ leads to $\alpha_3 = \alpha_6$ and $\alpha = 0$ leads to $s_1 > s_2$, since we assume $\beta_1 > 0$.

If $\beta_1 = 0$ then, by the assumption $\beta_1 \geq \beta_2 = \beta'$ we deduce $\beta' = 0$ and therefore $\beta_4 = 1$. Since $c < q$ (apply Lemma 3 to the pair (s_2, s_4)) and $b < s_1 = p$ (note that $\alpha_1 = \alpha_6 \leq 1$) we have $bc + 1 < pq$, i.e. $\alpha = 0$. But $\alpha = 0$ entails $s_2 = s_1 = p$, and this is a contradiction.

Now, let us consider the case $\beta_2 = \beta_5 \leq 1$ and $\alpha_1 = \alpha_6 = \alpha_2 - 1$. We note that the cases 3 and 4 in Proposition 2 cannot hold since we would obtain $\alpha_1 = \alpha_6 = \alpha_2 - 1 = \alpha_3 = \alpha_4$ and then $s_3 | s_6$ is a contradiction. Therefore we may assume $\alpha_3 = \alpha_4 \leq 1$. Since $s_2 > s_1$ we deduce that $\beta_1 \leq \beta_2$ and therefore also $\beta_1 < \beta_3, \beta_4$. Considering the unit equation (3), we obtain $\beta_1 = \beta_6$ since a sole minimum cannot exist. So $s_1 = s_6$ is a contradiction.

Now we treat the case $\beta_2 = \beta_5 = \beta_1$. Proposition 2 shows us that $\beta_2 = \beta_5 < \beta_4$ and in view of our actual case $\beta_1 < \beta_4$ holds. Hence, by (3) we deduce that either $\beta_1 = \beta_6$ or $\beta_1 = \beta_3$, which yields either $s_5|s_6$ or $s_3|s_5$.

The next case is $\beta_2 = \beta_5 = \beta_1 - 1$. First note that $\alpha_1 = \alpha_6 = \alpha_2 - 1$ cannot hold since $s_1 > s_2$ would mean a contradiction. Therefore we may assume that $\alpha_1 = \alpha_6 \leq 1$. Since the case $\beta_2 = \beta_5 \leq 1$ has already been treated, we deduce from Proposition 2 that $\beta_2 = \beta_5 = \beta_1 - 1 = \beta_3 - 1$ and either $\alpha_3 = \alpha_4 \leq 1$ or $\alpha_3 = \alpha_4 = \alpha_2 - 1$.

When $\beta = \beta_2 = \beta_5 = \beta_1 - 1 = \beta_3 - 1$, $\alpha_1 = \alpha_6 = 0$ and $\alpha_3 = \alpha_4 = 1$, by $a|s_3 - s_1$ and Lemma 3 we have $a < p$ and since $ab + 1 = q^{\beta+1}$ we deduce on the one hand $b < q^{\beta+1}$ and on the other hand $b > \frac{q^{\beta+1}}{p} > q^{\beta}$. Moreover, we have $s_2 < s_3$ and so $p^{\alpha_2 - 1} < q$ and $ac + 1 < pq^{\beta+1}$, i.e. $c < pq^{\beta+1}$. The bounds for b and c yield $pq^{\beta_4} = bc + 1 < pq^{2\beta+2}$, i.e. $\beta_4 \leq 2\beta + 1$. Now we consider the pairs (s_4, s_1) and (s_4, s_2) in view of Lemma 3. From the first pair we obtain $b|pq^{\beta_4 - \beta - 1} - 1$, hence $\beta_4 = 2\beta + 1$ because $b > q^{\beta}$. Then the second pair yields $c|q^{\beta+1} - p^{\alpha_2 - 1}$, i.e. $c \leq q^{\beta+1}$. Moreover since $s_4 = ad + 1 = pq^{\beta+1}$ and $d < pq^{\beta+1}$ we get $q^{\beta_6} = cd + 1 < pq^{2\beta+2}$ which results in $\beta_6 = 2\beta + 2$. Now the pair (s_6, s_4) yields a new bound for c, namely $c < q$ and together with $a < p$ we have $q^{\beta+1} = ab + 1 < ac + 1 < pq$ and therefore $\beta = 0$. Now we consider the pair (s_3, s_6) and obtain $d|q - p$. Thus $q^2 = cd + 1 < q^2$ is a contradiction finally.

Only the case $\beta = \beta_2 = \beta_5 = \beta_1 - 1 = \beta_3 - 1$, $\alpha' = \alpha_1 = \alpha_6 \leq 1$ and $\alpha = \alpha_3 = \alpha_4 = \alpha_2 - 1$ is still open. Note that $\alpha > \alpha'$. We know that

$$\mathbb{Z} \ni \frac{p(bc+1)}{ac+1} = \frac{pb}{a} - \frac{1}{a} \cdot \overbrace{\frac{p(b-a)}{ac+1}}^{\theta}.$$

If $|\theta| < 1$ we obtain a similar contradictory argument as in Lemma 2. Therefore $c > b > p^{\alpha}q^{\beta}$ follows. From the inequlity $p^{\alpha}q^{\beta} < b < s_1 < s_2$ we get $p^{\alpha - \alpha'} < q < p^{\alpha+1-\alpha'}$. Using this inequality in $c < ac + 1 = p^{\alpha+1}q^{\beta}$ we get $c < q^{\beta+1}p^{\alpha'+1}$ and $d < q^{\beta+2}p^{\alpha'}$. Thus

$$p^{\alpha'}q^{\beta_6} = cd + 1 < p^{1+2\alpha'}q^{2\beta+3}$$

and $\beta_6 \leq 2\beta + 3 + e$. Using the upper bound $b < ab + 1 = p^{\alpha'}q^{\beta+1}$ we similarly obtain

$$p^{\alpha}q^{\beta_4} = bc + 1 < p^{1+2\alpha'}q^{2\beta+2}$$

hence $\beta_4 \leq 2\beta + 2 + e$. We apply Lemma 3 to the pair (s_4, s_1) and obtain

$$p^{\alpha}q^{\beta} < b < p^{\alpha - \alpha'}q^{\beta_4 - \beta - 1} < q^{\beta_4 - \beta}$$

which yields $p^{\alpha'} < q^{\beta_4 - 2\beta - 1}$. Thus $\beta_4 = 2\beta + 2$ if $\alpha' = 0$ and $\beta_4 = 2\beta + 2$ or $\beta_4 = 2\beta + 3$ if $\alpha' = 1$. We consider the pair (s_6, s_4) and obtain an upper bound $c < q$ if $\alpha' = 0$ and $c < q^2$ if $\alpha' = 1$. But

$$p^{1-\alpha'}q^{\beta+1} < p^{\alpha}q^{\beta} < b < c < q^{1+\alpha'}$$

is a contradiction unless $\beta = 0$, $\alpha' = 1$, $\beta_6 = 4$ and $\beta_4 = 2$. Since in any other case we would obtain the sharper bound $c < q$. We remind that $d < q^{\beta+2}p^{\alpha'} = pq^2$, thus $pq^4 = cd + 1 < pq^4$ is a contradiction.

5.3.2 The subcase when $\beta_1 = \beta_5$ is minimal.

Since the case above we have $\beta_2 > \beta_5$ and from Proposition 2 we deduce $\alpha_2 = \alpha_5$. Then $s_2 > s_5$, which is impossible.

5.3.3 The subcase when $\beta_1 = \beta_2$ is minimal.

Now $\alpha_1 = \alpha_6 \leq \alpha_5$ implies $\beta_1 = \beta_2 \leq \beta_5 < \beta_6$, and Proposition 1 yields $\beta := \beta_2 = \beta_1 = \beta_5 - 1$. Note that the case $\beta_2 = \beta_5$ was treated above. Therefore we have $\alpha_2 = \alpha_5 = 1$, $\alpha_1 = \alpha_6 = 0$ and $\beta_3 = \beta_4 < \beta_2 = \beta_1$ by Proposition 2 and our assumptions. Considering $b|s_5 - s_1$, we obtain $b|qp-1$. Similarly, by $a|s_2 - s_1$ we gain $a|p-1$. Thus $ab+1 = q^\beta < p^2q$, hence $\beta \leq 2$. If $\beta = 2$ then we have $b|qp - 1$ and $b|q^2 - 1 = s_1 - 1$, and we obtain $b|q - p$, i.e. $q^2 > b^2 > ab + 1 = q^2$, a contradiction. Therefore we have $\beta = 1$ leading to $q^{\beta_6} = cd + 1 < (ac + 1)(bd + 1) = p^2q^3 < q^5$, i.e $\beta_6 = 3, 4$. Note that $\beta_6 \leq 2$ would yield $s_5 > s_6$. If we suppose $\beta_6 = 3$ we obtain, by $d|s_6 - s_5$ that $d|q - p$ and hence $q^3 = cd + 1 < q^2$ is a contradiction. Similarly, we obtain $d|q^2 - p$ in the case $\beta_6 = 4$, hence $q^4 = cd + 1 < q^4$ is also impossible. Note that $\beta = 0$ yields $\beta_3 < 0$, which is again a contradiction.

5.4 The case when $\alpha_2 = \alpha_5$ is minimal.

By Proposition 2 we have $\alpha_2 = \alpha_5 \leq 1$. Obviously, the relations $\beta_1 < \beta_2 < \beta_5$ hold since otherwise it would lead to $s_1 < s_2 < s_5$. Therefore we conclude $\beta_1 = \beta_6$, and by Proposition 1 $\beta_1 = \beta_6 = \beta_2 - 1$ or $\beta_1 = \beta_6 \leq 1$ follows. The case $\beta_1 = \beta_6 \leq 1$, together with Proposition 2 yields the cases II and III. On the other hand, $\beta_1 = \beta_6 = \beta_2 - 1$, together with the second case of Proposition 2 immediately yields a contradiction. The remaining case $\alpha_2 = \alpha_5 \leq 1$, $\beta_1 = \beta_6 = \beta_2 - 1$ and $\beta_3 = \beta_4 \leq 1$ provides $\beta_3 = \beta_4 < \beta_1 = \beta_6$. But this implies $\alpha_1 < \alpha_6 < \alpha_3$. Therefore we obtain, in view of equation (3) and Proposition 1 that $\alpha_1 = \alpha_4$. Consequently, $\beta_1 < \beta_4$, which contradicts $\beta_3 < \beta_1$.

5.5 The case when $\alpha_2 = \alpha_6$ is minimal.

Because of $s_1 < s_2, s_6$ and $\alpha_1 \geq \alpha_2, \alpha_6$ we gain $\beta_1 < \beta_2, \beta_6$. Therefore we have $\beta_1 = \beta_5 \leq \beta_2 < \beta_6$ and $\alpha_2 = \alpha_6 < \alpha_1 < \alpha_5$. Now, by Proposition 1, $\alpha_2 = \alpha_6 = \alpha_1 - 1$ and $\beta_1 = \beta_5 = \beta_2 - 1$ follow. Note that $\beta_1 = \beta_5 = \beta_2$ would imply the contradiction $s_2 < s_1$. Since $\beta_2 \neq \beta_5$ we deduce $\alpha_2 = \alpha_5$ and therefore in the actual case $\alpha_5 = \alpha_6$ holds. But $s_5|s_6$ is a contradiction again.

6 The unit equation (3)

In this section we concentrate on the equation

$$p^{\alpha_1+\alpha_6}q^{\beta_1+\beta_6} - p^{\alpha_3+\alpha_4}q^{\beta_3+\beta_4} = p^{\alpha_1}q^{\beta_1} + p^{\alpha_6}q^{\beta_6} - p^{\alpha_3}q^{\beta_3} - p^{\alpha_4}q^{\beta_4}. \tag{15}$$

As earlier, we have to distinguish several cases.

6.1 The case when $\alpha_1 = \alpha_3$ is minimal.

Obviously, we have $\beta_1 < \beta_3$, therefore either $\beta_1 = \beta_4$ or $\beta_1 = \beta_6$ or $\beta_4 = \beta_6$ holds. But, both the cases $\beta_1 = \beta_4$ and $\beta_4 = \beta_6$ give case I in Proposition 3 since otherwise $s_3|s_6$. But case I contradicts our assumption $\alpha_1 = \alpha_3$, since othewise $s_3|s_6$ again.

Therefore we may assume $\beta_1 = \beta_6$ and either case II or III holds. Since by assumption $\beta_4 \geq \beta_6$ we deduce that $\alpha_1 = \alpha_3 \leq \alpha_4 \leq \alpha_6$. Therefore Proposition 1 results in $\alpha_1 = \alpha_3 = \alpha_4 - 1$ or $\alpha_1 = \alpha_3 = \alpha_4$.

First suppose that case II holds. Then we have $\beta_1 = \beta_6 = 0$ and $\beta_3 = \beta_4 = 1$. Put $\alpha = \alpha_1 = \alpha_3$, $\alpha' = \alpha_2 = \alpha_5 \leq 1$ and $\alpha_4 = \alpha + h$ with $h \in \{0, 1\}$, and assume $h = 0$. Then, in the virtue of Lemma 4 there does no solution exist. Note that we may apply Lemma 4 only if $\beta_2 > 0$, but $\beta_2 = 0$ means $s_2 \leq p \leq s_1$. Similarly, we may also exclude the case $h = 1$ and $\alpha' = 1$. Hence we are reduced to the possibility $h = 1$ and $\alpha' = 0$. According to Lemma 5, we obtain

$$pa^2 = q^{\beta_2 - 1} - r$$

with $0 < r < 2p$. On the other hand, $a|s_3 - s_1$ implies $a|q - 1$ (Lemma 3), hence $pq^2 > pa^2 + 2p > q^{\beta_2-1}$. Since $\beta_2 > 1$ we deduce $\beta_2 = 2, 3$. Applying the second part of Lemma 5, after canceling common factors, we get

$$p^{\alpha+1} - 2pq^{\beta_2-2} < q^{\beta_2-1} < p^{\alpha+1}.$$

Note that $p^\delta q^\epsilon = p = \frac{s_4}{s_3} > \frac{s_4}{s_2}$. In case of $\beta_2 = 2$ we see from $c|s_4 - s_2$ that $c|p^{\alpha+1} - q$ (Lemma 3), and from the inequality above that $c \leq p^{\alpha+1} - q < 2p$. Therefore $p^{\alpha+1}q = bc + 1 < 4p^2$, subsequently $\alpha = 0$ and $\alpha_3 = \alpha_5$ and $s_3|s_5$.

Suppose now that $\beta_2 = 3$ and $p^{\alpha+1} - 2pq < q^2 < p^{\alpha+1}$. Evaluating

$$bd + 1 = \frac{(s_3 - 1)(s_4 - 1)}{s_2 - 1} = \frac{(p^{\alpha+1}q - 1)(p^\alpha q - 1)}{q^3 - 1} + 1 = \frac{p^{2\alpha+1}}{q} + L\left(\frac{2p^{\alpha+1}}{q^2}\right) =$$
$$\frac{p^{2\alpha+1}}{q} + L\left(2\frac{q^2}{q^2} + 4\frac{p}{q}\right) = \frac{p^{2\alpha+1}}{q} + L(6) < \frac{(q^2 + 2pq)^2}{pq} + 6 < q^3,$$

it leads to a contradiction by $\beta_2 = \beta_5 < 3$.

Now let us consider case III. Here we write $\beta' = \beta_1 = \beta_6 \leq 1$, $\beta = \beta_3 = \beta_4 = \beta_2 - 1$, $\alpha = \alpha_1 = \alpha_3$, $\alpha_4 = \alpha + h$ with $h \in \{0, 1\}$ and $\alpha' = \alpha_2 = \alpha_5 \leq 1$. Unless $h = 1$ and $\alpha' = \beta' = 0$ we can apply Lemma 4. Since $p^\delta q^\epsilon = p = \frac{s_4}{s_3} < \frac{s_4}{s_2}$ we can use the second part of Lemma 5 in the remaining case, and we obtain

$$p^{\alpha+1} - \frac{2p}{q^{\beta-1}} < q < p^{\alpha+1}.$$

But it contradicts the assumption q is odd unless $\beta = \beta_3 = \beta_4 \leq 1$. But this case has been treated above.

6.2 The case when $\alpha_1 = \alpha_4$ is minimal.

Observe, that only the cases II and III may hold under this assumption. By $\beta_1 < \beta_4$ we have $\beta_1 = \beta_3$ or $\beta_1 = \beta_6$. But the first equality is not possible in the cases II and III. Therefore we may assume $\beta_1 = \beta_6$. Since $\alpha_6 < \alpha_3$ would imply $s_3 > s_6$, we have $\alpha_1 = \alpha_4 \leq \alpha_3 < \alpha_6$, and now Proposition 1 yields $\alpha_1 = \alpha_4 = \alpha_3 - 1$. Note that $\alpha_1 = \alpha_3$ has already been investigated above.

In case II we write $\alpha = \alpha_1 = \alpha_4 = \alpha_3 - 1$ and $\alpha' = \alpha_2 = \alpha_5 \leq 1$ and we have $\beta_1 = \beta_6 = 0$ and $\beta_3 = \beta_4 = 1$. Therefore Lemma 4 settles this case.

Case III is analogous. Let $\alpha = \alpha_1 = \alpha_4 = \alpha_3 - 1$ and $\alpha' = \alpha_2 = \alpha_5 \leq 1$. Moreover, we have $\beta' = \beta_1 = \beta_6 \leq 1$ and $\beta = \beta_3 = \beta_4 = \beta_2 - 1$. We apply Lemma 4 again.

6.3 The case when $\alpha_1 = \alpha_6$ is minimal.

Obviously, only case I may hold. Therefore we have $\alpha_1 = \alpha_6 = 0$, $\alpha_3 = \alpha_4 = 1$ and $\beta' = \beta_2 = \beta_5 \leq 1$. Moreover, $\beta_3 < \beta_1$ or $\beta_4 < \beta_1$ would yield $s_3 < s_1$ or $s_4 < s_1$, and we obtain either $\beta_1 = \beta_3$ or $\beta_1 = \beta_4$. In case of $\beta_1 = \beta_4$, the application of Lemma 4 gives a contradiction. Therefore Proposition 1 implies $\beta := \beta_1 = \beta_3 = \beta_4 - 1$. Considering now $d | s_6 - s_3$ and $c | s_6 - s_4$, we obtain (by Lemma 3) $d < q^{\beta_6 - \beta}$ and $c < q^{\beta_6 - \beta - 1}$. Thus $q^{2\beta_6 - 2\beta - 1} > cd + 1 > q^{\beta_6}$, i.e. $\beta_6 > 2\beta + 1$. On the other hand, $ad + 1 = pq^\beta$ and therefore $c, d < pq^\beta$ and $q^{\beta_6} = cd + 1 < p^2 q^{2\beta} < q^{2\beta+2}$ follow, which contradicts the bound for β_6 found before.

6.4 The case when $\alpha_3 = \alpha_4$ is minimal.

From $\alpha = \alpha_3 = \alpha_4 \leq \alpha_1, \alpha_6$ we deduce that $\beta_1 < \beta_3, \beta_4$ hence $\beta' = \beta_1 = \beta_6 < \beta_3, \beta_4$. Note that only the cases II and III may hold, hence $\beta = \beta_3 = \beta_4$, $\beta' \leq 1$ and $\alpha' = \alpha_2 = \alpha_5 \leq 1$. We may exclude the case $\beta_2 < \beta_4$ since otherwise case II would be fulfilled, and $\beta_1 = \beta_6 = \beta_2 = 0$ and $\alpha_1 < \alpha_2 \leq 1$ would yield a contradiction by $ab + 1 = 1$. Therefore we suppose $\beta_4 \leq \beta_2$ and apply Lemma 4.

6.5 The case when $\alpha_4 = \alpha_6$ is minimal.

Clearly, under this assumption only the cases II and III may hold. Thus $\alpha_4 = \alpha_6 \leq \alpha_1$, and we obtain $\beta_1 < \beta_4, \beta_6$, hence $\beta_1 = \beta_3$ in the virtue of Proposition 1. But, this contradicts $\beta_1 = \beta_6$, since wwe obtain $s_3|s_6$.

References

[1] Y. Bugeaud and A. Dujella. On a problem of Diophantus for higher powers. *Math. Proc. Cambridge Philos. Soc.*, 135(1):1–10, 2003.

[2] H. Cohen. *Number theory. Vol. I. Tools and Diophantine equations*, volume 239 of *Graduate Texts in Mathematics*. Springer, New York, 2007.

[3] P. Corvaja and U. Zannier. On the greatest prime factor of $(ab+1)(ac+1)$. *Proc. Amer. Math. Soc.*, 131(6):1705–1709 (electronic), 2003.

[4] A. Dujella. Diophantine m-tuples.
available at http://web.math.hr/ duje/dtuples.html

[5] A. Dujella. There are only finitely many Diophantine quintuples. *J. Reine Angew. Math.*, 566:183–214, 2004.

[6] A. Dujella and C. Fuchs. Complete solution of the polynomial version of a problem of Diophantus. *J. Number Theory*, 106(2):326–344, 2004.

[7] P. Erdos and P. Turan. On a Problem in the Elementary Theory of Numbers. *Amer. Math. Monthly*, 41(10):608–611, 1934.

[8] C. Fuchs, F. Luca, and L. Szalay. Diophantine triples with values in binary recurrences. *Ann. Sc. Norm. Super. Pisa Cl. Sci. (5)*, 7(4):579–608, 2008.

[9] K. Győry, A. Sárközy, and C. L. Stewart. On the number of prime factors of integers of the form $ab + 1$. *Acta Arith.*, 74(4):365–385, 1996.

[10] C. Heuberger, A. Pethő, and R. F. Tichy. Thomas' family of Thue equations over imaginary quadratic fields. *J. Symbolic Comput.*, 34(5):437–449, 2002.

[11] M. Laurent, M. Mignotte, and Y. Nesterenko. Formes linéaires en deux logarithmes et déterminants d'interpolation. *J. Number Theory*, 55(2):285–321, 1995.

[12] E. M. Matveev. An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic numbers. II. *Izv. Ross. Akad. Nauk Ser. Mat.*, 64(6):125–180, 2000.

[13] W. M. Schmidt. *Diophantine approximations and Diophantine equations*, volume 1467 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1991.

[14] C. L. Stewart and R. Tijdeman. On the greatest prime factor of $(ab + 1)(ac + 1)(bc + 1)$. *Acta Arith.*, 79(1):93–101, 1997.

dc_871_14

László Szalay, Volker Ziegler

S-Diophantine quadruples with two primes congruent to 3 modulo 4

Integers, 13 (2013), Article A80.

S-Diophantine quadruples with two primes congruent to 3 modulo 4

László Szalay, Volker Ziegler

Abstract

Let S be a fixed set of primes and let $a_1, \dots, a_m$ denote positive distinct integers. We call the m-tuple $(a_1, \dots, a_m)$ S-Diophantine if the integers $a_i a_j + 1 = s_{i,j}$ are S-units for all $i \neq j$. In this paper, we show that if $S = \{p, q\}$ and $p, q \equiv 3 \pmod 4$ then no S-Diophantine quadruple exists.

1 Introduction

It is an old problem to find m-tuples $(a_1, \dots, a_m)$ of positive distinct integers such that

$$a_i a_j + 1 = \square \tag{1.1}$$

for $i \neq j$. Such m-tuples are called Diophantine and have been studied since ancient times by several authors. Most notable is Dujella's result [3] that no Diophantine sixtuple exists and that there are only finitely many quintuples. Even more is believed to be true. A folklore conjecture states that there exist no quintuples at all.

Beside Diophantine m-tuples various variants have also been considered. For instance, Bugeaud and Dujella [1] examined m-tuples, where $\square$ in (1.1) is replaced by a k-th power, and Dujella and Fuchs [4] investigated a polynomial version. Later Fuchs, Luca and the first author [5, 6] replaced $\square$ by terms of a given binary recurrence sequence (cf. [5]) and in particular, the Fibonacci sequence (cf. [6]). Recently the authors subsituted $\square$ by S-units [7]. For a complete overview we suggest Dujella's web page on Diophantine tuples [2].

In this paper, we continue our research on S-Diophantine m-tuples. Let S be a fixed set of primes. Then we call the m-tuple $(a_1, \dots, a_m)$ with positive and pairwise distinct integers a_i $(1 \leq i \leq m)$ an S-Diophantine m-tuple, if we have $a_i a_j + 1 = s_{i,j}$ being an S-unit for all $1 \leq i < j \leq n$.

In a recent paper [7] the authors showed that if $S = \{p, q\}$ and $C(\xi) < p < q < p^{\xi}$ hold for some $\xi > 1$ and some explicitly computable constant $C(\xi)$, then no S-Diophantine quadruple exists. This result and numerical experiments (see [7, Lemma 9], where we found no quadruples with $1 \leq a < b < c < d \leq 1000$) raise the question of whether S-Diophantine quadruples with $|S| = 2$ exist at all. We conjecture the following

Conjecture 1.1. *There exist no pairs of primes (p, q) such that $\{p, q\}$-Diophantine quadruples exist.*

Unfortunately, we can prove only the following weaker statement which admits the main result of this paper.

Theorem 1.2. *Let $S = \{p, q\}$ with primes $p, q \equiv 3 \pmod 4$. Then no S-Diophantine quadruple exists.*

The proof of Theorem 1.2 is organized as follows. In the next section we prove two auxiliary results which enable us to prove Theorem 1.2 partially in Section 3. The remaining difficulties are resolved in the last section of the paper. Here we note that Lemma 2.2 is the only place where we used the assertion that p and$q$ are congruent to 3 modulo 4, so the technique we applied later may be useful in the proof of the conjecture.

2 Auxiliary results

We start with a very useful lemma (see [7, Lemma 2]) which excludes some divisibility relations for S-Diophantine triples.

Lemma 2.1. *Assume that (a, b, c) is an S-Diophantine triple with $a < b < c$. If $ac + 1 = s$ and $bc + 1 = t$, then $s \nmid t$.*

This lemma is exactly Lemma 2 in [7]. The proof is short and, since we intend to keep this paper independent and self-contained, we repeat the proof here.

Proof. Assume that $s \mid t$. Then

$$m = \frac{bc+1}{ac+1} = \frac{b}{a} + \frac{a-b}{a^2c+a} = \frac{b}{a} + \frac{\theta}{a^2} \in \mathbb{Z}$$

hold with $|\theta| < 1$. Therefore m is integer if and only if $\theta = 0$. Thus $a = b$ leads to a contradiction. □

Now we deduce a few restrictions on the exponents appearing in the prime factorization of the S-units $s_{i,j}$.

Lemma 2.2. *Let $S = \{p, q\}$ with $p, q \equiv 3 \pmod 4$ and let (a, b, c) be an S-Diophantine triple. Further assume that*

$$ab + 1 = p^{\alpha_1} q^{\beta_1}, \qquad ac + 1 = p^{\alpha_2} q^{\beta_2}, \qquad bc + 1 = p^{\alpha_3} q^{\beta_3}.$$

Then at least one of $\alpha_1, \alpha_2, \alpha_3$ is zero and at least one of $\beta_1, \beta_2, \beta_3$ is zero.

Proof. Using the notation of the lemma we have

$$(abc)^2 = \left(p^{\alpha_1}q^{\beta_1} - 1\right)\left(p^{\alpha_2}q^{\beta_2} - 1\right)\left(p^{\alpha_3}q^{\beta_3} - 1\right).$$

If all α_1, α_2 and α_3 are positive, then $(abc)^2 \equiv -1 \pmod{p}$ and we arrive at a contradiction since the Legendre symbol $(-1/p) = -1$. Similarly, at least one of β_1, β_2 and β_3 must be zero. □

3 Proof of Theorem 1.2

For the rest of the paper we assume that $S = \{p, q\}$ and $p, q \equiv 3 \pmod{4}$.

Suppose now that (a, b, c, d) is an S-Diophantine quadruple. Therefore there exist non-negative integers α_i, β_i, $i = 1, \ldots, 6$ such that

$$\begin{aligned} ab + 1 &= p^{\alpha_1}q^{\beta_1}, & bc + 1 &= p^{\alpha_4}q^{\beta_4}, \\ ac + 1 &= p^{\alpha_2}q^{\beta_2}, & bd + 1 &= p^{\alpha_5}q^{\beta_5}, \\ ad + 1 &= p^{\alpha_3}q^{\beta_3}, & cd + 1 &= p^{\alpha_6}q^{\beta_6}. \end{aligned}$$

Since (a, b, c) is an S-Diophantine triple, according to Lemma 2.2, at least one of α_1, α_2 and α_4 is zero. Let us assume for the moment that all of them are vanished, i.e. $\alpha_1 = \alpha_2 = \alpha_4 = 0$. There is no loss of generality in supposing $a < b < c$. Thus $ac + 1 \mid bc + 1$ and Lemma 2.1 yields a contradiction.

Therefore at least one of α_1, α_2 and α_4 is non-zero, and similarly at least one of β_1, β_2 and β_4 is not vanishing.

Proposition 3.1. *If exactly one of α_1, α_2 and α_4 is zero or exactly one of β_1, β_2 and β_4 is zero then (a, b, c, d) cannot be an S-Diophantine quadruple.*

Proof. By switching p and q if necessary, and by rearranging the quadruple (a, b, c, d) we may assume that $\alpha_1 = 0$ and α_2, α_4 are positive. Notice that (b, c, d) is also an S-Diophantine triple. Then due to Lemma 2.2 one of α_5 and α_6 must be zero. So we distinguish two cases.

First, let $\alpha_5 = 0$. We now show that this implies $\alpha_6 = 0$. Indeed, consider the S-Diophantine triple (a, c, d) and the corresponding equations $ac+1 = p^{\alpha_2}q^{\beta_2}$, $ad+1 = p^{\alpha_3}q^{\beta_3}$ and $cd+1 = p^{\alpha_6}q^{\beta_6}$. By Lemma 2.2, one of α_3 and α_6 vanishes. But $\alpha_3 = 0$ leads to a contradiction because it would provide $ab + 1 = q^{\beta_1}$, $ad + 1 = q^{\beta_3}$ and $bd + 1 = q^{\beta_5}$ which contradicts Lemma 2.1. Hence $\alpha_5 = \alpha_6 = 0$.

Thus the following lemma completes the proof of the proposition.

Lemma 3.2. *There exist no S-Diophantine quadruples (a, b, c, d) with $\alpha_1 = \alpha_6 = 0$.*

The proof of this lemma is long and technical. Therefore we postpone the proof to the forthcoming section. □

In the virtue of Proposition 3.1 at least two of α_1, α_2 and α_4 are zero, and similarly at least two of β_1, β_2 and β_4 are zero. Therefore one pair fulfills $(\alpha_i, \beta_i) = (0, 0)$ with $i \in \{1, 2, 4\}$. But, this is impossible since all of $ab + 1$, $ac + 1$ and $bc + 1$ are at least 3.

Hence, up to the proof of Lemma 3.2 we have proved Theorem 1.2.

4 Proof of Lemma 3.2

In view of the assumptions of Lemma 3.2 we have to study the system

$$\begin{aligned} ab + 1 &= q^{\beta_1}, & bc + 1 &= p^{\alpha_4} q^{\beta_4}, \\ ac + 1 &= p^{\alpha_2} q^{\beta_2}, & bd + 1 &= p^{\alpha_5} q^{\beta_5}, \\ ad + 1 &= p^{\alpha_3} q^{\beta_3}, & cd + 1 &= q^{\beta_6}. \end{aligned}$$

Consider the triple (a, b, c). By Lemma 2.2 we deduce that either $\beta_2 = 0$ or $\beta_4 = 0$, and by switching a and b as well as the corresponding exponents we may assume that $\beta_2 = 0$. Thus we obtain the system

$$\begin{aligned} ab + 1 &= q^{\beta_1}, & bc + 1 &= p^{\alpha_4} q^{\beta_4}, \\ ac + 1 &= p^{\alpha_2}, & bd + 1 &= p^{\alpha_5} q^{\beta_5}, \\ ad + 1 &= p^{\alpha_3} q^{\beta_3}, & cd + 1 &= q^{\beta_6}. \end{aligned}$$

Subsequently, the equation

$$ab \cdot cd = \left(q^{\beta_1} - 1\right)\left(q^{\beta_6} - 1\right) = \left(p^{\alpha_2} - 1\right)\left(p^{\alpha_5} q^{\beta_5} - 1\right) = ac \cdot bd$$

is valid. Assuming $\beta_5 > 0$ we obtain

$$1 \equiv 1 - p^{\alpha_2} \pmod{q}. \tag{4.1}$$

Note that the positivity of a, b, c and d entails that β_1 and β_6 are also positive integers. However, equation (4.1) yields the contradiction $q | p^{\alpha_2}$. Therefore we have $\beta_5 = 0$. Further the system

$$\begin{aligned} ab + 1 &= q^{\beta_1}, & bc + 1 &= p^{\alpha_4} q^{\beta_4}, \\ ac + 1 &= p^{\alpha_2}, & bd + 1 &= p^{\alpha_5}, \\ ad + 1 &= p^{\alpha_3} q^{\beta_3}, & cd + 1 &= q^{\beta_6} \end{aligned}$$

follows. We consider now the equation

$$ac \cdot bd = \left(p^{\alpha_2} - 1\right)\left(p^{\alpha_5} - 1\right) = \left(p^{\alpha_3} q^{\beta_3} - 1\right)\left(p^{\alpha_4} q^{\beta_4} - 1\right) = ad \cdot bc.$$

The expansion of the sides provides

$$p^{\alpha_2+\alpha_5} - p^{\alpha_2} - p^{\alpha_5} = p^{\alpha_3+\alpha_4}q^{\beta_3+\beta_4} - p^{\alpha_3}q^{\beta_3} - p^{\alpha_4}q^{\beta_4}. \tag{4.2}$$

By simultaneously switching a, b and c, d we may assume that $\alpha_5 \geq \alpha_2$. Moreover, the p-adic valuation of the left and right side of (4.2) coincide, hence the least two of $\alpha_2, \alpha_3, \alpha_4$ and α_5 must be equal. In particular, we have the following three cases: $\alpha_2 = \alpha_3 \leq \alpha_4$, $\alpha_2 = \alpha_4 \leq \alpha_3$ and $\alpha_3 = \alpha_4 < \alpha_2$. Note that with $\alpha_2 = \alpha_5$ at least one further exponent is necessarily minimal.

Similarly, we can arrive at the equation

$$q^{\beta_1+\beta_6} - q^{\beta_1} - q^{\beta_6} = p^{\alpha_3+\alpha_4}q^{\beta_3+\beta_4} - p^{\alpha_3}q^{\beta_3} - p^{\alpha_4}q^{\beta_4},$$

where we may assume that $\beta_6 \geq \beta_1$. Thus the least two of $\beta_1, \beta_3, \beta_4$ and β_6 must be coincided. Hence, in total we have 9 possibilities which will be treated subsequently (see Table).

α	β
$\alpha_2 = \alpha_3 \leq \alpha_4$	$\beta_1 = \beta_3 \leq \beta_4$
	$\beta_1 = \beta_4 \leq \beta_3$
	$\beta_3 = \beta_4 < \beta_1$
$\alpha_2 = \alpha_4 \leq \alpha_3$	$\beta_1 = \beta_3 \leq \beta_4$
	$\beta_1 = \beta_4 \leq \beta_3$
	$\beta_3 = \beta_4 < \beta_1$
$\alpha_3 = \alpha_4 < \alpha_2$	$\beta_1 = \beta_3 \leq \beta_4$
	$\beta_1 = \beta_4 \leq \beta_3$
	$\beta_3 = \beta_4 < \beta_1$

List of cases

4.1 The case $\alpha_2 = \alpha_3 \leq \alpha_4$ and $\beta_1 = \beta_3 \leq \beta_4$

Consider the triple (a, b, c) with

$$ab + 1 = q^{\beta_1}, \qquad ac + 1 = p^{\alpha_2}, \qquad bc + 1 = p^{\alpha_4}q^{\beta_4}.$$

The assumption $\beta_1 \leq \beta_4$ implies immediately $ab < bc$, i.e. $a < c$. Similarly, $a < b$ is concluded from $\alpha_2 \leq \alpha_4$. Hence either $ab + 1 \mid bc + 1$ with $a < c < b$ or $ac + 1 \mid bc + 1$ with $a < b < c$ holds. But each case contradicts Lemma 2.1.

4.2 The case $\alpha_2 = \alpha_3 \leq \alpha_4$ and $\beta_1 = \beta_4 \leq \beta_3$

We clone the treatment of the previous case. Consider the triple (a, b, c) and deduce $a < c$ and $a < b$. Then either $ab + 1 \mid bc + 1$ with $a < c < b$ or $ac + 1 \mid bc + 1$ with $a < b < c$ follows and we arrive at a contradiction.

4.3 The case $\alpha_2 = \alpha_3 \leq \alpha_4$ and $\beta_3 = \beta_4 < \beta_1$

For simplicity we omit certain subscripts by writing $\beta := \beta_3 = \beta_4$ and $\alpha := \alpha_2 = \alpha_3$. By comparing $ac+1$ with $bc+1$ and $ad+1$ we obtain $a < b$ and $c < d$, and therefore $\alpha_4 < \alpha_5$. Moreover, by the triple (a, b, c) we have $c < b$, otherwise a contradiction to Lemma 2.1 would occur.

Now consider the equation

$$ad \cdot bc = \left(p^{\alpha}q^{\beta} - 1\right)\left(p^{\alpha_4}q^{\beta} - 1\right) = \left(p^{\alpha} - 1\right)\left(p^{\alpha_5} - 1\right) = ac \cdot bd$$

modulo p^{α_4}. We get

$$p^{\alpha}q^{\beta} - 1 \equiv p^{\alpha} - 1 \pmod{p^{\alpha_4}}$$

and then

$$q^{\beta} \equiv 1 \pmod{p^{\alpha_4 - \alpha}}. \tag{4.3}$$

This yields $p^{\alpha_4-\alpha} \mid q^{\beta} - 1$ i.e. $p^{\alpha_4-\alpha} \leq q^{\beta} - 1$.

At this point we distinguish the two cases $\beta_1 \geq 2\beta$ and $\beta_1 < 2\beta$. Let us start with the first case. Taking

$$ad \cdot bc = \left(p^{\alpha}q^{\beta} - 1\right)\left(p^{\alpha_4}q^{\beta} - 1\right) = \left(q^{\beta_6} - 1\right)\left(q^{\beta_1} - 1\right) = ab \cdot cd$$

modulo $q^{2\beta}$, the relation

$$q^{\beta}\left(p^{\alpha_4} + p^{\alpha}\right) \equiv 0 \pmod{q^{2\beta}}$$

follows. This yields $q^{\beta} \mid p^{\alpha_4-\alpha} + 1$ and therefore $p^{\alpha_4-\alpha} \geq q^{\beta} - 1$. Together with (4.3) we have $p^{\alpha_4-\alpha} = q^{\beta} - 1$, which is impossible because the parity of the two sides is different.

Proceeding to the case $2\beta > \beta_1$, consider again

$$ad \cdot bc = \left(p^{\alpha}q^{\beta} - 1\right)\left(p^{\alpha_4}q^{\beta} - 1\right) = \left(q^{\beta_1} - 1\right)\left(q^{\beta_6} - 1\right) = ab \cdot cd$$

modulo q^{β_1}. We obtain

$$q^{\beta}\left(p^{\alpha_4} + p^{\alpha}\right) \equiv 0 \pmod{q^{\beta_1}}.$$

Thus $q^{\beta_1-\beta} \mid p^{\alpha_4-\alpha} + 1$.

A simple calculation results

$$\frac{b}{a} = \frac{bc}{ac} = \frac{p^{\alpha_4}q^{\beta} - 1}{p^{\alpha} - 1} = p^{\alpha_4-\alpha}q^{\beta} + \frac{p^{\alpha_4-\alpha}q^{\beta} - 1}{p^{\alpha} - 1} > p^{\alpha_4-\alpha}q^{\beta}.$$

If we assume $q^{\beta_1-\beta} \neq p^{\alpha_4-\alpha} + 1$, then $2q^{\beta_1-\beta} \leq p^{\alpha_4-\alpha} + 1$ follows. Consequently, we have

$$\frac{b}{a} > 2q^{\beta_1} - q^{\beta} > \frac{5}{3}q^{\beta_1} > q^{\beta_1} > b,$$

which is a contradiction. Then $q^{\beta_1-\beta} = p^{\alpha_4-\alpha} + 1$ holds, and it contradicts the fact that the parity of $q^{\beta_1-\beta}$ and $p^{\alpha_4-\alpha} + 1$ does not coincide.

4.4 The case $\alpha_2 = \alpha_4 \le \alpha_3$ and $\beta_1 = \beta_3 \le \beta_4$

Similarly to the case 4.1. ($\alpha_2 = \alpha_3 \le \alpha_4$ and $\beta_1 = \beta_3 \le \beta_4$), consider the triple (a, b, c) to find a contradiction to Lemma 2.1.

4.5 The case $\alpha_2 = \alpha_4 \le \alpha_3$ and $\beta_1 = \beta_4 \le \beta_3$

Again the triple (a, b, c) leads to a contradiction.

4.6 The case $\alpha_2 = \alpha_4 \le \alpha_3$ and $\beta_3 = \beta_4 < \beta_1$

Write $\beta := \beta_3 = \beta_4$ and $\alpha := \alpha_2 = \alpha_4$. By comparing $ac + 1$ to $bc + 1$ we obtain $a < b$. Since $p^{\alpha_3}q^\beta - 1 = ad < bd = p^{\alpha_5} - 1$ we have $\alpha_3 \le \alpha_5$. The equations

$$ad \cdot bc = \left(p^{\alpha_3}q^\beta - 1\right)\left(p^\alpha q^\beta - 1\right) = \left(p^\alpha - 1\right)\left(p^{\alpha_5} - 1\right) = ac \cdot bd$$

modulo p^{α_3} admit

$$p^\alpha q^\beta - 1 \equiv p^\alpha - 1 \pmod{p^{\alpha_3}}.$$

Therefore

$$q^\beta \equiv 1 \pmod{p^{\alpha_3-\alpha}},$$

and $p^{\alpha_3-\alpha} \mid q^\beta - 1$ hold. We also have $c \mid c(b-a) = p^\alpha(q^\beta - 1)$. Thus $c \mid q^\beta - 1$ and $c < q^\beta$ follow. Since c and p are coprime (note that $ac + 1 = p^{\alpha_3}$) then $c \mid \frac{q^\beta - 1}{p^{\alpha_3-\alpha}}$ is valid. Clearly, $bc + 1 = p^\alpha q^\beta$ implies $p^\alpha q^\beta \le \frac{q^\beta-1}{p^{\alpha_3-\alpha}}b + 1$ and then

$$b \ge \frac{p^{\alpha_3}q^\beta - p^{\alpha_3-\alpha}}{q^\beta - 1} \ge p^{\alpha_3} - \frac{p^{\alpha_3}}{p^\alpha q^\beta} \ge p^{\alpha_3}\left(1 - \frac{1}{p^\alpha}\right).$$

On the other hand, $b \mid b(a-c) = q^\beta(q^{\beta_1-\beta} - p^\alpha)$ and thus $b \mid q^{\beta_1-\beta} - p^\alpha$. Assuming $b < p^\alpha$, it implies the contradiction $bc + 1 < p^\alpha q^\beta$. Therefore we necessarily obtain $q^{\beta_1-\beta} > p^\alpha$, hence $b \le q^{\beta_1-\beta} - p^\alpha$. But $ab + 1 = q^{\beta_1} \le (q^{\beta_1-\beta} - p^\alpha)a + 1$ also hold and we deduce

$$a \ge \frac{q^{\beta_1} - 1}{q^{\beta_1-\beta} - p^\alpha}.$$

For the moment assume that $d > b$. Then we have

$$\begin{aligned} p^{\alpha_3}q^\beta = ad + 1 > ab &> p^{\alpha_3}\left(1 - \frac{1}{p^\alpha}\right)\frac{q^{\beta_1} - 1}{q^{\beta_1-\beta} - p^\alpha} \\ &= p^{\alpha_3}q^\beta\left(1 - \frac{1}{p^\alpha}\right)\frac{q^{\beta_1} - 1}{q^{\beta_1} - p^\alpha q^\beta} \\ &> p^{\alpha_3}q^\beta. \end{aligned}$$

Indeed,

$$\frac{p^\alpha - 1}{p^\alpha} \cdot \frac{q^{\beta_1} - 1}{q^{\beta_1} - p^\alpha q^\beta} > 1$$

is implied by $p^\alpha + q^{\beta_1} < p^{2\alpha} q^\beta$ which is coming from

$$q^\beta p^{2\alpha} = (ac+1)(bc+1) > ab + 1 + ac + 1 = q^{\beta_1} + p^\alpha.$$

Hence $d < b$. But this, together with $c < a$ leads to

$$cd + 1 = q^{\beta_6} < q^{\beta_1} = ab + 1,$$

which contradicts the assumption $\beta_1 \leq \beta_6$.

4.7 The case $\alpha_3 = \alpha_4 < \alpha_2$ and $\beta_1 = \beta_3 \leq \beta_4$

By switching p and q respectively b and c we arrive at the case $\alpha_2 = \alpha_3 \leq \alpha_4$ and $\beta_3 = \beta_4 < \beta_1$.

4.8 The case $\alpha_3 = \alpha_4 < \alpha_2$ and $\beta_1 = \beta_4 \leq \beta_3$

This possibility is equivalent to the case $\alpha_2 = \alpha_4 \leq \alpha_3$ and $\beta_3 = \beta_4 < \beta_1$ by exchanging p and q respectively b and c.

4.9 The case $\alpha_3 = \alpha_4 < \alpha_2$ and $\beta_3 = \beta_4 < \beta_1$

First suppose $c < a$. By $cd + 1 = q^{\beta_6} \geq q^{\beta_1} = ab + 1$ we deduce $d > b$. Then $ad + 1 = p^\alpha q^\beta = bc + 1$ contradicts $c < a$ and $b < d$.

Assume now that $b < a$. Then $bd + 1 = p^{\alpha_5} \geq p^{\alpha_2} = ac + 1$ and therefore $d > c$ follow. Thus we get again a contradiction to $ad + 1 = p^\alpha q^\beta = bc + 1$.

Therefore $a < b$ and $a < c$. Consequently,

$$b \mid b(c-a) = q^\beta (p^\alpha - q^{\beta_1 - \beta}) \quad \text{and} \quad c \mid c(b-a) = p^\alpha (q^\beta - p^{\alpha_2 - \alpha})$$

hold. Hence $b < q^\beta$ and $c < p^\alpha$ follow, and $p^\alpha q^\beta < bc + 1 = p^\alpha q^\beta$ shows the final contradiction.

References

[1] Y. Bugeaud and A. Dujella. On a problem of Diophantus for higher powers. *Math. Proc. Cambridge Philos. Soc.*, 135(1):1–10, 2003.

[2] A. Dujella. Diophantine m-tuples. On `http://web.math.hr/~duje/dtuples.html`.

[3] A. Dujella. There are only finitely many Diophantine quintuples. *J. Reine Angew. Math.*, 566:183–214, 2004.

[4] A. Dujella and C. Fuchs. Complete solution of the polynomial version of a problem of Diophantus. *J. Number Theory*, 106(2):326–344, 2004.

[5] C. Fuchs, F. Luca, and L. Szalay. Diophantine triples with values in binary recurrences. *Ann. Sc. Norm. Super. Pisa Cl. Sci. (5)*, 7(4):579–608, 2008.

[6] F. Luca and L. Szalay. Fibonacci Diophantine triples. *Glas. Mat. Ser. III*, 43(63)(2):253–264, 2008.

[7] L. Szalay and V. Ziegler. On an S-unit variant of diophantine m-tuples. To appear in Publ. Math. Debrecen.

dc_871_14