Algebrai görbék a diofantikus számelméletben

Habilitációs cikkgyűjtemény

Tengely Szabolcs

A habilitációs értekezés elkészítését a TÁMOP 4.2.1./B-09/1/KONV-2010-0007 számú projekt valamint az OTKA PD75264 pályázat, illetve a Bolyai János Kutatási Ösztöndíj támogatta. A TÁMOP 4.2.1./B-09/1/KONV-2010-0007 számú projekt az Új Magyarország Fejlesztési Terven keresztül az Európai Unió támogatásával, az Európai Regionális Fejlesztési Alap és az Európai Szociális Alap társfinanszírozásával valósult meg.

Tartalomjegyzék

1

Bevezetés

A habilitációs cikkgyűjteményben tíz publikáció szerepel, amelyek közül nyolc Tengely Szabolcs PhD disszertációjának megvédése után született. Ezek a publikációk a következőek: [1],[22],[48],[49],[57],[62], [105] és [106]. Az eredmények tartalmuk szerint négy fejezetben kerülnek bemutatásra. A témakörökről, a kutatott problémák hátteréről, irodalmi beágyazásukról részletesebben a kapcsolódó fejezetekben olvashatunk.

Az első részben bizonyos exponenciális egyenletek vizsgálatával kapcsolatos tételek szerepelnek. Az $Ax^2 + B = Cy^n$ alakú diofantikus egyenletek irodalma meglehetősen gazdag. Különböző végességi állítások igazolása mellett sok esetben lehetővé vált az egyenlet összes megoldásainak meghatározására is. Az alkalmazott módszerek között megtaláljuk az algebrai számelmélet mély eredményeit, a Baker-módszer megfelelő változatainak az alkalmazását és ezen egyenletek esetében igen eredményesen alkalmazhatónak bizonyult Bilu, Hanrot és Voutier egy eredménye Lucas és Lehmer sorozatok primitív osztóival kapcsolatban. Abu Muriefahval, Lucaval és Siksekkel közösen Tengely vizsgálta az $x^2 + C = 2y^p$ egyenletet, ahol C egy $4k + 1$ alakú egész. Tételükben p-re gyakorlatban jól használható korlátot igazoltak, amit több példán keresztül illusztráltak is. Például meghatározták az $x^2 + 17^a = 2y^p$ egyenlet összes (x, y, a, p) megoldását. Lucaval és Togbéval közösen az $x^2 + C = 4y^p$ egyenlet esetében értek el eredményeket. A publikációkban Tengely társszerzői Abu Muriefah, Luca, Siksek és Togbé voltak.

A második részben számtani sorozatok elemeinek szorzatával összefüggésben végzett kutatások kapnak helyet. Az $n(n + d) \dots (n + (k - 1)d) = by^l$ diofantikus egyenlet speciális eseteivel már Euler is foglalkozott, igazolta, hogy nem létezik megoldás, ha $k = 4, l = 2$ és $b = 1$. Később is sokan vizsgálták a különböző eseteket, csak néhány nevet említve, Erdős, Győry, Hajdu, Obláth, Rigge, Saradha, Shorey, Tijdeman ért el több fontos eredményt. A fejezetben bemutatásra kerül Tengely egy eredménye, amelyben kiterjeszti Mukhopadhyay és Shorey egy tételét az $n(n + d)(n + 2d)(n + 3d)(n + 4d) = by^2$ egyenletre

vonatkozóan. Ugyanebben a dolgozatában Tengely megoldotta Hirata-Kohno, Laishram, Shorey és Tijdeman egy tételében szereplő kimaradó eseteket. Az előző probléma egy változatát vizsgálta Laishram, Shorey és Tengely a közös dolgozatukban. A számtani sorozat egymást követő tagjai közül néhányat törlünk a szorzatból és továbbra is olyan sorozatokat keresünk, amelyeknél ez a szorzat közel teljes négyzetszámot eredményez. A publikációkban Tengely társszerzői Hajdu, Laishram, Shorey és Tijdeman voltak.

A harmadik fejezetben a csupa teljes hatványból felépülő számtani sorozatokkal kapcsolatos eredmények találhatóak. A témakör kutatásában számos jól ismert matematikus vett részt. Már Fermat megfogalmazta a sejtést, hogy négy különböző négyzetszám nem alkothat számtani sorozatot, ezt később Euler be is bizonyította. Azonos hatványok esetében Mordell, Dirichlet és Lebesgue igazoltak eredményeket kis kitevőkre, később Dénes kiterjesztette a megoldást magasabb kitevőkre. Végül Darmon és Merel adott általános választ tetszőleges kitevőkre, felhasználva a Fermat-egyenlet esetében sikert jelentő moduláris technikát. Különböző hatványokból álló sorozatokat vizsgált Bruin, Győry, Hajdu és Tengely. Többek között bebizonyították, hogy négyzetszámokból és köbszámokból csak triviálisan lehet számtani sorozatot felépíteni. Később Hajdu és Tengely megmutatta, hogy négyzetszámokból és azonos kitevős teljes hatványokból legfeljebb hat hosszú nem triviális sorozat állítható elő, köbszámokból és azonos kitevős teljes hatványokból pedig legfeljebb négy. A publikációkban Tengely társszerzői Bruin, Győry és Hajdu voltak.

Végül a negyedik rész algebrai görbék egész- és racionális pontjainak meghatározásáról szól. Először Tengely egy háromszögekkel kapcsolat cikkét mutatjuk be, amelyben olyan egész x, y értékeket határozott meg, amelyekre teljesül, hogy ha egy óra kismutatójának hossza x, nagymutatójáé pedig y, akkor a két mutató távolabbi végpontjainak távolsága (i) 2 órakkor és 3 órakkor ((ii) 2 órakkor és 4 órakkor) is egész érték legyen. A második publikáció a fejezetben hiperelliptikus görbék egész pontjainak meghatározásával foglalkozik. A klasszikus témakörben Baker adott felső korlátot a megoldások méretére, ezt az eredményt később többen élesítették, általánosították. A Bugeaudval, Mignotteval, Siksekkel és Stoll-lal közös dolgozatban a Baker-módszer egy változatát felhasználva felső korlátot nyertek a megoldásokra, ez a korlát azonban túl nagy, hogy segítségével leszámolható legyen az összes megoldás. Viszont a Mordell-Weil szitát felhasználva megmutatható, hogy ha van nem ismert megoldás, akkor annak mérete az előző korlát felé esik. Így több esetben az összes megoldás meghatározható, illusztrációként az $y^2 - y = x^5 - x$ egyenletet és az $\binom{y}{2} = \binom{x}{5}$ egyenletet oldották meg a cikkben. A publikációkban Tengely társszerzői Bugeaud, Mignotte, Siksek és Stoll voltak.

2

Exponenciális diofantikus egyenletek vizsgálata

Ebben a fejezetben a [104] dolgozatban szereplő, a [1] cikkben szereplő, Abu Muriefahval, Lucaval és Siksekkel közösen nyert és a [62] publikációban megjelent, Lucaval és Togbével közösen igazolt eredmények kerülnek bemutatásra.

Az irodalomban jelentős számú eredmény található az

$$Ax^2 + B = Cy^n$$

diofantikus egyenlettel kapcsolatban, ahol $A, B, C \in \mathbb{Z}, ABC \neq 0$ és $n > 2, x, y$ ismeretlen egészek. Lebesgue [58] 1850-ben igazolta, hogy a fenti egyenletnek $B = 1$ esetében csak az $x = 0$ választással kaphatunk megoldást. Chao Ko [54] 1965-ben meghatározta a fenti egyenlet összes megoldását a $B = -1$ esetben. J.H.E. Cohn [26] megoldotta az egyenletet a $1 \leq B \leq 100, C = 1$ feltétel mellett, kivéve néhány B értéket. A kimaradó esetek közül Mignotte és De Weger [65] oldott meg néhányat. Bugeaud, Mignotte és Siksek [21] a Baker-módszer és a moduláris-módszer kombinálásával meghatározta a kimaradó esetekben a megoldásokat.

Bilu, Hanrot és Voutier [12] a Lucas és Lehmer számok primitív osztóival kapcsolatos elegáns eredménye egy jól alkalmazható eszköz lett a fenti egyenlet kezeléséhez, azokban az esetekben, amikor $B = p_1^{z_1} \cdots p_s^{z_s}$ és $C = 1, 2, 4$. Néhány eredmény a témakörből: [2], [3], [72], [73], [74], [4], [5], [20], [25], [27], [60], [61], [64], [70], [71], [77].

Tengely a [104] cikkében az

$$x^2 + q^{2m} = 2y^p, \tag{2.1}$$

egyenletet vizsgálta, ahol $x, y \in \mathbb{N}, (x, y) = 1, m \in \mathbb{N}$ és p, q páratlan prímek. A következő végességi állítás igaz az egyenlettel kapcsolatban.

2.1. Tétel. *Az* (2.1) *egyenletnek csak véges sok* (x, y, m, q, p) *megoldása létezik, ahol* $(x, y) = 1, x, y \in \mathbb{N}, m \in \mathbb{N}, p > 3, q$ *páratlan prímek és* y *nem áll elő, mint két egymást követő négyzetszám összege.*

Amikor y előáll két egymást követő négyzetszám összegeként, akkor léteznek nagy megoldások, ahogyan az alábbi példák is mutatják.

y	p	q
5	5	79
5	7	307
5	13	42641
5	29	1811852719
5	97	22993575370363230255945284717663 99
13	7	11003
13	13	13394159
13	101	22480363734265533023633690933103706711211958360218401799 9
25	11	69049993
25	47	37829305586052202725400160492296 7
41	31	40103338450160604152604 41

A tétel bizonyításában felhasználjuk, hogy a Gauss-egészek körében faktorizálva a megoldásokra paraméteres egyenleteket tudunk nyerni:

$$x = \Re((1+i)(u+iv)^p) =: F_p(u,v),$$
$$q^m = \Im((1+i)(u+iv)^p) =: G_p(u,v).$$

Ahol F_p és G_p kétváltozós egész együtthatós homogén polinomok. Valamint igaz a következő oszthatósági tulajdonság:

$$(u - \delta_4 v) \quad | \quad F_p(u,v),$$
$$(u + \delta_4 v) \quad | \quad G_p(u,v),$$

ahol

$$\delta_4 = \begin{cases} 1 \text{ if } p \equiv 1 \pmod 4, \\ -1 \text{ if } p \equiv 3 \pmod 4. \end{cases}$$

Az oszthatósági tulajdonságból a következő egyenletrendszereket kapjuk:

$$\begin{aligned} u + \delta_4 v &= q^k, \\ H_p(u,v) &= q^{m-k}, \end{aligned} \tag{2.2}$$

vagy

$$\begin{aligned} u + \delta_4 v &= -q^k, \\ H_p(u,v) &= -q^{m-k}, \end{aligned}$$

ahol $H_p(u,v) = \frac{G_p(u,v)}{u+\delta_4 v}$. A végességi állítás igazolásához szükség van egy felső korlátra a p kitevő esetében, ezt a Baker-módszer segítségével kapjuk meg. Itt

Mignotte [12, Theorem A.1.3] eredményét alkalmazzuk és a $p \leq 3803$ korlátot nyerjük. Végül a problémát visszavezetjük véges sok Thue-egyenletre:

$$H_p(u, v) = \pm p,$$

és

$$H_p(u, v) = \pm 1$$

alakban. Az ilyen egyenletek esetében Thue [108] igazolta, hogy csak véges sok megoldás létezhet. A cikkben még találhatóak eredmények a rögzített y és a rögzített q esetekkel kapcsolatban is. Így például igazolást nyer a következő tétel.

2.2. Tétel. *Az $x^2 + 3^{2m} = 2y^p$ diofantikus egyenlet összes relatív prím (x, y) megoldása az $m > 0$ és p prím feltételek mellett $(x, y, m, p) = (13, 5, 2, 3), (79, 5, 1, 5)$, vagy $(545, 53, 3, 3)$.*

Az Abu Muriefahval, Lucaval és Siksekkel [1] közösen írt cikkben az $x^2 + C = 2y^n$ vizsgálatával kapcsolatos eredmények találhatóak. Bizonyítást nyer a következő eredmény.

2.3. Tétel. *Legyen C pozitív egész, amelyre $C \equiv 1 \pmod 4$, és $C = cd^2$, ahol c négyzetmentes. Tegyük fel, hogy (x, y) megoldása az*

$$x^2 + C = 2y^p, \qquad x,\ y \in \mathbb{Z}^+, \quad (x, y) = 1, \tag{2.3}$$

egyenletnek, ahol $p \geq 5$ prím. Ekkor a következő lehetőségek vannak

(i) $x = y = C = 1$, *vagy*

(ii) p *osztja a* $\mathbb{Q}(\sqrt{-c})$ *számtest ideálosztály számát, vagy*

(iii) $p = 5$ *és* $(C, x, y) = (9, 79, 5), (125, 19, 3), (125, 183, 7), (2125, 21417, 47)$, *vagy*

(iv) $p \mid (q - (-c|q))$, *ahol q páratlan prím és $q \mid d$ de $q \nmid c$. Itt $(c|q)$ jelöli a Legendre-szimbólumot.*

A fenti tétel segítségével a szerzős meghatározták az $x^2 + C = 2y^n$ egyenlet összes megoldását $C \equiv 1 \pmod 4$, $1 \leq C < 100$ feltételek mellett.

2.4. Tétel. *Az $x^2 + C = 2y^n$ egyenlet relatív prím x, y megoldásai az $n \geq 3$, és $C \equiv 1 \pmod 4$, $1 \leq C < 100$ feltételek mellett a következőek*

$$1^2 + 1 = 2 \cdot 1^n, \quad 79^2 + 9 = 2 \cdot 5^5, \quad 5^2 + 29 = 2 \cdot 3^3,$$
$$117^2 + 29 = 2 \cdot 19^3, \quad 993^2 + 29 = 2 \cdot 79^3, \quad 11^2 + 41 = 2 \cdot 3^4,$$
$$69^2 + 41 = 2 \cdot 7^4, \quad 171^2 + 41 = 2 \cdot 11^4, \quad 1^2 + 53 = 2 \cdot 3^3,$$
$$25^2 + 61 = 2 \cdot 7^3, \quad 51^2 + 61 = 2 \cdot 11^3, \quad 37^2 + 89 = 2 \cdot 9^3.$$

A tétel alkalmazható olyan esetekben is, amikor C prímosztói rögzítettek, ennek illusztrálására a cikkben meghatározták az

$$x^2 + 17^{a_1} = 2y^n,$$
$$x^2 + 5^{a_1}13^{a_2} = 2y^n,$$
$$x^2 + 3^{a_1}11^{a_2} = 2y^n,$$

egyenletek összes megoldását is.

2.5. Tétel. *Az*

$$x^2 + 17^{a_1} = 2y^n, \qquad a_1 \geq 0, \quad \gcd(x, y) = 1, \quad n \geq 3,$$

egyenlet megoldásai a következőek

$$1^2 + 17^0 = 2 \cdot 1^n, \quad 239^2 + 17^0 = 2 \cdot 13^4, \quad 31^2 + 17^2 = 2 \cdot 5^4.$$

Az

$$x^2 + 5^{a_1}13^{a_2} = 2y^n, \qquad a_1, a_2 \geq 0, \quad \gcd(x, y) = 1, \quad n \geq 3,$$

egyenlet összes megoldása:

$$1^2 + 5^0 \cdot 13^0 = 2 \cdot 1^n, \quad 9^2 + 5^0 \cdot 13^2 = 2 \cdot 5^3,$$
$$7^2 + 5^1 \cdot 13^0 = 2 \cdot 3^3, \quad 99^2 + 5^2 \cdot 13^0 = 2 \cdot 17^3,$$
$$19^2 + 5^2 \cdot 13^1 = 2 \cdot 7^3, \quad 79137^2 + 5^2 \cdot 13^3 = 2 \cdot 1463^3,$$
$$253^2 + 5^2 \cdot 13^4 = 2 \cdot 73^3, \quad 188000497^2 + 5^8 \cdot 13^4 = 2 \cdot 260473^3,$$
$$239^2 + 5^0 \cdot 13^0 = 2 \cdot 13^4.$$

Az

$$x^2 + 3^{a_1}11^{a_2} = 2y^n, \qquad a_1, a_2 \geq 0, \quad \gcd(x, y) = 1, \quad n \geq 3,$$

diofantikus egyenlet megoldásai:

$$1^2+3^0\cdot 11^0=2\cdot 1^n,\quad 351^2+3^0\cdot 11^4=2\cdot 41^3,$$
$$13^2+3^4\cdot 11^0=2\cdot 5^3,\quad 5^2+3^4\cdot 11^2=2\cdot 17^3,$$
$$27607^2+3^4\cdot 11^2=2\cdot 725^3,\quad 545^2+3^6\cdot 11^0=2\cdot 53^3,$$
$$679^2+3^6\cdot 11^2=2\cdot 65^3,\quad 1093^2+3^8\cdot 11^4=2\cdot 365^3,$$
$$410639^2+3^{10}\cdot 11^2=2\cdot 4385^3,\quad 239^2+3^0\cdot 11^0=2\cdot 13^4,$$
$$79^2+3^2\cdot 11^0=2\cdot 5^5.$$

A Lucaval és Togbével közös [62] publikációban az $x^2+C=4y^n$ diofantikus egyenlettel kapcsolatos eredmények kaptak helyet.

2.6. Tétel. *Az*

$$x^2+C=4y^n,\ \ x,y\geq 1,\ \ (x,y)=1,\ \ n\geq 3,\ \ C\equiv 3 \mod 4,\ \ 1\leq C\leq 100 \tag{2.4}$$

diofantikus egyenlet (C,n,x,y) *megoldásait a következő táblázat tartalmazza*

$(3,n,1,1)$	$(3,3,37,7)$	$(7,3,5,2)$	$(7,5,11,2)$
$(7,13,181,2)$	$(11,5,31,3)$	$(15,4,7,2)$	$(19,7,559,5)$
$(23,3,3,2)$	$(23,3,29,6)$	$(23,3,45,8)$	$(23,3,83,12)$
$(23,3,7251,236)$	$(23,9,45,2)$	$(31,3,1,2)$	$(31,3,15,4)$
$(31,3,63,10)$	$(31,3,3313,140)$	$(31,6,15,2)$	$(35,4,17,3)$
$(39,4,5,2)$	$(47,5,9,2)$	$(55,4,3,2)$	$(59,3,7,3)$
$(59,3,21,5)$	$(59,3,525,41)$	$(59,3,28735,591)$	$(63,4,1,2)$
$(63,4,31,4)$	$(63,8,31,2)$	$(71,3,235,24)$	$(71,7,21,2)$
$(79,3,265,26)$	$(79,5,7,2)$	$(83,3,5,3)$	$(83,3,3785,153)$
$(87,3,13,4)$	$(87,3,1651,88)$	$(87,6,13,2)$	$(99,4,49,5)$

2.1. táblázat. Az $x^2+C=4y^n$ egyenlet megoldásai, ahol $1\leq C\leq 100$

Továbbá megoldották a $C=7^a\cdot 11^b, 7^a\cdot 13^b$, esetekben is az adódó diofantikus egyenleteket.

2.7. Tétel. • *Az*

$$x^2+7^a\cdot 11^b=4y^n,\ \ x,y\geq 1,\ \ (x,y)=1,\ \ n\geq 3,\ \ a,b\geq 0 \tag{2.5}$$

egyenlet megoldásai:

$5^2 + 7^1 \cdot 11^0 = 4 \cdot 2^3$, $11^2 + 7^1 \cdot 11^0 = 4 \cdot 2^5$, $31^2 + 7^0 \cdot 11^1 = 4 \cdot 3^5$,
$57^2 + 7^1 \cdot 11^2 = 4 \cdot 4^5$, $13^2 + 7^3 \cdot 11^0 = 4 \cdot 2^7$, $57^2 + 7^1 \cdot 11^2 = 4 \cdot 2^{10}$
$181^2 + 7^1 \cdot 11^0 = 4 \cdot 2^{13}$.

- *Az*

$$x^2 + 7^a \cdot 13^b = 4y^n, \quad x, y \geq 1, \quad \gcd(x, y) = 1, \quad n \geq 3, \quad a, b \geq 0 \tag{2.6}$$

diofantikus egyenlet megoldásai:

$5^2 + 7^1 \cdot 13^0 = 4 \cdot 2^3$, $5371655^2 + 7^3 \cdot 13^2 = 4 \cdot 19322^3$, $11^2 + 7^1 \cdot 13^0 = 4 \cdot 2^5$,
$13^2 + 7^3 \cdot 13^0 = 4 \cdot 2^7$, $87^2 + 7^3 \cdot 13^2 = 4 \cdot 4^7$,
$181^2 + 7^1 \cdot 13^0 = 4 \cdot 2^{13}$, $87^2 + 7^3 \cdot 13^2 = 4 \cdot 2^{14}$.

3

Számtani sorozat elemeinek szorzatával kapcsolatos diofantikus problémák

Ebben a fejezetben a [106] dolgozatban szereplő, a [57] cikkben szereplő, Laishrammal és Shoreyval közösen igazolt és a [49] publikációban Hajduval és Tijdemannal közösen nyert eredmények kerülnek bemutatásra.

Az irodalomban rengeteg eredmény található számtani sorozatokkal kapcsolatos diofantikus problémákról. Ebben a fejezetben a

$$n(n+d)\dots(n+(k-1)d) = by^l \tag{3.1}$$

egyenlettel foglalkozunk, ahol n, d, k, b, y, l pozitív egészek, $l \geq 2$, $k \geq 3$, $(n, d) = 1$, $P(b) \leq k$, itt $u \in \mathbb{Z}$ és $|u| > 1$ esetén $P(u)$ jelöli u legnagyobb prímosztóját és $P(\pm 1) = 1$.

Néhány publikációt emelnénk ki a témakörben: [15], [38], [41], [44], [50], [55], [56], [63], [81], [83], [84], [85], [87], [90], [91], [92], [93], [95], [96], [97], [98], [109], [110]. Továbbá néhány eredményről az alábbiakban részletesen is említést teszünk.

Tekintsük először az $l = 2$ esetet. Már Euler igazolta ([33] 440 és 635 oldalak), hogy a (3.1) egyenletnek nincs megoldása, ha $k = 4$ és $b = 1$. Később Obláth [75] kiterjesztette az eredményt a $k = 5$ esetre. Erdős [34] és Rigge [80] egymástól függetlenül belátták, hogy a (3.1) egyenletnek nincs megoldása, ha $b = d = 1$. Hirata-Kohno, Laishram, Shorey és Tijdeman [52] teljesen megoldották a (3.1) egyenletet, amikor $3 \leq k < 110$ és $b = 1$. Tengely [107] eredményével kombinálva a fenti probléma összes megoldását megkapjuk, ha $3 \leq k \leq 100$, $P(b) < k$.

Tekintsük most az $l \geq 3$ esettel kapcsolatos eredményeket. Erdős és Selfridge [35] igazolta, hogy a (3.1) egyenletnek nincs megoldása, ha $b = d = 1$. Általánosabb esetben, amikor $P(b) \leq k$ és $d = 1$ Saradha [82] bizonyította, hogy $k \geq 4$ feltétel mellett az egyenletnek nincs olyan megoldása, amelyre $P(y) > k$.

Felhasználva Darmon és Merel [29] eredményét, Győry [42] hasonló tételt igazolt a $k = 2, 3$ esetekben. Abban az esetben, amikor elhagyjuk a d-re vonatkozó megszorítást is, Győry [43] belátta, hogy $k = 3, P(b) \leq 2$ mellett nem létezik megoldása az egyenletnek. További általános eredményeket találunk a [8], [45] és a [46] dolgozatokban. Többek között igazolást nyert, hogy a (3.1) egyenletnek nincs megoldása, ha $b = 1$ és $k < 35$.

A [106] cikkben Tengely két korábbi tétellel kapcsolatban igazolt állításokat, először ezeket ismertetjük.

Tétel (Mukhopadhyay, Shorey). *Tegyük fel, hogy n és d relatív prím egészek úgy, hogy $nd \neq 0$. Ekkor az*

$$n(n+d)(n+2d)(n+3d)(n+4d) = by^2$$

diofantikus egyenletnek nem létezik $b, y, by \neq 0$ és $P(b) \leq 3$ feltételek mellett egész megoldása.

Az eredményt Tengely kiterjesztette a $P(b) = 5$ esetre és igazlta a következő tételt.

3.1. Tétel. *Az*

$$n(n+d)(n+2d)(n+3d)(n+4d) = by^2$$

egyenletnek $d > 1, k = 5$ és $P(b) = 5$ feltételekkel a következő (n, d) párokkal létezik megoldása $(n, d) \in \{(-12, 7), (-4, 3)\}$.

A fenti (3.1) egyenletet $l = 2$ esetén vizsgálva azt kapjuk, hogy a számtani sorozat tagjai is "közel" teljes négyzetszámok, azaz

$$n + id = a_i x_i^2 \text{ minden } 0 \leq i < k \tag{3.2}$$

adódik, ahol az a_i egészek már négyzetmentesek és $P(a_i) \leq \max(P(b), k-1)$. Az egyenlet minden megoldásához tartozik egy ilyen $(a_0, a_1, \ldots, a_{k-1})$ együttható lista. Egy ilyen együttható lista inverzén az $(a_{k-1}, a_{k-2}, \ldots, a_0)$ listát értjük.

Tétel (Hirata-Kohno, Laishram, Shorey, Tijdeman). *Tekintsük a* (3.1) *egyenletet $l = 2, d > 1, P(b) = k$ és $7 \leq k \leq 100$ feltételekkel. Ekkor a következő együttható listák vagy azok inverzei esetében létezhetnek megoldások.*

$k = 7$: $(2, 3, 1, 5, 6, 7, 2), (3, 1, 5, 6, 7, 2, 1), (1, 5, 6, 7, 2, 1, 10)$,

$k = 13$: $(3, 1, 5, 6, 7, 2, 1, 10, 11, 3, 13, 14, 15)$,

$(1, 5, 6, 7, 2, 1, 10, 11, 3, 13, 14, 15, 1)$,

$k = 19$: $(1, 5, 6, 7, 2, 1, 10, 11, 3, 13, 14, 15, 1, 17, 2, 19, 5, 21, 22)$,

$k = 23$: $(5, 6, 7, 2, 1, 10, 11, 3, 13, 14, 15, 1, 17, 2, 19, 5, 21, 22, 23, 6, 1, 26, 3)$,

$(6, 7, 2, 1, 10, 11, 3, 13, 14, 15, 1, 17, 2, 19, 5, 21, 22, 23, 6, 1, 26, 3, 7)$.

Tengely megoldotta a kimaradó eseteket, igazolva a következő állítást.

3.2. Tétel. *A* (3.1) *egyenletnek az* $l = 2, d > 1, P(b) = k$ *és* $7 \leq k \leq 100$ *feltételek mellett nincs megoldása.*

Az eredmények igazolásához algebrai számelméleti eszközökre és az elliptikus Chabauty-módszer [18],[19] alkalmazására volt szükség. Például az $(a_0, a_1, \ldots, a_6) = (1, 5, 6, 7, 2, 1, 10)$ együttható lista esetében a következő egyenletrendszerre jutunk

$$\begin{aligned} x_5^2 + 4x_0^2 &= 25x_1^2, \\ 4x_5^2 + x_0^2 &= 10x_4^2, \\ 6x_5^2 - x_0^2 &= 50x_6^2. \end{aligned}$$

A Gauss egészek körében történő faktorizáció segítségével számtest feletti elliptikus görbe speciális pontjainak a meghatározására redukálódik a probléma. Ebben az esetben a görbék:

$$C_\delta : \quad \delta(X + i)(X + 4i)(3X^2 - 2) = Y^2, \tag{3.3}$$

ahol $\delta \in \{-3 \pm i, -1 \pm 3i, 1 \pm 3i, 3 \pm i\}$. Megjegyezzük, hogy ha (X, Y) egy megfelelő pont ($X \in \mathbb{Q}$ és $Y \in \mathbb{Q}(i)$) a C_δ görbén, akkor (X, iY) egy megfelelő pont a $C_{-\delta}$ görbén. Így elegendő a $\delta \in \{1 - 3i, 1 + 3i, 3 - i, 3 + i\}$ eseteket vizsgálni.

1. $\delta = 1 - 3i$. Ekkor C_{1-3i} izomorf az

   $$E_{1-3i} : \quad y^2 = x^3 + ix^2 + (-17i - 23)x + (2291i + 1597)$$

   elliptikus görbével, amelynek a rangja nulla és nincs olyan pont, amelyre $X \in \mathbb{Q}$.

2. $\delta = 1 + 3i$. Szintén nulla rangú elliptikus görbét kapunk és itt sem adódik megoldáshoz vezető pont.

3. $\delta = 3 - i$. Az elliptikus görbe ekkor $E_{3-i} : y^2 = x^3 + x^2 + (-17i + 23)x + (-1597i - 2291)$, és a Mordell-Weil csoportra $E_{3-i}(\mathbb{Q}(i)) \simeq \mathbb{Z}_2 \oplus \mathbb{Z}$ adódik. Az elliptikus Chabauty-módszert alkalmazva a $p = 13$ választással kapjuk, hogy $x_5/z = -3$. Így tehát $n = 2$ és $d = 1$.

4. $\delta = 3 + i$. Ekkor ismét egy rangú elliptikus görbét kapunk és az elliptikus Chabauty-módszerrel $x_5/z = 3$.

Az előző probléma egy változatát vizsgálta Laishram, Shorey és Tengely a [57] dolgozatban. A számtani sorozat egymást követő tagjai közül néhányat törlünk a szorzatból és továbbra is olyan sorozatokat keresünk, amelyeknél ez a szorzat közel teljes négyzetszámot eredményez. Nézzük a probléma pontosabb megfogalmazását.

Legyen $k \geq 4, t \geq k-2$ és $\gamma_1 < \gamma_2 < \cdots < \gamma_t$ egészek, amelyekre $0 \leq \gamma_i < k$ minden $1 \leq i \leq t$ esetén. Jelölje ψ a $k-t$ különbséget, b legyen egy négyzetmentes egész, amelyre $P(b) \leq k$. A probléma ekkor a következő egyenletre vezet

$$\Delta = \Delta(n, d, k) = (n + \gamma_1 d) \cdots (n + \gamma_t d) = by^2. \tag{3.4}$$

Az egyenlettel foglalkozó korábbi eredményekkel kapcsolatban itt a [86], [69] és a [94] publikációkat említenénk.

A [57] cikkben a következő két állítás lett igazolva.

3.3. Tétel. *Legyen $\psi = 1, k \geq 7$ és $d \nmid n$. Ekkor a* (3.4) *egyenletnek nincs megoldása, ha $\omega(d) = 1$, ahol $\omega(d)$ jelöli d különböző prímosztóinak a számát.*

A tétel alapján könnyen adódik, hogy a fenti egyenletnek nincs megoldása, ha $\psi = 0, k \geq 7$, $d \nmid n$, $P(b) \leq p_{\pi(k)+1}$ és $\omega(d) = 1$. Amennyiben $k \geq 11$ a $P(b) \leq p_{\pi(k)+1}$ feltétel javítható, ami a következő eredményre vezet.

3.4. Tétel. *Legyen $\psi = 0, k \geq 11$ és $d \nmid n$. Tegyük fel, hogy $P(b) \leq p_{\pi(k)+2}$. Ekkor a* (3.4) *egyenletnek nincs megoldása, ha $\omega(d) = 1$.*

A fejezet hátralévő részében a (3.1) egyenlettel foglalkozunk az $l = 3$ esetben és bemutatjuk Hajdu, Tengely és Tijdeman [49] publikációban bizonyított eredményeit.

A vizsgált diofantikus egyenlet a következő

$$n(n+d)\dots(n+(k-1)d) = by^3, \tag{3.5}$$

ahol $n, d, k, b, y \in \mathbb{Z}$ és $k \geq 3$, $d > 0$, $(n, d) = 1$, $P(b) \leq k$, $n \neq 0, y \neq 0$. A dolgozat egyik tétele az alábbi.

3.5. Tétel. *Tegyük fel, hogy (n, d, k, b, y) megoldása a* (3.5) *egyenletnek, amelyre $k < 32$ és $P(b) < k$ ha $k = 3$ vagy $k \geq 13$. Ekkor (n, d, k) a következő listában*

szereplő elemek közül kerülhet ki:

$$(n,1,k) \text{ ahol } -30 \le n \le -4 \text{ vagy } 1 \le n \le 5,$$
$$(n,2,k) \text{ ahol } -29 \le n \le -3,$$
$$(-10,3,7),(-8,3,7),(-8,3,5),(-4,3,5),(-4,3,3),(-2,3,3),$$
$$(-9,5,4),(-6,5,4),(-16,7,5),(-12,7,5).$$

Megjegyezzük, hogy a tétel állítása $k < 12$ és $P(b) \le P_k$ ahol $P_3 = 2$, $P_4 = P_5 = 3$, $P_6 = P_7 = P_8 = P_9 = P_{10} = P_{11} = 5$ esetekben következik Bennett, Bruin, Győry és Hajdu [8] publikációban közölt eredményéből.

A $b = 1$ speciális esetben Hajdu, Tengely és Tijdeman belátták a következő állítást.

3.6. Tétel. *Tegyük fel, hogy* (n,d,k,y) *megoldása a* (3.5) *egyenletnek, amelyre* $b = 1$ *és* $k < 39$. *Ekkor*

$$(n,d,k,y) = (-4,3,3,2),(-2,3,3,-2),(-9,5,4,6) \text{ vagy } (-6,5,4,6).$$

A fenti eredmények igazolásánál kihasználjuk, hogy a sorozat tagjaira teljesül, hogy

$$n + id = a_i x_i^3 \quad (i = 0,1,\dots,k-1) \tag{3.6}$$

ahol $P(a_i) \le k$ és a_i nem osztható prímszám teljes köbével. A bizonyításban fel lettek használva Selmer [89] eredményei bizonyos diofantikus egyenletekkel kapcsolatban.

3.1. Lemma. *A következő diofantikus egyenleteknek nem létezik* $x,y,z, xyz \neq 0$ *egész megoldása*

$$x^3 + y^3 = cz^3, \quad c \in \{1,2,4,5,10,25,45,60,100,150,225,300\},$$
$$ax^3 + by^3 = z^3, \ (a,b) \in \{(2,9),(4,9),(4,25),(4,45),(12,25)\}.$$

Ezen felül különféle kongruencia tesztek kombinatorikus alkalmazása tette lehetővé nagy számú együttható listák eliminálását, amelyeknél nem létezhet megfelelő számtani sorozat. A kimaradó együttható listákat külön meg kellett vizsgálni és Selmer eredményeit vagy pedig az elliptikus Chabauty-módszert alkalmazva ki lehetett zárni vagy pedig a megoldásokat megadni. A nagyobb k értékeknél a kongruencia tesztek segítségével sikerült indukciót is alkalmazni és a korábban igazolt eredmények segítségével együttható listákat kezelni. Így a kombinatorikus robbanás kezelése elérhetővé vált nagyobb k értékek esetében is. Tekintsünk néhány példát a fentiekre.

Legyen $k = 5$. Ekkor könnyen igazolható, hogy az

$$(a_0, a_1, a_2, a_3, a_4) = (1, 1, 1, 10, 1)$$

együttható lista nem vezethet megoldáshoz modulo 7. Szintén egyszerűen adódik, hogy az

$$(a_0, a_1, a_2, a_3, a_4) = (1, 1, 15, 1, 1)$$

együttható lista kizárható modulo 9. Viszont az

$$(a_0, a_1, a_2, a_3, a_4) = (2, 3, 4, 5, 6)$$

együttható lista esetében sem modulo 7 sem modulo 9 nem kapunk ellentmondást. Selmer eredményei itt segítenek, felhasználva a $4(n + d) - 3n = n + 4d$ azonosságot kapjuk, hogy $n = 2$ és $d = 1$. Az előző gondolatmenettel minden együttható lista kezelhető kivéve az

$$(a_0, a_1, a_2, a_3, a_4) = (2, 9, 2, 5, 12).$$

Ebben az esetben

$$x_0^3 + x_2^3 = 9x_1^3 \text{ és } x_0^3 - 2x_2^3 = -6x_4^3.$$

A $\mathbb{Q}(\sqrt[3]{2})$ számtestben dolgozva kapjuk, hogy

$$(x_0 - \alpha x_2)(x_0^2 - x_0x_2 + x_2^2) = (-3\alpha + 6)z^3.$$

Ez számtest feletti elliptikus görbére vezet. Ezen görbén kell meghatározni azon pontokat, ahol az első koordináta racionális értéket vesz fel, ezt az elliptikus Chabauty-módszer segítségével tehetjük meg.

3.2. Lemma. *Legyen $\alpha = \sqrt[3]{2}$ és $K = \mathbb{Q}(\alpha)$. Ekkor a*

$$\mathcal{C}_1 : \quad X^3 - (\alpha + 1)X^2 + (\alpha + 1)X - \alpha = (-3\alpha + 6)Y^3$$

görbén csak az $(X, Y) = (2, 1)$ pont tesz eleget annak a feltételnek, hogy $X \in \mathbb{Q}$ és $Y \in K$.

4

Számtani sorozatot alkotó teljes hatványok

Ebben a fejezetben a [17] dolgozatban szereplő, Bruinnal, Győryvel és Hajduval közösen nyert és a [48] cikkben igazolt, Hajduval közös eredmények kerülnek bemutatásra.

Már Fermat megfogalmazta a sejtést, hogy négy különböző négyzetszám nem alkothat számtani sorozatot, ezt később Euler be is bizonyította ([33] 440. és 635. oldal). Legyen $n \geq 3$ és X^n, Z^n, Y^n egy számtani sorozat három egymást követő tagja. Ekkor a következő diofantikus egyenlethez jutunk:

$$X^n + Y^n = 2Z^n.$$

Az egyenlet megoldása $n = 3$ esetben már Mordell könyvében [68] megtalálható. Az $n = 5$ eset vizsgálata pedig Dirichlet és Lebesgue (lásd [33] 735. és 738. oldal) eredményei alapján kezelhető. Dénes [32] ért el később jelentős eredményt megoldva az egyenletet az $n \leq 31$ esetekben. Végül Darmon és Merel [29], felhasználva a Fermat-egyenlet megoldásánál is alkalmazott moduláris módszert, megmutatta, hogy a triviális esetektől eltekintve nem létezik három elemű számtani sorozat teljes hatványokból.

A homogén hatványokról most térjünk át egy még általánosabb esetre, tekintsük az

$$a_0 x_0^{n_0}, a_1 x_1^{n_1}, \ldots, a_{k-1} x_{k-1}^{n_{k-1}} \tag{4.1}$$

alakú számtani sorozatokat, ahol $a_i, x_i \in \mathbb{Z}, n_i \geq 2$ és a_i prímosztói korlátosak, azaz $P(a_i) \leq P$ valamilyen P-re. Plusz feltételek nélkül k értéke nem korlátozható, ahogyan azt Hajdu [47] konstrukciója is mutatja. Az n_i kitevők és $(a_0 x_0, a_1 x_1)$ korlátozásával már kezelhetőbbé válik a probléma. Vegyes hatványok esetében az egyik alkalmazható mély eszközt Darmon és Granville [28] eredménye jelenti, amelyben az általánosított Fermat-egyenlettel foglalkoznak. Ineffektív formában végességet biztosítanak az

$$AX^p + BY^q = CZ^r, \quad ABC \neq 0$$

egyenlettel kapcsolatban, ha

$$\frac{1}{p}+\frac{1}{q}+\frac{1}{r}>1.$$

A (4.1) alakú számtani sorozatokkal kapcsolatban először tekintsük Hajdu [47] egy eredményét.

4.1. Tétel (Hajdu). *Legyen $L \geq 2$ egy rögzített egész. Ekkor bármely* (4.1) *alakú számtani sorozat esetében, ahol $n_i \leq L, (i = 0, 1, \ldots, k-1)$, létezik csak L és P értékétől függő $C(L, P)$ konstans úgy, hogy $k \leq C(L, P)$.*

A [17] dolgozatban Bruin, Győry, Hajdu és Tengely a következő tételt igazolták.

4.2. Tétel. *Legyen $k \geq 4$ és $L \geq 2$ egy rögzített egész. Ekkor csak véges sok* (4.1) *alakú számtani sorozat létezik, melyre $n_i \leq L, a_i = 1, (i = 0, 1, \ldots, k-1)$ és $(x_0, x_1) = 1$.*

A tétel bizonyításában olyan mély eszközök alkalmazása volt szükséges, mint a korábban már említett eredménye Darmonnak és Granvillenek és Faltings [36] dolgozata a Mordell-sejtés bizonyításáról.

Amennyiben $n_i \in \{2, 3\}$ még több bizonyítható, ebben az esetben a [17] dolgozatban az összes megoldást megadta Bruin, Győry, Hajdu és Tengely.

4.3. Tétel. *Legyen $k \geq 4, (x_0, x_1) = 1, a_i = 1, n_i \in \{2, 3\}$ minden $i = 0, 1, \ldots, k-1$ esetén. Ekkor a* (4.1) *számtani sorozat csak a triviális $1, 1, \ldots, 1$ és $-1, -1, \ldots, -1$ sorozatok egyike lehet.*

Megjegyezzük, hogy a $(x_0, x_1) = 1$ feltétel szükséges, ahogyan azt a következő példák is igazolják.

- Legyen $(n_0, n_1, n_2, n_3) = (2, 2, 2, 3)$. Ekkor

  $$((u^2-2uv-v^2)f(u,v))^2, ((u^2+v^2)f(u,v))^2, ((u^2+2uv-v^2)f(u,v))^2, (f(u,v))^3$$

  egy számtani sorozat négy egymást követő tagja, ahol $u, v \in \mathbb{Z}$ és $f(u, v) = u^4 + 8u^3v + 2u^2v^2 - 8uv^3 + v^4$.

- Legyen $(n_0, n_1, n_2, n_3) = (2, 2, 3, 2)$. Ekkor

  $$((u^2-2uv-2v^2)g(u,v))^2, ((u^2+2v^2)g(u,v))^2, (g(u,v))^3, ((u^2+4uv-2v^2)g(u,v))^2$$

  számtani sorozatot alkot, ahol $u, v \in \mathbb{Z}$ és $g(u, v) = u^4 + 4u^3v + 8u^2v^2 - 8uv^3 + 4v^4$.

A tétel állításának igazolásához a már ismert eredményeken felül a klasszikus Chabauty-módszer és az elliptikus Chabauty-módszer került alkalmazásra. Ezt az egyik eset bemutatásával illusztráljuk. Tekintsük az $x_0^2, x_1^2, x_2^2, x_3^3$ alakú sorozatot. Ekkor

$$2x_2^2 - x_2^2 = x_3^3.$$

Az egyenlet parametrikus megoldása

$$x_1 = \pm(x^3 + 6xy^2), \quad x_2 = \pm(3x^2y + 2y^3)$$

vagy

$$x_1 = \pm(x^3 + 6x^2y + 6xy^2 + 4y^3), \quad x_2 = \pm(x^3 + 3x^2y + 6xy^2 + 2y^3),$$

ahol x, y relatív prím egészek. Felhasználva, hogy $x_0^2 = 2x_1^2 - x_2^2$ adódik a következő egyenlet:

$$x_0^2 = 2x^6 + 15x^4y^2 + 60x^2y^4 - 4y^6.$$

Ez az egyenlet elliptikus görbére vezet, amelynek nincs affin racionális pontja. A második parametrizációból az

$$x_0^2 = x^6 + 18x^5y + 75x^4y^2 + 120x^3y^3 + 120x^2y^4 + 72xy^5 + 28y^6$$

egyenlet adódik. Itt az $y = 0$ eset könnyen látható módon a triviális $1, 1, 1, 1$ sorozatra vezet. Az $y \neq 0$ esetben legyen $Y = x_0/y^3$, $X = x/y$. Így az előző egyenlet a

$$\mathcal{C}_1 : Y^2 = X^6 + 18X^5 + 75X^4 + 120X^3 + 120X^2 + 72X + 28$$

génusz kettes görbét eredményezi. Itt a klasszikus Chabauty-módszert [24] alkalmazzuk és az ezzel kapcsolatos algoritmusokat, amelyek Stolltól [102] származnak és a MAGMA programcsomagban megtalálhatóak. Először is szükségünk van a $\mathcal{J}(\mathbb{Q})$ Mordell-Weil csoportjával kapcsolatos információkra. A torziós részcsoport triviális, ami egyszerűen adódik abból, hogy a rendje osztja a $(\#\mathcal{J}(\mathbb{F}_5), \#\mathcal{J}(\mathbb{F}_7)) = (21, 52) = 1$ értéket. A Mordell-Weil csoport rangjáról megmutatható, hogy eggyel egyenlő és $D = [\infty^+ - \infty^-]$ egy végtelen rendű elem. A klasszikus Chabauty-módszert alkalmazva a $p = 29$ választással kapjuk, hogy legfeljebb két darab racionális pont lehet a görbén, ennyit pedig ismerünk is, így több racionális pont nem lehet a görbén, azaz $\mathcal{C}_1(\mathbb{Q}) = \{\infty^+, \infty^-\}$.

Most rátérünk a Hajdu és Tengely által [48] publikációban igazolt állítások bemutatására. A cikkben olyan $x_0^{n_0}, x_1^{n_1}, \ldots, x_{k-1}^{n_{k-1}}$ alakú számtani sorozatok vizsgálatával találkozunk, ahol $(x_0, x_1) = 1$ és $n_i \in \{2, n\}, \{2, 5\}$ vagy $\{3, n\}$. A különböző esetekre bizonyított tételeket az alábbiakban ismertetjük.

4.4. Tétel. *Legyen n egy prím és $x_0^{n_0}, x_1^{n_1}, \ldots, x_{k-1}^{n_{k-1}}$ egy nem konstans számtani sorozat, amelyre $(x_0, x_1) = 1, x_i \in \mathbb{Z}, n_i \in \{2, n\}$ minden $i = 0, 1, \ldots, k-1$ értékre. Ekkor $k \leq 5$, továbbá, ha $k = 5$, akkor*

$$(n_0, n_1, n_2, n_3, n_4, n_5) = (2, n, n, 2, 2, 2), (2, 2, 2, n, n, 2).$$

Az $n = 5$ speciális esetben élesebb állítás is igaz.

4.5. Tétel. *Legyen $x_0^{n_0}, x_1^{n_1}, \ldots, x_{k-1}^{n_{k-1}}$ egy nem konstans számtani sorozat, amelyre $(x_0, x_1) = 1, x_i \in \mathbb{Z}, n_i \in \{2, 5\}$ minden $i = 0, 1, \ldots, k-1$ értékre. Ekkor $k \leq 3$, továbbá, ha $k = 3$, akkor*

$$(n_0, n_1, n_2, n_3) = (2, 2, 2, 5), (5, 2, 2, 2).$$

Megjegyezzük, hogy a tételben szereplő két kivételes esetben Siksek és Stoll [99] a közelmúltban megmutatták, hogy csak a triviális $1, 1, 1, 1$ sorozat létezik. Visszavezették a problémát génusz 4 görbék racionális pontjainak vizsgálatára. Tekintsük most az $n_i \in \{3, n\}$ esetre vonatkozó állítást.

4.6. Tétel. *Legyen n egy prím és $x_0^{n_0}, x_1^{n_1}, \ldots, x_{k-1}^{n_{k-1}}$ egy nem konstans számtani sorozat, amelyre $(x_0, x_1) = 1, x_i \in \mathbb{Z}, n_i \in \{3, n\}$ minden $i = 0, 1, \ldots, k-1$ értékre. Ekkor $k \leq 3$, továbbá, ha $k = 3$, akkor*

$$(n_0, n_1, n_2, n_3) = (3, 3, n, n), (n, n, 3, 3), (3, n, n, 3), (n, 3, 3, n).$$

A bizonyításban felhasználjuk az alábbi, moduláris módszer segítségével igazolt tételeket.

Tétel. *Legyen n egy prím. Ekkor az*

$$\begin{aligned} X^n + Y^n &= 2Z^2 \quad (n \geq 5), \\ X^n + Y^n &= 3Z^2 \quad (n \geq 5), \\ X^n + 4Y^n &= 3Z^2 \quad (n \geq 7) \end{aligned}$$

diofantikus egyenleteknek nem létezik páronként relatív prím (X, Y, Z) megoldása, amelyre $XY \neq \pm 1$.

A tételben szereplő állítások Bennett és Skinner [9], illetve Bruin [16] eredményeiből következnek. Az X^n, Z^3, Y^n alakú számtani sorozatok esetében a következő, Bennett, Vatsal és Yazdani [10] által bizonyított tétel igaz.

Tétel. *Legyen $n \geq 5$ egy prím. Ekkor az*

$$X^n + Y^n = 2Z^3$$

diofantikus egyenletnek nem létezik relatív prím X, Y, Z megoldása, amelyre $XYZ \neq 0, \pm 1$.

Az X^n, Z^n, Y^n alakú sorozatok esetében pedig a korábban már említett, Darmon és Merel [29] dolgozatában található eredményt használhatjuk.

Tétel. *Legyen $n \geq 3$ egy prím. Ekkor az*

$$X^n + Y^n = 2Z^n$$

diofantikus egyenletnek nem létezik relatív prím X, Y, Z megoldása, amelyre $XYZ \neq 0, \pm 1$.

Az X^3, Z^n, Y^3 alakú számtani sorozatokkal kapcsolatban Hajdu és Tengely belátta a következő állítást.

4.7. Tétel. *Legyen $n \geq 3$ egy prím. Ekkor az*

$$X^3 + Y^3 = 2Z^n$$

diofantikus egyenletnek nem létezik relatív prím X, Y, Z megoldása, amelyre $XYZ \neq 0, \pm 1$ és $3 \nmid Z$.

Az előző eredmények hasznos segítséget jelentenek az $n_i \in \{2, n\}, \{3, n\}$ esetek vizsgálatakor. Az $n_i \in \{2, 5\}$ esetre vonatkozó tétel bizonyításához a problémát bizonyos számtest feletti elliptikus görbe speciális alakú pontjainak meghatározására vezetjük vissza algebrai számelméleti módszerekkel. Az elliptikus Chabauty-módszer segítségével pedig meghatározzuk a racionális első koordinátával rendelkező pontokat, amelyekből vissza tudjuk fejteni az eredeti probléma lehetséges megoldásait. Az itt felhasznált és bizonyított állítások a következőek.

4.1. Lemma. *Legyen $\alpha = \sqrt[5]{2}$ és $K = \mathbb{Q}(\alpha)$. Ekkor a*

$$C_1: \quad \alpha^4 X^4 + \alpha^3 X^3 + \alpha^2 X^2 + \alpha X + 1 = (\alpha - 1)Y^2 \tag{4.2}$$

és

$$C_2: \quad \alpha^4 X^4 - \alpha^3 X^3 + \alpha^2 X^2 - \alpha X + 1 = (\alpha^4 - \alpha^3 + \alpha^2 - \alpha + 1)Y^2 \tag{4.3}$$

algebrai görbéken azon pontok, amelyekre $X \in \mathbb{Q}$, $Y \in K$ a következőek

$$(X, Y) = (1, \pm(\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1)), \ \left(-\frac{1}{3}, \pm\frac{3\alpha^4 + 5\alpha^3 - \alpha^2 + 3\alpha + 5}{9}\right)$$

a C_1 görbe esetében és $(X, Y) = (1, \pm 1)$ a C_2 görbe esetében.

4.2. Lemma. *Legyen $\beta = (1 + \sqrt{5})/2$ és $L = \mathbb{Q}(\beta)$. Ekkor a*

$$C_3: \quad X^4 + (8\beta - 12)X^3 + (16\beta - 30)X^2 + (8\beta - 12)X + 1 = Y^2 \tag{4.4}$$

algebrai görbén egyedül az $(X, Y) = (0, \pm 1)$ pontokra teljesül, hogy $X \in \mathbb{Q}$ és $Y \in L$.

5

Algebrai görbék pontjaival kapcsolatos eredmények

Ebben a fejezetben a [105] dolgozatban szereplő és a [22] cikkben megjelent, Bugeaudval, Mignotteval, Siksekkel és Stoll-lal közös eredmények kerülnek bemutatásra.

A fejezet első részében bemutatjuk a [105] publikációban található eredményeket, amelyek geometriai problémával összefüggő diofantikus egyenletekkel kapcsolatosak. Az irodalomban jelentős számú geometriai hátterű diofantikus probléma található. Az egyik jól ismert a derékszögű háromszögek oldalaival kapcsolatos Pitagorasz-tétel, azaz a derékszögű háromszög oldalaira teljesül, hogy $a^2 + b^2 = c^2$.

Már egy régi arab kézirat is foglalkozott az úgynevezett kongruens számok problémájával, azaz olyan derékszögű háromszögek megadásával, amelyeknek az oldalaiknak hossza racionális szám, a területük pedig egész. Például 6 kongruens szám, mert a $(3, 4, 5)$ hosszú oldalakkal rendelkező derékszögű háromszög területe 6. Fibonacci fogalmazta meg azt az állítást, hogy 1 nem kongruens szám. Az állítást később Fermat igazolta, a végtelen leszállás módszerének segítségével. A jelenleg ismert legpontosabb általános eredményt Tunnell bizonyította [111] a moduláris módszert felhasználva.

Az egész oldalhosszúságú háromszögek közül azokat, amelyeknek a területe is egész szám, Hérón-féle háromszögeknek nevezzük. Az ilyen típusú háromszögekkel kapcsolatban is több eredmény található az irodalomban, például a [51] és a [39] cikkekben, további információk és megoldatlan problémák a [40] könyvben szerepelnek.

Petulante és Kaja [76] megadták azon egész oldalú háromszögeknek a parametrizációját, amelyekben egy adott szög koszinusza racionális, azaz meghatározták az $u^2 - 2\alpha uv + v^2 = 1$ görbe racionális parametrizációját, ahol α jelöli a racionális koszinusz értékét.

Bertalan Zoltán olyan egész x, y értékeket keresett, amelyekre teljesül, hogy ha egy óra kismutatójának hossza x, nagymutatójáé pedig y, akkor a két mutató távolabbi végpontjainak távolsága (i) 2 órakkor és 3 órakkor ((ii) 2 órakkor és 4 órakkor) is egész érték legyen. Legyenek $\varphi_1 = \cos(\alpha)$ és $\varphi_2 = \cos(\beta)$, ahol α, β a két mutató által bezárt szögek a vizsgált időpontokban. Ekkor a koszinusz-tétel alapján

$$x^2 - 2\varphi_1 xy + y^2 = z_\alpha^2,$$
$$x^2 - 2\varphi_2 xy + y^2 = z_\beta^2,$$

itt z_α és z_β jelöli az adott szöggel szemközti oldal hosszát. A két egyenlet összeszorzása után a következő algebrai görbét kapjuk:

$$\mathcal{C}_{\alpha,\beta} : X^4 - 2(\varphi_1 + \varphi_2)X^3 + (4\varphi_1\varphi_2 + 2)X^2 - 2(\varphi_1 + \varphi_2)X + 1 = Y^2,$$

ahol $X = x/y$ és $Y = z_\alpha z_\beta / y^2$. Tengely a [105] dolgozatában megoldotta a Bertalan Zoltán által felvetett problémákat. Például igazolta, hogy az (i) esetben végtelen sok megoldás létezik, mivel a kapcsolódó algebrai görbe 1 rangú elliptikus görbére vezet. Néhány megoldás:

x	y	$z_{\pi/3}$	$z_{\pi/2}$
8	15	13	17
1768	2415	2993	3637
10130640	8109409	9286489	12976609
498993199440	136318711969	517278459169	579309170089

A fejezet hátralévő részében a [22] pulikáció eredményeit tárgyaljuk. Legyen $C : Y^2 = a_n X^n + \cdots + a_0 := f(X)$ egy hiperelliptikus görbe, ahol $a_i \in \mathbb{Z}, n \geq 5$ és az f polinom irreducibilis. Ilyen görbék esetében Baker [7] igazolta, hogy a görbén található (X, Y) egész pontokra

$$\max(|X|, |Y|) \leq \exp\exp\exp\{(n^{10n} H)^{n^2}\},$$

ahol $H = \max\{|a_0|, \ldots, |a_n|\}$. A korlátot később többen élesítették, így például Sprindžuk [101], Brindza [13], Schmidt [88], Poulakis [79], Bilu [11], Bugeaud [23] és Voutier [112]. A Baker-módszer segítségével tehát az egész pontok méretére korlát adható, ezt kombinálva a Mordell-Weil szitával adott görbe esetében igazolható, hogy az ismert egész pontokon felül nincs más. Ez a módszer került tárgyalásra a dolgozatban, illusztrációként pedig két konkrét problémára alkalmazták sikerrel.

5.1. Tétel. *Az*

$$Y^2 - Y = X^5 - X \tag{5.1}$$

diofantikus egyenlet egész megoldásai:

$$(X, Y) = (-1, 0),\ (-1, 1),\ (0, 0),\ (0, 1),\ (1, 0),\ (1, 1),\ (2, -5),$$
$$(2, 6),\ (3, -15),\ (3, 16),\ (30, -4929),\ (30, 4930).$$

5.2. Tétel. *Az*

$$\binom{Y}{2} = \binom{X}{5} \tag{5.2}$$

diofantikus egyenlet egész megoldásai:

$$(X, Y) = (0, 0),\ (0, 1),\ (1, 0),\ (1, 1),\ (2, 0),\ (2, 1),\ (3, 0),\ (3, 1),\ (4, 0),\ (4, 1),$$
$$(5, -1),\ (5, 2),\ (6, -3),\ (6, 4),\ (7, -6),\ (7, 7),\ (15, -77),$$
$$(15, 78),\ (19, -152),\ (19, 153).$$

Az

$$Y^p - Y = X^q - X, \qquad 2 \le p < q. \tag{5.3}$$

egyenlettel kapcsolatban Mordell [67] igazolta, hogy ha $p = 2$, $q = 3$, akkor

$$(X, Y) = (0, 0), (0, 1), (\pm 1, 0), (\pm 1, 1), (2, 3), (2, -2), (6, 15), (6, -14).$$

Fielder és Alford [37] a következő X, $Y > 1$ megoldásokat adták meg:

$$(p, q, X, Y) = (2, 3, 2, 3), (2, 3, 6, 15), (2, 5, 2, 6), (2, 5, 3, 16),$$
$$(2, 5, 30, 4930), (2, 7, 5, 280), (2, 13, 2, 91), (3, 7, 3, 13).$$

Mignotte és Pethő [66] igazolta, hogy adott p és q esetén, ahol $2 \le p < q$, csak véges sok egész megoldás létezik. Továbbá, ha feltesszük az abc-sejtést, akkor az (5.3) egyenletnek csak véges sok egész X, $Y > 1$ megoldása létezik.

Az (5.2) egyenlet speciális esete az

$$\binom{n}{k} = \binom{m}{l} \tag{5.4}$$

diofantikus egyenletnek. A $2 \le k \le n/2$ és $2 \le l \le m/2$ kikötések mellett az ismert megoldások a következőek:

$$\binom{16}{2} = \binom{10}{3}, \quad \binom{56}{2} = \binom{22}{3}, \quad \binom{120}{2} = \binom{36}{3},$$
$$\binom{21}{2} = \binom{10}{4}, \quad \binom{153}{2} = \binom{19}{5}, \quad \binom{78}{2} = \binom{15}{5} = \binom{14}{6},$$
$$\binom{221}{2} = \binom{17}{8}, \quad \binom{F_{2i+2}F_{2i+3}}{F_{2i}F_{2i+3}} = \binom{F_{2i+2}F_{2i+3} - 1}{F_{2i}F_{2i+3} + 1} \text{ for } i = 1, 2, \ldots,$$

ahol F_n Fibonacci számok sorozata. Ismert a [31] dolgozatból, hogy nincs több megoldás, ha $\binom{n}{k} \leq 10^{30}$ vagy $n \leq 1000$. A végtelen megoldás család Lind [59] és Singmaster [100] publikációiban lett közölve. Az (5.4) diofantikus egyenlet összes megoldása meghatározásra került, ha

$$(k,l) = (2,3),\ (2,4),\ (2,6),\ (2,8),\ (3,4),\ (3,6),\ (4,6),\ (4,8).$$

Ezen esetekben a probléma visszavezethető elliptikus görbékre vagy Thue egyenletekre. Avanesov 1966-ban [6] megoldotta az (5.4) egyenletet, amikor $(k,l) = (2,3)$. De Weger [30] és tőle függetlenül Pintér [78] megoldotta a $(k,l) = (2,4)$ esetet. A $(k,l) = (3,4)$ párnál az egyenlet az $Y(Y+1) = X(X+1)(X+2)$ görbére vezet, amely megoldásait Mordell [67] határozta meg. A fennmaradó $(2,6),(2,8),(3,6),(4,6),(4,8)$ esetekben a megoldásokat Stroeker és de Weger [103] adta meg. A (5.4) egyenlettel kapcsolatban általános végességi tételt nyert 1988-ban Kiss [53]. Igazolta, hogy ha $k = 2$ és l adott páratlan prím, akkor csak véges sok pozitív megoldás létezik. Felhasználva a Baker-módszert, Brindza [14] megmutatta, hogy az (5.4) egyenletnek $k = 2$ és $l \geq 3$ mellett csak véges sok pozitív megoldása van.

Irodalomjegyzék

[1] F. S. Abu Muriefah, F. Luca, S. Siksek, and Sz. Tengely. On the Diophantine equation $x^2 + C = 2y^n$. *Int. J. Number Theory*, 5(6):1117–1128, 2009.

[2] S. A. Arif and F. S. A. Muriefah. On the Diophantine equation $x^2+2^k = y^n$. *Internat. J. Math. Math. Sci.*, 20(2):299–304, 1997.

[3] S. A. Arif and F. S. A. Muriefah. The Diophantine equation $x^2 + 3^m = y^n$. *Internat. J. Math. Math. Sci.*, 21(3):619–620, 1998.

[4] S. A. Arif and F S. A. Muriefah. On the Diophantine equation $x^2+2^k = y^n$. II. *Arab J. Math. Sci.*, 7(2):67–71, 2001.

[5] S. A. Arif and F. S. A. Muriefah. On the Diophantine equation $x^2+q^{2k+1} = y^n$. *J. Number Theory*, 95(1):95–100, 2002.

[6] È. T. Avanesov. Solution of a problem on figurate numbers. *Acta Arith.*, 12:409–420, 1966/1967.

[7] A. Baker. Bounds for the solutions of the hyperelliptic equation. *Proc. Cambridge Philos. Soc.*, 65:439–444, 1969.

[8] M. A. Bennett, N. Bruin, K. Győry, and L. Hajdu. Powers from products of consecutive terms in arithmetic progression. *Proc. London Math. Soc. (3)*, 92(2):273–306, 2006.

[9] M.A. Bennett and C.M. Skinner. Ternary Diophantine equations via Galois representations and modular forms. *Canad. J. Math.*, 56(1):23–54, 2004.

[10] M.A. Bennett, V. Vatsal, and S. Yazdani. Ternary Diophantine equations of signature $(p, p, 3)$. *Compos. Math.*, 140(6):1399–1416, 2004.

[11] Yu. Bilu. Effective analysis of integral points on algebraic curves. *Israel J. Math.*, 90(1-3):235–252, 1995.

[12] Yu. Bilu, G. Hanrot, and P. M. Voutier. Existence of primitive divisors of Lucas and Lehmer numbers. *J. Reine Angew. Math.*, 539:75–122, 2001. With an appendix by M. Mignotte.

[13] B. Brindza. On S-integral solutions of the equation $y^m = f(x)$. *Acta Math. Hungar.*, 44(1-2):133–139, 1984.

[14] B. Brindza. On a special superelliptic equation. *Publ. Math. Debrecen*, 39(1-2):159–162, 1991.

[15] B. Brindza, L. Hajdu, and I. Z. Ruzsa. On the equation $x(x+d)\cdots(x+(k-1)d) = by^2$. *Glasg. Math. J.*, 42(2):255–261, 2000.

[16] N. Bruin. Some ternary Diophantine equations of signature $(n, n, 2)$. In *Discovering mathematics with Magma*, volume 19 of *Algorithms Comput. Math.*, pages 63–91. Springer, Berlin, 2006.

[17] N. Bruin, K. Győry, L. Hajdu, and Sz. Tengely. Arithmetic progressions consisting of unlike powers. *Indag. Math. (N.S.)*, 17(4):539–555, 2006.

[18] N. R. Bruin. *Chabauty methods and covering techniques applied to generalized Fermat equations*, volume 133 of *CWI Tract*. Stichting Mathematisch Centrum Centrum voor Wiskunde en Informatica, Amsterdam, 2002. Dissertation, University of Leiden, Leiden, 1999.

[19] Nils Bruin. Chabauty methods using elliptic curves. *J. Reine Angew. Math.*, 562:27–49, 2003.

[20] Y. Bugeaud. On the Diophantine equation $x^2 - p^m = \pm y^n$. *Acta Arith.*, 80(3):213–223, 1997.

[21] Y. Bugeaud, M. Mignotte, and S. Siksek. Classical and modular approaches to exponential Diophantine equations. II. The Lebesgue-Nagell equation. *Compos. Math.*, 142(1):31–62, 2006.

[22] Y. Bugeaud, M. Mignotte, S. Siksek, M. Stoll, and Sz. Tengely. Integral points on hyperelliptic curves. *Algebra Number Theory*, 2(8):859–885, 2008.

[23] Yann Bugeaud. Bounds for the solutions of superelliptic equations. *Compositio Math.*, 107(2):187–219, 1997.

[24] C. Chabauty. Sur les points rationnels des courbes algébriques de genre supérieur à l'unité. *C. R. Acad. Sci. Paris*, 212:882–885, 1941.

[25] J. H. E. Cohn. The Diophantine equation $x^2+2^k = y^n$. *Arch. Math. (Basel)*, 59(4):341–344, 1992.

[26] J. H. E. Cohn. The Diophantine equation $x^2 + C = y^n$. *Acta Arith.*, 65(4):367–381, 1993.

[27] J. H. E. Cohn. The Diophantine equation $x^2 + 2^k = y^n$. II. *Int. J. Math. Math. Sci.*, 22(3):459–462, 1999.

[28] H. Darmon and A. Granville. On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$. *Bull. London Math. Soc.*, 27(6):513–543, 1995.

[29] H. Darmon and L. Merel. Winding quotients and some variants of Fermat's last theorem. *J. Reine Angew. Math.*, 490:81–100, 1997.

[30] B. M. M. de Weger. A binomial Diophantine equation. *Quart. J. Math. Oxford Ser. (2)*, 47(186):221–231, 1996.

[31] Benjamin M. M. de Weger. Equal binomial coefficients: some elementary considerations. *J. Number Theory*, 63(2):373–386, 1997.

[32] P. Dénes. Über die Diophantische Gleichung $x^l + y^l = cz^l$. *Acta Math.*, 88:241–251, 1952.

[33] L.E. Dickson. *History of the theory of numbers. Vol II: Diophantine analysis*. Chelsea Publishing Co., New York, 1966.

[34] P. Erdös. Note on the product of consecutive integers (II). *J. London Math. Soc.*, 14:245–249, 1939.

[35] P. Erdős and J. L. Selfridge. The product of consecutive integers is never a power. *Illinois J. Math.*, 19:292–301, 1975.

[36] G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.*, 73(3):349–366, 1983.

[37] Daniel C. Fielder and Cecil O. Alford. Observations from computer experiments on an integer equation. In *Applications of Fibonacci numbers, Vol. 7 (Graz, 1996)*, pages 93–103. Kluwer Acad. Publ., Dordrecht, 1998.

[38] P. Filakovszky and L. Hajdu. The resolution of the Diophantine equation $x(x+d)\cdots(x+(k-1)d) = by^2$ for fixed d. *Acta Arith.*, 98(2):151–154, 2001.

[39] I. Gaál, I. Járási, and F. Luca. A remark on prime divisors of lengths of sides of Heron triangles. *Experiment. Math.*, 12(3):303–310, 2003.

[40] Richard K. Guy. *Unsolved problems in number theory*. Problem Books in Mathematics. Springer-Verlag, New York, second edition, 1994. Unsolved Problems in Intuitive Mathematics, I.

[41] K. Győry. On the Diophantine equation $\binom{n}{k} = x^l$. *Acta Arith.*, 80(3):289–295, 1997.

[42] K. Győry. On the Diophantine equation $n(n+1)\cdots(n+k-1) = bx^l$. *Acta Arith.*, 83(1):87–92, 1998.

[43] K. Györy. Power values of products of consecutive integers and binomial coefficients. In *Number theory and its applications (Kyoto, 1997)*, volume 2 of *Dev. Math.*, pages 145–156. Kluwer Acad. Publ., Dordrecht, 1999.

[44] K. Győry. Perfect powers in products with consecutive terms from arithmetic progressions. In *More sets, graphs and numbers*, volume 15 of *Bolyai Soc. Math. Stud.*, pages 143–155. Springer, Berlin, 2006.

[45] K. Győry, L. Hajdu, and Á. Pintér. Perfect powers from products of consecutive terms in arithmetic progression. *Compos. Math.*, 145(4):845–864, 2009.

[46] K. Győry, L. Hajdu, and N. Saradha. On the Diophantine equation $n(n+d)\cdots(n+(k-1)d) = by^l$. *Canad. Math. Bull.*, 47(3):373–388, 2004.

[47] L. Hajdu. Perfect powers in arithmetic progression. A note on the inhomogeneous case. *Acta Arith.*, 113(4):343–349, 2004. Dedicated to Robert Tijdeman on the occasion of his 60th birthday.

[48] L. Hajdu and Sz. Tengely. Arithmetic progressions of squares, cubes and n-th powers. *Funct. Approx. Comment. Math.*, 41(, part 2):129–138, 2009.

[49] Lajos Hajdu, Szabolcs Tengely, and Robert Tijdeman. Cubes in products of terms in arithmetic progression. *Publ. Math. Debrecen*, 74(1-2):215–232, 2009.

[50] G. Hanrot, N. Saradha, and T. N. Shorey. Almost perfect powers in consecutive integers. *Acta Arith.*, 99(1):13–25, 2001.

[51] H. Harborth, A. Kemnitz, and N. Robbins. Non-existence of Fibonacci triangles. *Congr. Numer.*, 114:29–31, 1996. Twenty-fifth Manitoba Conference on Combinatorial Mathematics and Computing (Winnipeg, MB, 1995).

[52] N. Hirata-Kohno, S. Laishram, T. N. Shorey, and R. Tijdeman. An extension of a theorem of Euler. *Acta Arith.*, 129(1):71–102, 2007.

[53] Péter Kiss. On the number of solutions of the Diophantine equation $\binom{x}{p} = \binom{y}{2}$. *Fibonacci Quart.*, 26(2):127–130, 1988.

[54] Chao Ko. On the Diophantine equation $x^2 = y^n + 1$, $xy \neq 0$. *Sci. Sinica*, 14:457–460, 1965.

[55] Shanta Laishram. An estimate for the length of an arithmetic progression the product of whose terms is almost square. *Publ. Math. Debrecen*, 68(3-4):451–475, 2006.

[56] Shanta Laishram and T. N. Shorey. The equation $n(n+d)\cdots(n+(k-1)d) = by^2$ with $\omega(d) \leq 6$ or $d \leq 10^{10}$. *Acta Arith.*, 129(3):249–305, 2007.

[57] Shanta Laishram, T. N. Shorey, and Szabolcs Tengely. Squares in products in arithmetic progression with at most one term omitted and common difference a prime power. *Acta Arith.*, 135(2):143–158, 2008.

[58] V.A. Lebesgue. Sur l'impossibilité en nombres entiers de l'équation $x^m = y^2 + 1$. *Nouv. Annal. des Math.*, 9:178–181, 1850.

[59] D. A. Lind. The quadratic field $Q(\sqrt{5})$ and a certain Diophantine equation. *Fibonacci Quart.*, 6(3):86–93, 1968.

[60] F. Luca. On a Diophantine equation. *Bull. Austral. Math. Soc.*, 61(2):241–246, 2000.

[61] F. Luca. On the equation $x^2 + 2^a \cdot 3^b = y^n$. *Int. J. Math. Math. Sci.*, 29(4):239–244, 2002.

[62] F. Luca, Sz. Tengely, and A. Togbé. On the diophantine equation $x^2 + c = 4y^n$. *Ann. Sci. Math. Québec*, 33(2):171–184, 2009.

[63] R. Marszałek. On the product of consecutive elements of an arithmetic progression. *Monatsh. Math.*, 100(3):215–222, 1985.

[64] M. Mignotte. On the Diophantine equation $D_1x^2 + D_2^m = 4y^n$. *Portugal. Math.*, 54(4):457–460, 1997.

[65] M. Mignotte and B.M.M. De Weger. On the Diophantine equations $x^2 + 74 = y^5$ and $x^2 + 86 = y^5$. *Glasgow Math. J.*, 38:77–85, 1996.

[66] M. Mignotte and A. Pethő. On the Diophantine equation $x^p - x = y^q - y$. *Publ. Mat.*, 43(1):207–216, 1999.

[67] L. J. Mordell. On the integer solutions of $y(y+1) = x(x+1)(x+2)$. *Pacific J. Math.*, 13:1347–1351, 1963.

[68] L. J. Mordell. *Diophantine equations*. Pure and Applied Mathematics, Vol. 30. Academic Press, London, 1969.

[69] Anirban Mukhopadhyay and T. N. Shorey. Almost squares in arithmetic progression. III. *Indag. Math. (N.S.)*, 15(4):523–533, 2004.

[70] F. S. A. Muriefah. On the Diophantine equation $px^2 + 3^n = y^p$. *Tamkang J. Math.*, 31(1):79–84, 2000.

[71] F. S. A. Muriefah. On the Diophantine equation $Ax^2 + 2^{2m} = y^n$. *Int. J. Math. Math. Sci.*, 25(6):373–381, 2001.

[72] F. S. A. Muriefah and S. A. Arif. On a Diophantine equation. *Bull. Austral. Math. Soc.*, 57(2):189–198, 1998.

[73] F. S. A. Muriefah and S. A. Arif. The Diophantine equation $x^2+5^{2k+1} = y^n$. *Indian J. Pure Appl. Math.*, 30(3):229–231, 1999.

[74] F. S. A. Muriefah and S. A. Arif. The Diophantine equation $x^2 + q^{2k} = y^n$. *Arab. J. Sci. Eng. Sect. A Sci.*, 26(1):53–62, 2001.

[75] Richard Obláth. Über das Produkt fünf aufeinander folgender Zahlen in einer arithmetischen Reihe. *Publ. Math. Debrecen*, 1:222–226, 1950.

[76] N. Petulante and I. Kaja. How to generate all integral triangles containing a given angle. *Int. J. Math. Math. Sci.*, 24(8):569–572, 2000.

[77] I. Pink. On the Diophantine equation $x^2+(p_1^{z_1}\dots p_s^{z_s})^2 = 2y^n$. *Publ. Math. Debrecen*, 65(1-2):205–213, 2004.

[78] Ákos Pintér. A note on the Diophantine equation $\binom{x}{4} = \binom{y}{2}$. *Publ. Math. Debrecen*, 47(3-4):411–415, 1995.

[79] Dimitrios Poulakis. Solutions entières de l'équation $Y^m = f(X)$. *Sém. Théor. Nombres Bordeaux (2)*, 3(1):187–199, 1991.

[80] O. Rigge. über ein diophantisches problem. In *9th Congress Math. Scand.*, pages 155–160. Mercator 1939, Helsingfors 1938.

[81] J. W. Sander. Rational points on a class of superelliptic curves. *J. London Math. Soc. (2)*, 59(2):422–434, 1999.

[82] N. Saradha. On perfect powers in products with terms from arithmetic progressions. *Acta Arith.*, 82(2):147–172, 1997.

[83] N. Saradha. Squares in products with terms in an arithmetic progression. *Acta Arith.*, 86(1):27–43, 1998.

[84] N. Saradha and T. N. Shorey. Almost perfect powers in arithmetic progression. *Acta Arith.*, 99(4):363–388, 2001.

[85] N. Saradha and T. N. Shorey. Almost squares and factorisations in consecutive integers. *Compositio Math.*, 138(1):113–124, 2003.

[86] N. Saradha and T. N. Shorey. Almost squares in arithmetic progression. *Compositio Math.*, 138(1):73–111, 2003.

[87] N. Saradha and T. N. Shorey. Contributions towards a conjecture of Erdős on perfect powers in arithmetic progression. *Compos. Math.*, 141(3):541–560, 2005.

[88] Wolfgang M. Schmidt. Integer points on curves of genus 1. *Compositio Math.*, 81(1):33–59, 1992.

[89] Ernst S. Selmer. The Diophantine equation $ax^3 + by^3 + cz^3 = 0$. *Acta Math.*, 85:203–362 (1 plate), 1951.

[90] T. N. Shorey. Perfect powers in products of arithmetical progressions with fixed initial term. *Indag. Math. (N.S.)*, 7(4):521–525, 1996.

[91] T. N. Shorey. Powers in arithmetic progression. In *A panorama of number theory or the view from Baker's garden (Zürich, 1999)*, pages 325–336. Cambridge Univ. Press, Cambridge, 2002.

[92] T. N. Shorey. Powers in arithmetic progressions. II. *Sūrikaisekikenkyūsho Kōkyūroku*, (1274):202–214, 2002. New aspects of analytic number theory (Japanese) (Kyoto, 2001).

[93] T. N. Shorey. Diophantine approximations, Diophantine equations, transcendence and applications. *Indian J. Pure Appl. Math.*, 37(1):9–39, 2006.

[94] T. N. Shorey. Powers in arithmetic progressions. III. In *The Riemann zeta function and related themes: papers in honour of Professor K. Ramachandra*, volume 2 of *Ramanujan Math. Soc. Lect. Notes Ser.*, pages 131–140. Ramanujan Math. Soc., Mysore, 2006.

[95] T. N. Shorey and R. Tijdeman. Perfect powers in products of terms in an arithmetical progression. *Compositio Math.*, 75(3):307–344, 1990.

[96] T. N. Shorey and R. Tijdeman. Perfect powers in products of terms in an arithmetical progression. II. *Compositio Math.*, 82(2):119–136, 1992.

[97] T. N. Shorey and R. Tijdeman. Perfect powers in products of terms in an arithmetical progression. III. *Acta Arith.*, 61(4):391–398, 1992.

[98] T. N. Shorey and R. Tijdeman. Some methods of Erdős applied to finite arithmetic progressions. In *The mathematics of Paul Erdős, I*, volume 13 of *Algorithms Combin.*, pages 251–267. Springer, Berlin, 1997.

[99] S. Siksek and M. Stoll. On a problem of Hajdu and Tengely. *ArXiv e-prints*, December 2009.

[100] David Singmaster. Repeated binomial coefficients and Fibonacci numbers. *Fibonacci Quart.*, 13(4):295–298, 1975.

[101] V. G. Sprindžuk. The arithmetic structure of integer polynomials and class numbers. *Trudy Mat. Inst. Steklov.*, 143:152–174, 210, 1977. Analytic number theory, mathematical analysis and their applications (dedicated to I. M. Vinogradov on his 85th birthday).

[102] Michael Stoll. Implementing 2-descent for Jacobians of hyperelliptic curves. *Acta Arith.*, 98(3):245–277, 2001.

[103] Roelof J. Stroeker and Benjamin M. M. de Weger. Elliptic binomial Diophantine equations. *Math. Comp.*, 68(227):1257–1281, 1999.

[104] Sz. Tengely. On the Diophantine equation $x^2 + q^{2m} = 2y^p$. *Acta Arith.*, 127(1):71–86, 2007.

[105] Sz. Tengely. Triangles with two integral sides. *Annales Mathematicae et Informaticae*, 34:89–95, 2007.

[106] Sz. Tengely. Note on the paper: „An extension of a theorem of Euler" [Acta Arith. 129 (2007), no. 1, 71–102; mr2326488] by N. Hirata-Kohno, S. Laishram, T. N. Shorey and R. Tijdeman. *Acta Arith.*, 134(4):329–335, 2008.

[107] Sz. Tengely. Note on the paper: „An extension of a theorem of Euler" [Acta Arith. 129 (2007), no. 1, 71–102; mr2326488] by N. Hirata-Kohno, S. Laishram, T. N. Shorey and R. Tijdeman. *Acta Arith.*, 134(4):329–335, 2008.

[108] A. Thue. Über Annäherungswerte algebraischer Zahlen. *J. Reine Angew Math.*, 135:284–305, 1909.

[109] R. Tijdeman. Diophantine equations and Diophantine approximations. In *Number theory and applications (Banff, AB, 1988)*, volume 265 of *NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci.*, pages 215–243. Kluwer Acad. Publ., Dordrecht, 1989.

[110] R. Tijdeman. Exponential Diophantine equations 1986–1996. In *Number theory (Eger, 1996)*, pages 523–539. de Gruyter, Berlin, 1998.

[111] J. B. Tunnell. A classical Diophantine problem and modular forms of weight 3/2. *Invent. Math.*, 72(2):323–334, 1983.

[112] Paul M. Voutier. An upper bound for the size of integral solutions to $Y^m = f(X)$. *J. Number Theory*, 53(2):247–271, 1995.

Cikkgyűjtemény

Contents

1

On the Diophantine equation $x^2 + q^{2m} = 2y^p$

*T*engely, Sz.,
Acta Arithmetica **127** (2007), 71–86.

Abstract

In this paper we consider the Diophantine equation $x^2 + q^{2m} = 2y^p$ where m, p, q, x, y are integer unknowns with $m > 0$, p and q are odd primes and $\gcd(x, y) = 1$. We prove that there are only finitely many solutions (m, p, q, x, y) for which y is not a sum of two consecutive squares. We study the above equation for fixed y and in particular solve the case $y = 17$ completely. We also study the equation for fixed q and resolve the equation for $q = 3$.

1.1 Introduction

There are many results in the literature concerning the Diophantine equation $Ax^2 + q_1^{z_1} \cdots q_s^{z_s} = By^n$, where A, B are given non-zero integers, $q_1, \ldots, q_s$ are given primes and $n, x, y, z_1, \ldots, z_s$ are integer unknowns with $n > 2, x$ and y coprime and non-negative, and $z_1, \ldots, z_s$ non-negative, see e.g. [1], [2], [3], [4], [5], [6], [7], [11], [12], [15], [18], [19], [20], [21], [22], [25]. Here the elegant result of Bilu, Hanrot and Voutier [10] on the existence of primitive divisors of Lucas and Lehmer numbers has turned out to be a very powerful tool. Using this result Luca [19] solved completely the Diophantine equation $x^2+2^a3^b = y^n$. Le [17] obtained necessary conditions for the solutions of the equation $x^2 + q^2 = y^n$ in positive integers x, y, n with $\gcd(x, y) = 1, q$ prime and $n > 2$. He also determined all solutions of this equation for $q < 100$. In [25] Pink considered the equation $x^2 + (q_1^{z_1} \cdots q_s^{z_s})^2 = 2y^n$, and gave an explicit upper bound for n depending only on $\max q_i$ and s. The equation $x^2 + 1 = 2y^n$ was solved by Cohn [14]. Pink and

Tengely [26] considered the equation $x^2 + a^2 = 2y^n$. They gave an upper bound for the exponent n depending only on a, and completely resolved the equation with $1 \leq a \leq 1000$ and $3 \leq n \leq 80$.

In the present paper we study the equation $x^2 + q^{2m} = 2y^p$ where m, p, q, x and y are integer unknowns with $m > 0$, p and q odd primes and x and y coprime. In Theorem 1.2.1 we show that all but finitely many solutions are of a special type. Proposition 1.2.1 provides bounds for p. Theorem 1.3.1 deals with the case of fixed y, we completely resolve the equation $x^2 + q^{2m} = 2 \cdot 17^p$. Theorem 1.4.1 deals with the case of fixed q. In Propositions 3 and 4 certain high degree Thue equations are solved related to primes $p < 1000$. The proof of Proposition 4 is due to Hanrot. It is proved that if the Diophantine equation $x^2 + 3^{2m} = 2y^p$ with $m > 0$ and p prime admits a coprime integer solution (x, y), then $(x, y, m, p) \in \{(13, 5, 2, 3), (79, 5, 1, 5), (545, 53, 3, 3)\}$. It means that the equation $x^2 + 3^m = 2y^p$ in coprime integers x, y and prime p is completely solved because solutions clearly do not exist when m is odd.

1.2 A finiteness result

Consider the Diophantine equation

$$x^2 + q^{2m} = 2y^p, \tag{1.1}$$

where $x, y \in \mathbb{N}$ with $\gcd(x, y) = 1, m \in \mathbb{N}$ and p, q are odd primes and $\mathbb{N}$ denotes the set of positive integers. Since the case $m = 0$ was solved by Cohn [14] (he proved that the equation has only the solution $x = y = 1$ in positive integers) we may assume without loss of generality that $m > 0$. If $q = 2$, then it follows from $m > 0$ that $\gcd(x, y) > 1$, therefore we may further assume that q is odd.

Theorem 1.2.1. *There are only finitely many solutions* (x, y, m, q, p) *of* (7.1) *with* $\gcd(x, y) = 1, x, y \in \mathbb{N}$, *such that* y *is not a sum of two consecutive squares,* $m \in \mathbb{N}$ *and* $p > 3, q$ *are odd primes.*

Remark. The question of finiteness if y is a sum of two consecutive squares is interesting. The following examples, all for $m = 1$, show that very large solutions exist.

y	p	q
5	5	79
5	7	307
5	13	42641
5	29	1811852719
5	97	229935753703632302559452847176639 9
13	7	11003
13	13	13394159
13	101	22480363734265533023633690933103706711211958360218401799 9
25	11	69049993
25	47	37829305586052202725400160492296 7
41	31	4010333845016060415260441

All solutions of (7.1) with small q^m and $x > q^{2m}$ have been determined in [27].

Lemma 1.2.1. *Let q be an odd prime and $m \in \mathbb{N} \cup \{0\}$ such that $3 \leq q^m \leq 501$. If there exist $(x, y) \in \mathbb{N}^2$ with $\gcd(x, y) = 1$ and an odd prime p such that (7.1) holds, then*

$$(x, y, q, m, p) \in$$
$$\big\{(3,5,79,1,5),(9,5,13,1,3),(13,5,3,2,3),(55,13,37,1,3),$$
$$(79,5,3,1,5),(99,17,5,1,3),(161,25,73,1,3),(249,5,307,1,7),$$
$$(351,41,11,2,3),(545,53,3,3,3),(649,61,181,1,3),(1665,113,337,1,3),$$
$$(2431,145,433,1,3),(5291,241,19,1,3),(275561,3361,71,1,3)\big\}.$$

Proof. This result follows from Corollary 1 in [27]. The solutions with $x \leq q^{2m}$ can be found by an exhaustive search. □

We introduce some notation. Put

$$\delta_4 = \begin{cases} 1 \text{ if } p \equiv 1 \pmod 4, \\ -1 \text{ if } p \equiv 3 \pmod 4. \end{cases} \tag{1.2}$$

and

$$\delta_8 = \begin{cases} 1 \text{ if } p \equiv 1 \text{ or } 3 \pmod 8, \\ -1 \text{ if } p \equiv 5 \text{ or } 7 \pmod 8. \end{cases} \tag{1.3}$$

Since $\mathbb{Z}[i]$ is a unique factorization domain, (7.1) implies the existence of integers u, v with $y = u^2 + v^2$ such that

$$\begin{aligned} x &= \Re((1+i)(u+iv)^p) =: F_p(u,v), \\ q^m &= \Im((1+i)(u+iv)^p) =: G_p(u,v). \end{aligned} \tag{1.4}$$

Here F_p and G_p are homogeneous polynomials in $\mathbb{Z}[X, Y]$.

Lemma 1.2.2. *Let F_p, G_p be the polynomials defined by (1.4). We have*

$$\begin{aligned} (u - \delta_4 v) &\mid F_p(u,v), \\ (u + \delta_4 v) &\mid G_p(u,v). \end{aligned}$$

Proof. This is Lemma 3 in [27]. □

Lemma 1.2.2 and (1.4) imply that there exists a $k \in \{0, 1, \ldots, m\}$ such that either

$$\begin{aligned} u + \delta_4 v &= q^k, \\ H_p(u, v) &= q^{m-k}, \end{aligned} \tag{1.5}$$

or

$$\begin{aligned} u + \delta_4 v &= -q^k, \\ H_p(u, v) &= -q^{m-k}, \end{aligned} \tag{1.6}$$

where $H_p(u, v) = \frac{G_p(u,v)}{u+\delta_4 v}$.

For all solutions with large q^m we derive an upper bound for p in case of $k = m$ in (1.5) or (1.6) and in case of $q = p$.

Proposition 1.2.1. *If* (7.1) *admits a relatively prime solution* $(x, y) \in \mathbb{N}^2$ *then we have*

$$\begin{aligned} &p \leq 3803 \text{ if } u + \delta_4 v = \pm q^m, q^m \geq 503, \\ &p \leq 3089 \text{ if } p = q, \\ &p \leq 1309 \text{ if } u + \delta_4 v = \pm q^m, m \geq 40, \\ &p \leq 1093 \text{ if } u + \delta_4 v = \pm q^m, m \geq 100, \\ &p \leq 1009 \text{ if } u + \delta_4 v = \pm q^m, m \geq 250. \end{aligned}$$

We shall use the following lemmas in the proof of Proposition 1.2.1. The first result is due to Mignotte [10, Theorem A.1.3]. Let α be an algebraic number, whose minimal polynomial over $\mathbb{Z}$ is $A\prod_{i=1}^{d}(X - \alpha^{(i)})$. The absolute logarithmic height of α is defined by

$$h(\alpha) = \frac{1}{d}\left(\log|A| + \sum_{i=1}^{d} \log \max(1, |\alpha^{(i)}|)\right).$$

Lemma 1.2.3. *Let* α *be a complex algebraic number with* $|\alpha| = 1$, *but not a root of unity, and* $\log \alpha$ *the principal value of the logarithm. Put* $D = [\mathbb{Q}(\alpha) : \mathbb{Q}]/2$. *Consider the linear form*

$$\Lambda = b_1 i\pi - b_2 \log \alpha,$$

where b_1, b_2 are positive integers. Let λ be a real number satisfying $1.8 \le \lambda < 4$, and put

$$\rho = e^{\lambda}, \quad K = 0.5\rho\pi + Dh(\alpha), \quad B = \max(13, b_1, b_2),$$
$$t = \frac{1}{6\pi\rho} - \frac{1}{48\pi\rho(1+2\pi\rho/3\lambda)}, \quad T = \left(\frac{1/3+\sqrt{1/9+2\lambda t}}{\lambda}\right)^2,$$
$$H = \max\Big\{3\lambda, D\left(\log B + \log\left(\frac{1}{\pi\rho}+\frac{1}{2K}\right) - \log\sqrt{T} + 0.886\right) +$$
$$+\frac{3\lambda}{2} + \frac{1}{T}\left(\frac{1}{6\rho\pi}+\frac{1}{3K}\right) + 0.023\Big\}.$$

Then

$$\log|\Lambda| > -(8\pi T\rho\lambda^{-1}H^2 + 0.23)K - 2H - 2\log H + 0.5\lambda + 2\log\lambda - (D+2)\log 2.$$

The next result can be found as Corollary 3.12 at p. 41 of [23].

Lemma 1.2.4. *If $\Theta \in 2\pi\mathbb{Q}$, then the only rational values of the tangent and the cotangent functions at Θ are $0, \pm 1$.*

Proof of Proposition 1.2.1. Without loss of generality we assume that $p > 1000$ and $q^m \ge 503$. We give the proof of Proposition 1.2.1 in the case $u + \delta_4 v = \pm q^m, q^m \ge 503$, the proofs of the remaining four cases being analogous. From $u + \delta_4 v = \pm q^m$ we get

$$\frac{503}{2} \le \frac{q^m}{2} \le \frac{|u|+|v|}{2} \le \sqrt{\frac{u^2+v^2}{2}} = \sqrt{\frac{y}{2}},$$

which yields that $y \ge \frac{q^{2m}}{2} > 126504$. Hence

$$\left|\frac{x+q^m i}{x-q^m i} - 1\right| = \frac{2\cdot q^m}{\sqrt{x^2+q^{2m}}} \le \frac{2\sqrt{y}}{y^{p/2}} = \frac{2}{y^{\frac{p-1}{2}}}. \tag{1.7}$$

We have

$$\frac{x+q^m i}{x-q^m i} = \frac{(1+i)(u+iv)^p}{(1-i)(u-iv)^p} = i\left(\frac{u+iv}{u-iv}\right)^p. \tag{1.8}$$

If $\left|i\left(\frac{u+iv}{u-iv}\right)^p - 1\right| > \frac{1}{3}$ then $6 > y^{\frac{p-1}{2}}$, which yields a contradiction with $p > 1000$ and $y > 126504$. Thus $\left|i\left(\frac{u+iv}{u-iv}\right)^p - 1\right| \le \frac{1}{3}$. Since $|\log z| \le 2|z-1|$ for $|z-1| \le \frac{1}{3}$, we obtain

$$\left|i\left(\frac{u+iv}{u-iv}\right)^p - 1\right| \ge \frac{1}{2}\left|\log i\left(\frac{u+iv}{u-iv}\right)^p\right|. \tag{1.9}$$

Suppose first that $\alpha := \delta_4 \left(\frac{u-iv}{-v+iu}\right)^\sigma$ is a root of unity for some $\sigma \in \{-1, 1\}$. Then

$$\left(\frac{u-iv}{-v+iu}\right)^\sigma = \frac{-2uv}{u^2+v^2} + \frac{\sigma(-u^2+v^2)}{u^2+v^2}i = \pm\alpha = \exp\left(\frac{2\pi ij}{n}\right),$$

for some integers j, n with $0 \leq j \leq n-1$. Therefore

$$\tan\left(\frac{2\pi j}{n}\right) = \frac{\sigma(-u^2+v^2)}{-2uv} \in \mathbb{Q} \text{ or } (u,v) = (0,0).$$

The latter case is excluded. Hence, by Lemma 1.2.4, $\frac{u^2-v^2}{2uv} \in \{0, 1, -1\}$. This implies that $|u| = |v|$, but this is excluded by the requirement that the solutions x, y of (7.1) are relatively prime, but $y > 126504$. Therefore α is not a root of unity.

Note that α is irrational, $|\alpha| = 1$, and it is a root of the polynomial $(u^2 + v^2)X^2 + 4\delta_4 uvX + (u^2 + v^2)$. Therefore $h(\alpha) = \frac{1}{2}\log y$.

Choose $l \in \mathbb{Z}$ such that $|p\log(i^{\delta_4}\frac{u+iv}{u-iv}) + 2l\pi i|$ is minimal, where logarithms have their principal values. Then $|2l| \leq p$. Consider the linear form in two logarithms ($\pi i = \log(-1)$)

$$\Lambda = 2|l|\pi i - p\log\alpha. \tag{1.10}$$

If $l = 0$ then by Liouville's inequality and Lemma 1 of [29],

$$|\Lambda| \geq |p\log\alpha| \geq |\log\alpha| \geq 2^{-2}\exp(-2h(\alpha)) \geq \exp(-8(\log 6)^3 h(\alpha)). \tag{1.11}$$

From (1.7) and (1.11) we obtain

$$\log 4 - \frac{p-1}{2}\log y \geq \log|\Lambda| \geq -4(\log 6)^3 \log y.$$

Hence $p \leq 47$. Thus we may assume without loss of generality that $l \neq 0$.

We apply Lemma 1.2.3 with $\sigma = \text{sign}(l), \alpha = \delta_4(\frac{u-iv}{-v+iu})^\sigma, b_1 = 2|l|$ and $b_2 = p$. Set $\lambda = 1.8$. We have $D = 1$ and $B = p$. By applying (1.7)-(1.10) and Lemma 1.2.3 we obtain

$$\log 4 - \frac{p-1}{2}\log y \geq \log|\Lambda| \geq -(13.16H^2 + 0.23)K - 2H - 2\log H - 0.004.$$

We have

$$\begin{aligned}
&15.37677 \leq K < 9.5028 + \frac{1}{2}\log y,\\
&0.008633 < t < 0.008634,\\
&0.155768 < T < 0.155769,\\
&H < \log p + 2.270616,\\
&\log y > 11.74803,
\end{aligned}$$

From the above inequalities we conclude that $p \leq 3803$. □

The following lemma gives a more precise description of the polynomial H_p, the notation $p \mod 4$ is defined as the number from the set $\{0,1,2,3\}$ that is congruent to p modulo 4.

Lemma 1.2.5. *The polynomial $H_p(\pm q^k - \delta_4 v, v)$ has degree $p-1$ and*

$$H_p(\pm q^k - \delta_4 v, v) = \pm\delta_8 2^{\frac{p-1}{2}} p v^{p-1} + q^k p \widehat{H}_p(v) + q^{k(p-1)},$$

where $\widehat{H}_p \in \mathbb{Z}[X]$ has degree $< p-1$. The polynomial $H_p(X,1) \in \mathbb{Z}[X]$ is irreducible and

$$H_p(X,1) = \prod_{\substack{k=0 \\ k \neq k_0}}^{p-1} \left(X - \tan\frac{(4k+3)\pi}{4p} \right),$$

where $k_0 = \left[\frac{p}{4}\right](p \mod 4)$.

Proof. By definition we have

$$H_p(u,v) = \frac{G_p(u,v)}{u+\delta_4 v} = \frac{(1+i)(u+iv)^p - (1-i)(u-iv)^p}{2i(u+\delta_4 v)}. \tag{1.12}$$

Hence

$$H_p(\pm q^k - \delta_4 v, v) = \frac{(1+i)(\pm q^k + (i-\delta_4)v)^p - (1-i)(\pm q^k + (-i-\delta_4)v)^p}{\pm 2 i q^k}.$$

Therefore the coefficient of v^p is $(1+i)(-\delta_4+i)^p + (1-i)(\delta_4+i)^p$. If $\delta_4 = 1$, then it equals $-2(-1+i)^{p-1} + 2(1+i)^{p-1} = -2(-4)^{\frac{p-1}{4}} + 2(-4)^{\frac{p-1}{4}} = 0$, since $p \equiv 1 \pmod 4$. If $\delta_4 = -1$, then it equals $(1+i)^{p+1} - (-1+i)^{p+1} = (-4)^{\frac{p+1}{4}} - (-4)^{\frac{p+1}{4}} = 0$. Similarly the coefficient of v^{p-1} is $\pm\frac{(1+i)(\delta_4-i)^{p-1} - (1-i)(\delta_4+i)^{p-1}}{2i} p = \pm\delta_8 2^{\frac{p-1}{2}} p$. It is easy to see that the constant is $q^{k(p-1)}$. The coefficient of v^t for $t = 1, \ldots, p-2$ is $\pm\binom{p}{t}(q^k)^{p-t-1} c_t$, where c_t is a power of 2. The irreducibility of $H_p(X,1)$ follows from the fact that $H_p(X-\delta_4, 1)$ satisfies Eisenstein's irreducibility criterion. The last statement of the lemma is a direct consequence of Lemma 4 from [27]. □

Remark. Schinzel's Hypothesis H says that if $P_1(X), \ldots, P_r(X) \in \mathbb{Z}[X]$ are irreducible polynomials with positive leading coefficients such that no integer $l > 1$ divides $P_i(x)$ for all integers x for some $i \in \{1, \ldots, k\}$, then there exist infinitely many positive integers x such that $P_1(x), \ldots, P_r(x)$ are simultaneously prime. Since $\pm H_p(\pm 1 - \delta_4 v, v)$ is irreducible having constant term ± 1, the Hypothesis implies that in case of $k = 0, m = 1$ there are infinitely many solutions of (1.5) and (1.6). Hence there are infinitely many solutions of (7.1).

Lemma 1.2.6. *If there exists a $k \in \{0, 1, \ldots, m\}$ such that* (1.5) *or* (1.6) *has a solution $(u,v) \in \mathbb{Z}^2$ with $\gcd(u,v) = 1$, then either $k = 0$ or $(k = m, p \neq q)$ or $(k = m-1, p = q)$.*

Proof. Suppose $0 < k < m$. It follows from Lemma 1.2.5 that $q \mid \pm\delta_8 2^{\frac{p-1}{2}} p v^{p-1}$. If $q \neq p$, we obtain that $q \mid v$ and $q \mid u$, which is a contradiction with $\gcd(u, v) = 1$. Thus $k = 0$ or $k = m$. If $p = q$, then from Lemma 1.2.5 and (1.5), (1.6) we get

$$\pm\delta_8 2^{\frac{p-1}{2}} v^{p-1} + p^k \widehat{H}_p(v) + p^{k(p-1)-1} = \pm p^{m-k-1}.$$

Therefore $k = 0$ or $k = m - 1$. □

Now we are in the position to prove Theorem 1.2.1.

Proof of Theorem 1.2.1. By Lemma 1.2.6 we have that $k = 0, m-1$ or $k = m$. If $k = 0$, then $u+\delta_4 v = \pm 1$ and y is a sum of two consecutive squares. If $k = m-1$, then $p = q$. Hence $u + \delta_4 v = \pm p^{m-1}$ which implies that $y \geq \frac{p^{2(m-1)}}{2} \geq \frac{p^2}{2}$. From Proposition 1.2.1 we obtain that $p \leq 3089$. We recall that $H_p(u, v)$ is an irreducible polynomial of degree $p - 1$. Thus we have only finitely many Thue equations (if $p > 3$)

$$H_p(u, v) = \pm p.$$

By a result of Thue [28] we know that for each p there are only finitely many integer solutions, which proves the statement.

Let $k = m$. Here we have $u + \delta_4 v = \pm q^m$ and $H_p(\pm q^m - \delta_4 v, v) = \pm 1$. If $q^m \leq 501$ then there are only finitely many solutions which are given in Lemma 1.2.1. We have computed an upper bound for p in Proposition 1.2.1 when $q^m \geq 503$. This leads to finitely many Thue equations

$$H_p(u, v) = \pm 1.$$

From Thue's result it follows that there are only finitely many integral solutions (u, v) for any fixed p, which implies the remaining part of the theorem. □

1.3 Fixed y

First we consider (7.1) with given y which is not a sum of two consecutive squares. Since $y = u^2 + v^2$ there are only finitely many possible pairs $(u, v) \in \mathbb{Z}^2$. Among these pairs we have to select those for which $u \pm v = \pm q^{m_0}$, for some prime q and for some integer m_0. Thus there are only finitely many pairs (q, m_0). The method of [27] makes it possible to compute (at least for moderate q and m_0) all solutions of $x^2 + q^{2m_0} = 2y^p$ even without knowing y. Let us consider the concrete example $y = 17$.

Theorem 1.3.1. *The only solution (m, p, q, x) in positive integers m, p, q, x with p and q odd primes of the equation $x^2 + q^{2m} = 2 \cdot 17^p$ is $(1, 3, 5, 99)$.*

Proof. Note that 17 cannot be written as a sum of two consecutive squares. From $y = u^2 + v^2$ we obtain that q is 3 or 5 and $m = 1$. This implies that 17 does not divide x. We are left with the equations

$$x^2 + 3^2 = 2 \cdot 17^p,$$
$$x^2 + 5^2 = 2 \cdot 17^p.$$

From Lemma 1.2.1 we see that the first equation has no solutions and the second only the solution $(p, x) = (3, 99)$. □

1.4 Fixed q

If m is small, then one can apply the method of [27] to obtain all solutions. Proposition 1.2.1 provides an upper bound for p in case $u+\delta_4 v = \pm q^m$. Therefore it is sufficient to resolve the Thue equations

$$H_p(u, v) = \pm 1$$

for primes less than the bound. In practice this is a difficult job but in some special cases there exist methods which work, see [8], [9], [10], [16]. Lemma 1.4.1 shows that we have a cyclotomic field in the background just as in [10]. Probably the result of the following lemma is in the literature, but we have not found a reference. We thank Peter Stevenhagen for the short proof.

Lemma 1.4.1. *For any positive integer M denote by ζ_M a primitive Mth root of unity. If α is a root of $H_p(X, 1)$ for some odd prime p, then $\mathbb{Q}(\zeta_p + \overline{\zeta}_p) \subset \mathbb{Q}(\alpha) \cong \mathbb{Q}(\zeta_{4p} + \overline{\zeta}_{4p})$.*

Proof. Since $\tan z = \frac{1}{i}\frac{\exp(iz)-\exp(-iz)}{\exp(iz)+\exp(-iz)}$, we can write $\alpha = \tan(\frac{(4k+3)\pi}{4p})$ as

$$\frac{1}{i}\frac{\zeta_{8p}^{4k+3} - \zeta_{8p}^{-4k-3}}{\zeta_{8p}^{4k+3} + \zeta_{8p}^{-4k-3}} = -\zeta_4 \frac{\zeta_{4p}^{4k+3} - 1}{\zeta_{4p}^{4k+3} + 1} \in \mathbb{Q}(\zeta_{4p}).$$

Since it is invariant under complex conjugation, α is an element of $\mathbb{Q}(\zeta_{4p} + \overline{\zeta}_{4p})$. We also know that $[\mathbb{Q}(\zeta_{4p} + \overline{\zeta}_{4p}) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}] = p - 1$, thus $\mathbb{Q}(\zeta_{4p} + \overline{\zeta}_{4p}) \cong \mathbb{Q}(\alpha)$. The claimed inclusion follows from the fact that $\zeta_p + \overline{\zeta}_p$ can be expressed easily in terms of $\zeta_{4p} + \overline{\zeta}_{4p}$. □

It is important to remark that the Thue equations $H_p(u, v) = \pm 1$ do not depend on q. By combining the methods of composite fields [9] and non-fundamental units [16] for Thue equations we may rule out some cases completely. If the

method applies it remains to consider the cases $u + \delta_4 v = \pm 1$ and $p = q$. If q is fixed one can follow as a strategy to eliminate large primes p. Here we use the fact that when considering the Thue equation

$$H_p(u, v) = \pm 1. \tag{1.13}$$

we are looking for integer solutions (u, v) for which $u + \delta_4 v$ is a power of q. Let w be a positive integer relatively prime to q. Then the set $S(q, w) = \{q^m \bmod w : m \in \mathbb{N}\}$ has $\mathrm{ord}_w(q)$ elements. Let

$$L(p, q, w) = \\ \left\{s \in \{0, 1, \ldots, \mathrm{ord}_w(q)\} : H_p(q^s - \delta_4 v, v) = 1 \text{ has a solution modulo } w\right\}.$$

We search for numbers $w_1, \ldots, w_N$ such that $\mathrm{ord}_{w_1}(q) = \ldots = \mathrm{ord}_{w_N}(q) =: w$, say. Then

$$m_0 \mod w \in L(p, q, w_1) \cap \ldots \cap L(p, q, w_N),$$

where $m_0 \mod w$ denotes the smallest non-negative integer congruent to m modulo w. Hopefully this will lead to some restrictions on m. As we saw before the special case $p = q$ leads to a Thue equation $H_p(u, v) = \pm p$ and the previously mentioned techniques may apply even for large primes. In case of $u + \delta_4 v = \pm 1$ one encounters a family of superelliptic equations $H_p(\pm 1 - \delta_4 v, v) = \pm q^m$. We will see that sometimes it is possible to solve these equations completely using congruence conditions only.

From now on we consider (7.1) with $q = 3$, that is

$$x^2 + 3^{2m} = 2y^p. \tag{1.14}$$

The equation $x^2 + 3 = y^n$ was completely resolved by Cohn [13]. Arif and Muriefah [2] found all solutions of the equation $x^2 + 3^{2m+1} = y^n$. There is one family of solutions, given by $(x, y, m, n) = (10 \cdot 3^{3t}, 7 \cdot 3^{2t}, 5 + 6t, 3)$. Luca [18] proved that all solutions of the equation $x^2 + 3^{2m} = y^n$ are of the form $x = 46 \cdot 3^{3t}, y = 13 \cdot 3^{2t}, m = 4 + 6t, n = 3$.

Remark. We note that equation (1.14) with odd powers of 3 is easily solvable. From $x^2 + 3^{2m+1} = 2y^p$ we get

$$4 \equiv 2y^p \pmod 8,$$

hence $p = 1$ which contradicts the assumption that p is prime.

Let us first treat the special case $p = q = 3$. By (1.4) and Lemma 1.2.2 we have

$$\begin{aligned} x &= F_3(u, v) = (u + v)(u^2 - 4uv + v^2), \\ 3^m &= G_3(u, v) = (u - v)(u^2 + 4uv + v^2). \end{aligned}$$

Therefore there exists an integer k with $0 \leq k \leq m$, such that

$$\begin{aligned} u - v &= \pm 3^k, \\ u^2 + 4uv + v^2 &= \pm 3^{m-k}. \end{aligned}$$

Hence we have

$$6v^2 \pm 6(3^k)v + 3^{2k} = \pm 3^{m-k}.$$

Both from $k = m$ and from $k = 0$ it follows easily that $k = m = 0$. This yields the solutions $(x, y) = (\pm 1, 1)$.

If $k = m - 1 > 0$, then $3 \mid 2v^2 \pm 1$. Thus one has to resolve the system of equations

$$\begin{aligned} u - v &= -3^{m-1}, \\ u^2 + 4uv + v^2 &= -3. \end{aligned}$$

The latter equation has infinitely many solutions parametrized by

$$\begin{aligned} u &= \frac{-\varepsilon}{2}\left((2+\sqrt{3})^{t-1} + (2-\sqrt{3})^{t-1}\right), \\ v &= \frac{\varepsilon}{2}\left((2+\sqrt{3})^{t} + (2-\sqrt{3})^{t}\right), \end{aligned}$$

where $t \in \mathbb{N}, \varepsilon \in \{-1, 1\}$. Hence we get that

$$\frac{1}{2}\left((3+\sqrt{3})(2+\sqrt{3})^{t-1} + (3-\sqrt{3})(2-\sqrt{3})^{t-1}\right) = \pm 3^{m-1}. \tag{1.15}$$

The left-hand side of (1.15) is the explicit formula of the linear recursive sequence defined by $r_0 = r_1 = 3, r_t = 4r_{t-1} - r_{t-2}, t \geq 2$. One can easily check that

$$r_t \equiv 0 \pmod{27} \;\Leftrightarrow\; t \equiv 5 \pmod{9} \;\Leftrightarrow\; r_t \equiv 0 \pmod{17}.$$

Thus $m = 2$ or $m = 3$. If $m = 2, k = 1$, then we obtain the solution $(x, y) = (13, 5)$, if $m = 3, k = 2$, then we get $(x, y) = (545, 53)$. From now on we assume that $p > 3$.

As we mentioned, sometimes it is possible to handle the case $k = 0$ using congruence arguments only. In case of $q = 3$ it works.

Lemma 1.4.2. *In case of $q = 3$ there is no solution of* (1.5) *and* (1.6) *with $k = 0$.*

Proof. We give a proof for (1.5) which also works for (1.6). In case of (1.5) if $k = 0$, then $u = 1 - \delta_4 v$. Observe that by (1.12)

- if $v \equiv 0 \pmod 3$, then $H_p(1 - \delta_4 v, v) \equiv 1 \pmod 3$,

- if $v \equiv 1 \pmod 3$ and $p \equiv 1 \pmod 4$, then $H_p(1 - \delta_4 v, v) \equiv 1 \pmod 3$,
- if $v \equiv 1 \pmod 3$ and $p \equiv 3 \pmod 4$, then $H_p(1 - \delta_4 v, v) \equiv \pm 1 \pmod 3$,
- if $v \equiv 2 \pmod 3$ and $p \equiv 1 \pmod 4$, then $H_p(1 - \delta_4 v, v) \equiv \pm 1 \pmod 3$,
- if $v \equiv 2 \pmod 3$ and $p \equiv 3 \pmod 4$, then $H_p(1 - \delta_4 v, v) \equiv 1 \pmod 3$.

Thus $H_p(1 - \delta_4 v, v) \not\equiv 0 \pmod 3$. Therefore there is no $v \in \mathbb{Z}$ such that $H_p(1 - \delta_4 v, v) = 3^m$, as should be the case by (1.5) and (1.6). □

Finally we investigate the remaining case, that is $u + \delta_4 v = 3^m$. We remark that $u + \delta_4 v = -3^m$ is not possible because from (1.6) and Lemma 1.2.5 we obtain $-1 \equiv H_p(-3^m - \delta_4 v, v) \equiv 3^{k(p-1)} \equiv 1 \pmod p$.

Proposition 1.4.1. *If there is a coprime solution* $(u, v) \in \mathbb{Z}^2$ *of* (1.5) *with* $q = 3, k = m$, *then* $p \equiv 5$ *or* $11 \pmod{24}$.

Proof. In case of $k = m$ we have, by (1.5) and Lemma 1.2.5,

$$H_p(3^m - \delta_4 v, v) = \delta_8 2^{\frac{p-1}{2}} p v^{p-1} + 3^m p \widehat{H}_p(v) + 3^{m(p-1)} = 1. \tag{1.16}$$

Therefore

$$\delta_8 2^{\frac{p-1}{2}} p \equiv 1 \pmod 3$$

and we get that $p \equiv 1, 5, 7, 11 \pmod{24}$. Since by Lemma 1.2.1 the only solution of the equation $x^2 + 3^{2m} = 2y^p$ with $1 \leq m \leq 5$ is given by $(x, y, m, p) \in \{(79, 5, 1, 5), (545, 53, 3, 3)\}$, we may assume without loss of generality that $m \geq 6$. To get rid of the classes 1 and 7 we work modulo 243. If $p = 8t + 1$, then from (1.16) we have

$$2^{4t}(8t + 1)v^{8t} \equiv 1 \pmod{243}.$$

It follows that $243 | t$ and the first prime of the appropriate form is 3889 which is larger than the bound we have for p. If $p = 8t + 7$, then

$$-2^{4t+3}(8t + 7)v^{8t+6} \equiv 1 \pmod{243}.$$

It follows that $t \equiv 60 \pmod{243}$ and it turns out that $p = 487$ is in this class, so we work modulo 3^6 to show that the smallest possible prime is larger than the bound we have for p. Here we have to resolve the case $m = 6$ using the method from [27]. This value of m is not too large so the method worked. We did not get any new solution. Thus $p \equiv 5$ or $11 \pmod{24}$. □

Proposition 1.4.2. *There exists no coprime integer solution* (x, y) *of* $x^2 + 3^{2m} = 2y^p$ *with* $m > 0$ *and* $p < 1000, p \equiv 5 \pmod{24}$ *or* $p \in \{131, 251, 491, 971\}$ *prime.*

Proof. To prove the theorem we resolve the Thue equations (1.13) for the given primes. In each case there is a small subfield, hence we can apply the method of [9]. We wrote a PARI [24] script to handle the computation. We note that if $p = 659$ or $p = 827$, then there is a degree 7 subfield, but the regulator is too large to get unconditional result. The same holds for $p = 419, 683, 947$, in which cases there is a degree 11 subfield. In the computation we followed the paper [9], but at the end we skipped the enumeration step. Instead we used the bound for $|x|$ given by the formula (34) at page 318. The summary of the computation is in Table 1. We obtained small bounds for $|u|$ in each case. It

Table 1.1: Summary of the computation (AMD64 Athlon 1.8GHz)

p	X_3	time	p	X_3	time	p	X_3	time	p	X_3	time	p	X_3	time
29	4	1s	173	2	6s	317	2	13s	557	2	27s	797	2	45s
53	3	2s	197	2	7s	389	2	25s	653	2	33s	821	2	56s
101	2	3s	251	2	14s	461	2	22s	677	2	28s	941	2	62s
131	2	6s	269	2	14s	491	2	25s	701	2	37s	971	2	75s
149	2	7s	293	2	10s	509	2	23s	773	2	44s			

remained to find the integer solutions of the polynomial equations $H_p(u_0, v) = 1$ for the given primes with $|u_0| \leq X_3$. It turns out that there is no solution for which $u + \delta v = 3^m, m > 0$, and the statement follows. □

The remaining Thue equations related to the remaining primes ($p < 1000$) were solved by G. Hanrot.

Proposition 1.4.3 (G. Hanrot). *There exists no coprime integer solution* (x, y) *of* $x^2 + 3^{2m} = 2y^p$ *with* $m > 0$ *and*

$$p \in \{59, 83, 107, 179, 227, 347, 419, 443, 467, 563, 587, 659, 683, 827, 947\}.$$

Proof. By combining the effective methods of composite fields [9] and non-fundamental units [16] all Thue equations were solved related to the given primes. The computations were done using PARI. Most of the computation time is the time for $p - 1$ LLL-reductions in dimension 3 on a lattice with integer entries of size about the square of the Baker bound. The numerical precision required for the reduction step is 7700 in the worst case ($p = 587$). The summary of the computation is in Table 2. We got small bounds for $|u|$ in each case. There is no solution for which $u + \delta v = 3^m, m > 0$, and the statement follows. □

Table 1.2: Summary of the computation (AMD Opteron 2.6GHz)

p	X_3	time	p	X_3	time	p	X_3	time
59	47	2s	347	186	33m	587	279	248m
83	62	9s	419	216	67m	659	1	3s
107	74	23s	443	2	5s	683	2	7s
179	111	2m29s	467	233	102m	827	2	4s
227	134	6m13s	563	270	211m	947	2	10s

We recall that Cohn [14] showed that the only positive integer solution of $x^2 + 1 = 2y^p$ is given by $x = y = 1$.

Theorem 1.4.1. *If the Diophantine equation $x^2 + 3^{2m} = 2y^p$ with $m > 0$ and p prime admits a coprime integer solution (x, y), then $(x, y, m, p) = (13, 5, 2, 3), (79, 5, 1, 5)$, or $(545, 53, 3, 3)$.*

Proof. We will provide lower bounds for m which contradict the bound for p provided by Proposition 1.2.1. By Proposition 1.2.1 we have $p \leq 3803$ and by Proposition 1.4.1 we have $p \equiv 5$ or $11 \pmod{24}$. We are left with the primes $p < 1000, p \equiv 5$ or $11 \pmod{24}$. They are treated in Propositions 1.4.2 and 1.4.3. We compute the following sets for each prime p with $1000 \leq p \leq 3803, p \equiv 5$ or $11 \pmod{24}$:

$$A5 := L(p, 3, 242),$$
$$A16 := L(p, 3, 136) \cap L(p, 3, 193) \cap L(p, 3, 320) \cap L(p, 3, 697),$$
$$A22 := L(p, 3, 92) \cap L(p, 3, 134) \cap L(p, 3, 661),$$
$$A27 := L(p, 3, 866) \cap L(p, 3, 1417),$$
$$A34 := L(p, 3, 103) \cap L(p, 3, 307) \cap L(p, 3, 1021),$$
$$A39 := L(p, 3, 169) \cap L(p, 3, 313),$$
$$A69 := L(p, 3, 554) \cap L(p, 3, 611).$$

About half of the primes can be disposed of by the following reasoning. In case of $A5$ we have $\mathrm{ord}_{242}3 = 5$, hence this set contains those congruence classes modulo 5 for which (1.14) is solvable. The situation is similar for the other sets. How can we use this information? Suppose it turns out that for a prime $A5 = \{0\}$ and $A16 = \{0\}$. Then we know that $m \equiv 0 \pmod{5 \cdot 16}$ and Proposition 1.2.1 implies $p \leq 1309$. If the prime is larger than this bound, then we have a contradiction. In Table 3 we included those primes for which we obtained a contradiction in this way. In the columns mod the numbers n are

Table 1.3: Excluding some primes using congruences.

p	mod	p	mod	p	mod	p	mod	p	mod
1013	16,27	1571	5,22	1973	16,22	2357	16,22	3011	5,22
1109	16,22	1613	16,22	1979	16,22	2459	16,22	3203	16,22
1181	16,22	1619	16,22	2003	16,22	2477	16,22	3221	16,22
1187	16,22	1667	16,22	2027	16,22	2531	5,22	3323	16,22
1229	16,22	1709	16,22	2069	16,22	2579	16,22	3347	16,22
1259	16,22	1733	16,22	2099	16,22	2693	16,22	3371	5,22
1277	16,22	1787	16,22	2141	16,22	2741	16,27	3413	16,22
1283	16,22	1811	5,22	2237	16,22	2861	16,22	3533	16,22
1307	16,22	1877	16,27	2243	16,22	2909	16,22	3677	16,22
1493	16,22	1931	5,22	2309	16,27	2957	16,22	3701	16,22
1523	16,22	1949	16,22	2333	16,22	2963	16,22		

stated for which sets An were used for the given prime. It turned out that only 4 sets were needed. In case of $5, 22$ we have $m \geq 110, p \leq 1093$, in case of $16, 22$ we have $m \geq 176, p \leq 1093$ and in the case $16, 27$ we have $m \geq 432, p \leq 1009$.

Table 1.4: Excluding some primes using CRT.

p	r_m	CRT	p	r_m	CRT	p	r_m	CRT
1019	384	5,16,27	2267	448	5,16,69	3389	170	5,27,34
1061	176	5,16,39	2339	208	5,16,39	3461	116	5,16,39
1091	580	5,16,27	2381	44	5,27,34	3467	336	5,16,27
1163	586	5,27,34	2411	180	5,16,27	3491	850	5,27,34
1301	416	5,16,39	2549	320	5,16,27	3539	112	5,16,39
1427	270	5,27,34	2699	640	5,16,69	3557	176	5,16,39
1451	340	5,16,27	2789	204	5,27,34	3581	150	5,27,34
1499	112	5,16,39	2819	352	5,16,27	3659	112	5,16,39
1637	121	5,27,34	2837	131	5,27,34	3779	72	5,27,34
1901	304	5,16,39	2843	136	5,27,34	3797	416	5,16,39
1907	102	5,27,34	3083	340	5,27,34	3803	136	5,27,34
1997	170	5,27,34	3251	580	5,16,27			
2213	170	5,27,34	3299	64	5,16,39			

For the remaining primes we combine the available information by means of the Chinese remainder theorem. Let $CRT(5, 16, 39)$ be the smallest non-negative solution of the system of congruences

$$\begin{aligned} m &\equiv a5 \pmod 5 \\ m &\equiv a16 \pmod{16} \\ m &\equiv a39 \pmod{39}, \end{aligned}$$

where $a5 \in A5, a16 \in A16$ and $a39 \in A39$. Let r_m be the smallest non-zero element of the set $\{CRT(5, 16, 39) : a5 \in A5, a16 \in A16, a39 \in A39\}$, In Table 4 we included the values of r_m and the numbers related to the sets $A5 - A69$. We see that $m \geq r_m$ in all cases. For example, if $p = 1019$ then $m \geq 384$, and Proposition 1.2.1 implies $p \leq 1009$, which is a contradiction. For $p = 2381$ we used $A5, A27$ and $A34$, given by $A5 = \{0, 1, 4\}, A27 = \{0, 14, 15, 17\}, A34 = \{0, 10\}$. Hence

$$\begin{aligned} &\{CRT(5, 27, 34) : a5 \in A5, a27 \in A27, a34 \in A34\} = \\ &= \{0, 44, 204, 476, 486, 554, 690, 986, 1394, 1404, 1836, 1880, 1904, \\ &2040, 2390, 2526, 2754, 3230, 3240, 3444, 3716, 3740, 3876, 4226\}. \end{aligned}$$

The smallest non-zero element is 44 (which comes from $[a5, a27, a34] = [4, 17, 10]$), therefore $m \geq 44$ and $p \leq 1309$, a contradiction. In this way all remaining primes > 1000 can be handled. □

Acknowledgement. The author wish to thank Guillaume Hanrot for the computations related to Proposition 1.4.3 and for giving some hints how to modify

the PARI code, which was used in [10], to make the computations necessary for Proposition 1.4.2. Furthermore, he would like to thank Robert
Tijdeman for his valuable remarks and suggestions, Peter Stevenhagen for the useful discussions on algebraic number theory, and for the proof of Lemma 1.4.1 and Kálmán Győry for calling his attention to Schinzel's Hypothesis.

Bibliography

[1] S. A. Arif and F. S. A. Muriefah. On the Diophantine equation $x^2+2^k = y^n$. *Internat. J. Math. Math. Sci.*, 20(2):299–304, 1997.

[2] S. A. Arif and F. S. A. Muriefah. The Diophantine equation $x^2 + 3^m = y^n$. *Internat. J. Math. Math. Sci.*, 21(3):619–620, 1998.

[3] S. A. Arif and F. S. A. Muriefah. On a Diophantine equation. *Bull. Austral. Math. Soc.*, 57(2):189–198, 1998.

[4] S. A. Arif and F. S. A. Muriefah. The Diophantine equation $x^2+5^{2k+1} = y^n$. *Indian J. Pure Appl. Math.*, 30(3):229–231, 1999.

[5] S. A. Arif and F. S. A. Muriefah. The Diophantine equation $x^2 + q^{2k} = y^n$. *Arab. J. Sci. Eng. Sect. A Sci.*, 26(1):53–62, 2001.

[6] S. A. Arif and F S. A. Muriefah. On the Diophantine equation $x^2+2^k = y^n$. II. *Arab J. Math. Sci.*, 7(2):67–71, 2001.

[7] S. A. Arif and F. S. A. Muriefah. On the Diophantine equation $x^2 + q^{2k+1} = y^n$. *J. Number Theory*, 95(1):95–100, 2002.

[8] Yu. Bilu and G. Hanrot. Solving Thue equations of high degree. *J. Number Theory*, 60(2):373–392, 1996.

[9] Yu. Bilu and G. Hanrot. Thue equations with composite fields. *Acta Arith.*, 88(4):311–326, 1999.

[10] Yu. Bilu, G. Hanrot, and P. M. Voutier. Existence of primitive divisors of Lucas and Lehmer numbers. *J. Reine Angew. Math.*, 539:75–122, 2001. With an appendix by M. Mignotte.

[11] Y. Bugeaud. On the Diophantine equation $x^2 - p^m = \pm y^n$. *Acta Arith.*, 80(3):213–223, 1997.

[12] J. H. E. Cohn. The Diophantine equation $x^2+2^k = y^n$. *Arch. Math. (Basel)*, 59(4):341–344, 1992.

[13] J. H. E. Cohn. The Diophantine equation $x^2 + 3 = y^n$. *Glasgow Math. J.*, 35(2):203–206, 1993.

[14] J. H. E. Cohn. Perfect Pell powers. *Glasgow Math. J.*, 38(1):19–20, 1996.

[15] J. H. E. Cohn. The Diophantine equation $x^2 + 2^k = y^n$. II. *Int. J. Math. Math. Sci.*, 22(3):459–462, 1999.

[16] G. Hanrot. Solving Thue equations without the full unit group. *Math. Comp.*, 69(229):395–405, 2000.

[17] Maohua Le. On the Diophantine equation $x^2 + p^2 = y^n$. *Publ. Math. Debrecen*, 63(1-2):67–78, 2003.

[18] F. Luca. On a Diophantine equation. *Bull. Austral. Math. Soc.*, 61(2):241–246, 2000.

[19] F. Luca. On the equation $x^2 + 2^a \cdot 3^b = y^n$. *Int. J. Math. Math. Sci.*, 29(4):239–244, 2002.

[20] M. Mignotte. On the Diophantine equation $D_1x^2 + D_2^m = 4y^n$. *Portugal. Math.*, 54(4):457–460, 1997.

[21] F. S. A. Muriefah. On the Diophantine equation $px^2 + 3^n = y^p$. *Tamkang J. Math.*, 31(1):79–84, 2000.

[22] F. S. A. Muriefah. On the Diophantine equation $Ax^2 + 2^{2m} = y^n$. *Int. J. Math. Math. Sci.*, 25(6):373–381, 2001.

[23] I. Niven. *Irrational numbers*. The Carus Mathematical Monographs, No. 11. The Mathematical Association of America. Distributed by John Wiley and Sons, Inc., New York, N.Y., 1956.

[24] The PARI Group, Bordeaux. *PARI/GP, version 2.2.8*, 2004. available from http://pari.math.u-bordeaux.fr/.

[25] I. Pink. On the Diophantine equation $x^2 + (p_1^{z_1} \dots p_s^{z_s})^2 = 2y^n$. *Publ. Math. Debrecen*, 65(1-2):205–213, 2004.

[26] I. Pink and Sz. Tengely. Full powers in arithmetic progressions. *Publ. Math. Debrecen*, 57(3-4):535–545, 2000.

[27] Sz. Tengely. On the Diophantine equation $x^2 + a^2 = 2y^p$. *Indag. Math. (N.S.)*, 15(2):291–304, 2004.

[28] A. Thue. Über Annäherungswerte algebraischer Zahlen. *J. Reine Angew Math.*, 135:284–305, 1909.

[29] P. M. Voutier. Primitive divisors of Lucas and Lehmer sequences. II. *J. Théor. Nombres Bordeaux*, 8(2):251–274, 1996.

2

On the Diophantine Equation $x^2 + C = 2y^n$

*A*bu Muriefah, F. S., Luca, F., Siksek, S. and Tengely, Sz.,
Int. J. Number Theory **5** (2009), 1117–1128.

Abstract

In this paper, we study the Diophantine equation $x^2 + C = 2y^n$ in positive integers x, y with $\gcd(x, y) = 1$, where $n \geq 3$ and C is a positive integer. If $C \equiv 1 \pmod 4$ we give a very sharp bound for prime values of the exponent n; our main tool here is the result on existence of primitive divisors in Lehmer sequence due Bilu, Hanrot and Voutier. We illustrate our approach by solving completely the equations $x^2 + 17^{a_1} = 2y^n$, $x^2 + 5^{a_1}13^{a_2} = 2y^n$, and $x^2 + 3^{a_1}11^{a_2} = 2y^n$.

2.1 Introduction

The Diophantine equation $x^2 + C = y^n$, in integer unknowns x, y and $n \geq 3$, has a long and distinguished history. The first case to have been solved appears to be $C = 1$: in 1850, Victor Lebesgue [16] showed, using an elementary factorization argument, that the only solution is $x = 0$, $y = 1$. Over the next 140 years many equations of the form $x^2 + C = y^n$ have been solved using Lebesgue's elementary trick. In 1993, John Cohn [12] published an exhaustive historical survey of this equation which completes the solution for all but 23 values of C in the range $1 \leq C \leq 100$. In a second paper, [14], Cohn shows that the tedious elementary argument can be eliminated by appealing to the remarkable recent theorem [4] on the existence of primitive divisors of Lucas sequences, due to Bilu, Hanrot and Voutier. The next major breakthrough came in 2006 when Bugeaud, Mignotte and Siksek [8] applied a combination of Baker's Theory and

the modular approach to the equation $x^2 + C = y^n$ and completed its solution for $1 \leq C \leq 100$.

It has been noted recently (e.g. [1], [2], [3]) that the result of Bilu, Hanrot and Voutier can sometimes be applied to equations of the form $x^2 + C = y^n$ where instead of C being a fixed integer, C is the product of powers of fixed primes $p_1, \ldots, p_k$.

By comparison, the Diophantine equation $x^2 + C = 2y^n$, with the same restrictions, has received little attention. For $C = 1$, John Cohn [13], showed that the only solutions to this equation are $x = y = 1$ and $x = 239$, $y = 13$ and $n = 4$. The fourth-named author studied [19] the equation $x^2 + q^{2m} = 2y^p$ where m, p, q, x, y are integer unknowns with $m > 0$, and p, q are odd primes and $\gcd(x, y) = 1$. He proved that there are only finitely many solutions (m, p, q, x, y) for which y is not a sum of two consecutive squares. He also studied the equation for fixed q and resolved it when $q = 3$.

The purpose of this paper is to perform a deeper study of the equation $x^2 + C = 2y^n$, both in the case where C is a fixed integer, as well as in the case where C is the product of powers of fixed primes. Principally, we show that in some cases this equation can be solved by appealing to the theorem of Bilu, Hanrot and Voutier on primitive divisors of *Lehmer sequences*. In particular, we prove the following theorem.

Theorem 2.1.1. *Let C be a positive integer satisfying $C \equiv 1 \pmod 4$, and write $C = cd^2$, where c is square-free. Suppose that (x, y) is a solution to the equation*

$$x^2 + C = 2y^p, \qquad x,\ y \in \mathbb{Z}^+, \quad \gcd(x, y) = 1, \tag{2.1}$$

where $p \geq 5$ is a prime. Then either

(i) $x = y = C = 1$, *or*

(ii) p *divides the class number of the quadratic field* $\mathbb{Q}(\sqrt{-c})$, *or*

(iii) $p = 5$ *and* $(C, x, y) = (9, 79, 5)$, $(125, 19, 3)$, $(125, 183, 7)$, $(2125, 21417, 47)$, *or*

(iv) $p \mid (q - (-c|q))$, *where q is some odd prime such that $q \mid d$ and $q \nmid c$. Here $(c|q)$ denotes the Legendre symbol of the integer c with respect to the prime q.*

Theorem 2.1.2. *The only solutions to the equation $x^2 + C = 2y^n$ with x, y coprime integers, $n \geq 3$, and $C \equiv 1 \pmod 4$, $1 \leq C < 100$ are*

$$1^2 + 1 = 2 \cdot 1^n, \quad 79^2 + 9 = 2 \cdot 5^5, \quad 5^2 + 29 = 2 \cdot 3^3,$$
$$117^2 + 29 = 2 \cdot 19^3, \quad 993^2 + 29 = 2 \cdot 79^3, \quad 11^2 + 41 = 2 \cdot 3^4,$$
$$69^2 + 41 = 2 \cdot 7^4, \quad 171^2 + 41 = 2 \cdot 11^4, \quad 1^2 + 53 = 2 \cdot 3^3,$$
$$25^2 + 61 = 2 \cdot 7^3, \quad 51^2 + 61 = 2 \cdot 11^3, \quad 37^2 + 89 = 2 \cdot 9^3.$$

Proof. Theorem 2.1.1 implies that either $(C, x, y) \in \{(1, 1, 1), (9, 79, 5)\}$ or $p \in \{2, 3\}$. It remains to solve the equations $x^2 + C = 2y^3$ and $x^2 + C = 2y^4$ for $C \equiv 1 \pmod 4$, $1 \leq C < 100$. Hence, we have reduced the problem to computing integral points on certain elliptic curves. Using the computer package MAGMA [5], we find the solutions listed in the theorem. □

Theorem 2.1.1 yields the following straightforward corollary.

Corollary. *Let $q_1, \ldots, q_k$ be distinct primes satisfying $q_i \equiv 1 \pmod 4$. Suppose that $(x, y, p, a_1, \ldots, a_k)$ is a solution to the equation*

$$x^2 + q_1^{a_1} \ldots q_k^{a_k} = 2y^p, \tag{2.2}$$

satisfying

$$x,\ y \in \mathbb{Z}^+, \qquad \gcd(x, y) = 1, \qquad a_i \geq 0, \qquad p \geq 5 \text{ prime}.$$

Then either

(i) $x = y = 1$ *and all the* $a_i = 0$, *or*

(ii) p *divides the class number of the quadratic field* $\mathbb{Q}(\sqrt{-c})$ *for some square-free* c *dividing* $q_1 q_2 \ldots q_k$, *or*

(iii) $p = 5$ *and* $(\prod q_i^{a_i}, x, y) = (125, 19, 3), (125, 183, 7), (2125, 21417, 47)$, *or*

(iv) $p \mid (q_i^2 - 1)$ *for some* i.

We illustrate by solving completely the equations

$$x^2 + 17^{a_1} = 2y^n,$$
$$x^2 + 5^{a_1} 13^{a_2} = 2y^n,$$
$$x^2 + 3^{a_1} 11^{a_2} = 2y^n,$$

under the restrictions $\gcd(x, y) = 1$, and $n \geq 3$.

Theorem 2.1.3. *The only solutions to the equation*

$$x^2 + 17^{a_1} = 2y^n, \qquad a_1 \geq 0, \quad \gcd(x, y) = 1, \quad n \geq 3,$$

are

$$1^2 + 17^0 = 2 \cdot 1^n, \quad 239^2 + 17^0 = 2 \cdot 13^4, \quad 31^2 + 17^2 = 2 \cdot 5^4.$$

The only solutions to the equation

$$x^2 + 5^{a_1}13^{a_2} = 2y^n, \qquad a_1, a_2 \geq 0, \quad \gcd(x, y) = 1, \quad n \geq 3,$$

are

$$1^2 + 5^0 \cdot 13^0 = 2 \cdot 1^n, \quad 9^2 + 5^0 \cdot 13^2 = 2 \cdot 5^3,$$
$$7^2 + 5^1 \cdot 13^0 = 2 \cdot 3^3, \quad 99^2 + 5^2 \cdot 13^0 = 2 \cdot 17^3,$$
$$19^2 + 5^2 \cdot 13^1 = 2 \cdot 7^3, \quad 79137^2 + 5^2 \cdot 13^3 = 2 \cdot 1463^3,$$
$$253^2 + 5^2 \cdot 13^4 = 2 \cdot 73^3, \quad 188000497^2 + 5^8 \cdot 13^4 = 2 \cdot 260473^3,$$
$$239^2 + 5^0 \cdot 13^0 = 2 \cdot 13^4.$$

The only solutions to the equation

$$x^2 + 3^{a_1}11^{a_2} = 2y^n, \qquad a_1, a_2 \geq 0, \quad \gcd(x, y) = 1, \quad n \geq 3,$$

are

$$1^2 + 3^0 \cdot 11^0 = 2 \cdot 1^n, \quad 351^2 + 3^0 \cdot 11^4 = 2 \cdot 41^3,$$
$$13^2 + 3^4 \cdot 11^0 = 2 \cdot 5^3, \quad 5^2 + 3^4 \cdot 11^2 = 2 \cdot 17^3,$$
$$27607^2 + 3^4 \cdot 11^2 = 2 \cdot 725^3, \quad 545^2 + 3^6 \cdot 11^0 = 2 \cdot 53^3,$$
$$679^2 + 3^6 \cdot 11^2 = 2 \cdot 65^3, \quad 1093^2 + 3^8 \cdot 11^4 = 2 \cdot 365^3,$$
$$410639^2 + 3^{10} \cdot 11^2 = 2 \cdot 4385^3, \quad 239^2 + 3^0 \cdot 11^0 = 2 \cdot 13^4,$$
$$79^2 + 3^2 \cdot 11^0 = 2 \cdot 5^5.$$

2.2 Arithmetic of Some Biquadratic Fields

In this section, we let c be a square-free positive integer such that $c \equiv 1 \pmod 4$. We let $\mathbb{K} = \mathbb{Q}(\sqrt{2}, \sqrt{-c})$.

Lemma 2.2.1. *The field $\mathbb{K}$ has Galois group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and precisely three quadratic subfields: $\mathbb{L}_1 = \mathbb{Q}(\sqrt{2})$, $\mathbb{L}_2 = \mathbb{Q}(\sqrt{-c})$ and $\mathbb{L}_3 = \mathbb{Q}(\sqrt{-2c})$. The ring of integers $\mathbb{O}_\mathbb{K}$ has $\mathbb{Z}$-basis*

$$\left\{1, \ \sqrt{2}, \ \sqrt{-c}, \ \frac{1 + \sqrt{-c}}{\sqrt{2}}\right\}.$$

The class number of h of $\mathbb{K}$ is $h = 2^{-i}h_2h_3$ where h_2, h_3 are respectively the class numbers of $\mathbb{L}_2$ and $\mathbb{L}_3$, and $0 \leq i \leq 2$.

Proof. The ring of integers can be read off from the tables in Kenneth Williams' seminal paper on integers of biquadratic fields [21].

For the relation between class numbers, see [6].

□

2.3 Lehmer Sequences

We briefly define Lehmer sequences and state some relevant facts about them. A *Lehmer pair* is a pair (α, β) of algebraic integers such that $(\alpha+\beta)^2$ and $\alpha\beta$ are non-zero coprime rational integers and α/β is not a root of unity. For a Lehmer pair (α, β), the corresponding *Lehmer sequence* $\{u_n\}$ is given by

$$u_n = \begin{cases} (\alpha^n - \beta^n)/(\alpha - \beta) & \text{if } n \text{ is odd,} \\ (\alpha^n - \beta^n)/(\alpha^2 - \beta^2) & \text{if } n \text{ is even.} \end{cases}$$

Two Lehmer pairs (α_1, β_1) and (α_2, β_2) are said to be *equivalent* if $\alpha_1/\alpha_2 = \beta_1/\beta_2 \in \{\pm 1, \pm\sqrt{-1}\}$. One sees that general terms of Lehmer sequences corresponding to equivalent pairs are the same up to signs.

A prime q is called a *primitive divisor* of the term u_n if q divides u_n but q does not divide $(\alpha^2-\beta^2)^2 u_1 \dots u_{n-1}$. We shall not state the full strength of the theorems of Bilu, Hanrot and Voutier [4] as this would take too long, but merely the following special cases:

(i) if $n > 30$, then u_n has a primitive divisor;

(ii) if $n = 11$, 17, 19, 23 or 29, then u_n has a primitive divisor;

(iii) u_7 and u_{13} have primitive divisors unless (α, β) is equivalent to

$$\left((\sqrt{a} - \sqrt{b})/2, (\sqrt{a} + \sqrt{b})/2\right), \tag{2.3}$$

where (a, b) is one of $(1, -7)$, $(1, -19)$, $(3, -5)$, $(5, -7)$, $(13, -3)$, $(14, -22)$.

(iv) u_5 has a primitive divisor unless (α, β) is equivalent to a Lehmer pair of the form (2.3) where

- $a = F_{k+2\epsilon}$, $b = F_{k+2\epsilon} - 4F_k$ for some $k \geq 3$, $\epsilon = \pm 1$, where F_n is the Fibonacci sequence given by $F_0 = F_1 = 1$ and $F_{n+2} = F_{n+1} + F_n$ for all $n \geq 0$;

- $a = L_{k+2\epsilon}$, $b = L_{k+2\epsilon} - 4L_k$ for some $k \geq 0$, $k \neq 1$, $\epsilon = \pm 1$, where L_n is the Lucas sequence given by $L_0 = 2$, $L_1 = 1$ and $L_{n+2} = L_{n+1} + L_n$ for all $n \geq 0$.

Lemma 2.3.1. *Let c be a positive square-free integer, $c \equiv 1 \pmod 4$. Let U, V be odd integers such that $\gcd(U, cV) = 1$. Suppose moreover that $(c, U^2, V^2) \neq (1, 1, 1)$. Write*

$$\alpha = \frac{U + V\sqrt{-c}}{\sqrt{2}}, \qquad \beta = \frac{U - V\sqrt{-c}}{\sqrt{2}}. \tag{2.4}$$

Then (α, β) is a Lehmer pair. Denote the corresponding Lehmer sequence by $\{u_n\}$. Then u_p has a primitive divisor for all prime $p \geq 7$. Moreover, u_5 has a primitive divisor provided that

$$(c, U^2, V^2) \neq (1, 1, 9),\ (5, 1, 1),\ (5, 9, 1),\ (85, 9, 1). \tag{2.5}$$

Proof. Throughout, we shall write $x = U/(V\sqrt{-c})$ and use the fact that

$$t = \frac{x+1}{x-1} \qquad \text{iff} \qquad x = \frac{t+1}{t-1}.$$

We shall also repeatedly use the easy fact that, for $\epsilon = \pm 1$ and $k \geq 0$, both $\gcd(F_{k+2\epsilon}, F_{k+2\epsilon} - 4F_k)$ and $\gcd(L_{k+2\epsilon}, L_{k+2\epsilon} - 4L_k)$ are either 1, 2 or 4.

Note that α, β are algebraic integers by Lemma 2.2.1. Moreover $(\alpha + \beta)^2 = 2U^2$, $\alpha\beta = (U^2 + cV^2)/2$ are coprime rational integers. We next show that α/β is not a root of unity. But

$$\alpha/\beta = \frac{x+1}{x-1}$$

is in $\mathbb{Q}(\sqrt{-c})$ and so if it is a root of unity, it must be ± 1, $\pm\sqrt{-1}$, $(\pm 1 \pm \sqrt{-3})/2$. From our assumptions on c, U and V, we find that this is impossible. In particular, $\pm\sqrt{-1}$ leads to $(c, U^2, V^2) = (1, 1, 1)$, which we have excluded.

It remains to show that u_p has a primitive divisor. Suppose otherwise. Then

$$\frac{x+1}{x-1} = \pm\left(\frac{\sqrt{a} - \sqrt{b}}{\sqrt{a} + \sqrt{b}}\right) \qquad \text{or} \qquad \frac{x+1}{x-1} = \pm\sqrt{-1}\left(\frac{\sqrt{a} - \sqrt{b}}{\sqrt{a} + \sqrt{b}}\right),$$

where (a, b) is one of the pairs listed in (iii), (iv) above.

Let us first deal with the case $(x+1)/(x-1) = \pm\sqrt{-1}(\sqrt{a} - \sqrt{b})/(\sqrt{a} + \sqrt{b})$. Solving for x and squaring we obtain

$$\frac{U^2}{-cV^2} = \frac{a - b \mp 2\sqrt{-ab}}{b - a \mp 2\sqrt{-ab}},$$

which implies that $a = b$ or that $-ab$ is a square. This is not possible for the pairs listed in (iii), whilst for (iv) it leads to equations that can easily be solved with the help of Lemma 2.3.2 below.

Next we deal with the case $(x+1)/(x-1) = \pm(\sqrt{a}-\sqrt{b})/(\sqrt{a}+\sqrt{b})$. This leads to $x = -(\sqrt{a}/\sqrt{b})^{\pm 1}$. Squaring we obtain

$$\frac{U^2}{-cV^2} = \left(\frac{a}{b}\right)^{\pm 1} = \left(\frac{a'}{b'}\right)^{\pm 1}.$$

where $a' = a/\gcd(a,b)$ and $b' = b/\gcd(a,b)$. Since U and cV are coprime we have

$$\begin{cases} \pm U^2 = a', \\ \mp cV^2 = b', \end{cases} \quad \text{or} \quad \begin{cases} \pm U^2 = b', \\ \mp cV^2 = a'. \end{cases}$$

One quickly eliminates all the possibilities in (iii) mostly using the fact that $c \equiv 1 \pmod 4$. For the possibilities in (iv), we obtain equations of the form solved in Lemma 2.3.2 and these lead to one of the possibilities excluded in (2.5). This completes the proof of the lemma. □

In the proof of Lemma 2.3.1, we needed the following results about Fibonacci and Lucas numbers.

Lemma 2.3.2. *Let $\{F_n\}_{n\geq 0}$ and $\{L_n\}_{n\geq 0}$ be the Fibonacci and Lucas sequences. The only solutions to the equation $F_n = u^2$ have $n = 0, 1, 2$ or 12. The only solutions to $F_n = 2u^2$ have $n = 3$ or 12. The only solutions to the equation $L_n = v^2$ have $n = 1$ or 3. The only solutions to the equation $L_n = 2v^2$ have $n = 0$ or 6.*

The only solutions to the equation

$$F_{k+2\epsilon} - 4F_k = \pm 2^r u^2, \qquad \epsilon = \pm 1, \quad k, r \geq 0, \quad u \in \mathbb{Z}, \tag{2.6}$$

have $(k,\epsilon) = (0,\pm 1),\ (1,1),\ (2,\pm 1),\ (4,1),\ (5,-1),\ (7,1)$. The only solutions to the equation

$$L_{k+2\epsilon} - 4L_k = \pm 2^r u^2, \qquad \epsilon = \pm 1, \quad k, r \geq 0, \quad u \in \mathbb{Z}, \tag{2.7}$$

have $(k,\epsilon) = (1,1),\ (4,-1),\ (6,1)$.

Proof. The results about Fibonacci and Lucas numbers of the form $2^r u^2$ are classical. See, for example, [10], [11].

It remains to deal with (2.6) and (2.7). Here, we may take $r = 0, 1$. We explain how to deal with (2.6) with $r = 0$:

$$F_{k+2\epsilon} - 4F_k = \pm u^2, \qquad \epsilon = \pm 1, \quad k \geq 0, \quad u \in \mathbb{Z};$$

the other cases are similar. We make use of Binet's formula for Fibonacci numbers:

$$F_n = \frac{\lambda^n - \mu^n}{\sqrt{5}}, \qquad \lambda = \frac{1+\sqrt{5}}{2}, \quad \mu = \frac{1-\sqrt{5}}{2}.$$

Our equation can thus be rewritten as

$$\gamma\lambda^k - \delta\mu^k = u^2\sqrt{5}, \qquad \gamma = \lambda^{2\epsilon} - 4, \quad \delta = \mu^{2\epsilon} - 4.$$

Let $v = \gamma\lambda^k + \delta\mu^k$. It is clear that $v \in \mathbb{Z}$. Moreover,

$$v^2 = (\gamma\lambda^k + \delta\mu^k)^2 = (\gamma\lambda^k - \delta\mu^k)^2 + 4\gamma\delta(\lambda\mu)^k = 5u^4 \pm 20.$$

Let $X = 5u^2$, and $Y = 5uv$. Then $Y^2 = X(X^2 \pm 100)$. Thus, we have reduced the problem to computing integral points on a pair of elliptic curves. Using the computer package MAGMA [5], we find that

$$(X, Y) = (0, 0),\ (5, \pm 25),\ (20, \pm 100),\ (\pm 100, 0).$$

The remaining equations similarly lead to integral points on elliptic curves which we found using MAGMA. Working backwards, we obtain the solutions given in the lemma. □

2.4 Proof of Theorem 2.1.1

We follow the notation from the statement of the theorem. We shall suppose that $(C, x, y) \neq (1, 1, 1)$ and p does not divide the class number of the $\mathbb{Q}(\sqrt{-c})$. We will show that either statement (iii) or (iv) of the theorem must hold.

Considering equation (2.1) modulo 4 reveals that x and y are odd. We work first in $\mathbb{Q}(\sqrt{-c})$. Since $c \equiv 1 \pmod 4$, this has ring of integers $\mathbb{O} = \mathbb{Z}[\sqrt{-c}]$. Moreover, $(2) = \mathfrak{q}^2$, where $\mathfrak{q}$ is a prime ideal of $\mathbb{O}$. It is clear that the principal ideals $(x + d\sqrt{-c})$ and $(x - d\sqrt{-c})$ have $\mathfrak{q}$ as their greatest common factor. From (2.1) we deduce that

$$(x + d\sqrt{-c})\mathbb{O} = \mathfrak{q} \cdot \gamma^p,$$

where γ is some ideal of $\mathbb{O}$. Now multiply both sides by $2^{(p-1)/2}$. We obtain

$$2^{(p-1)/2}(x + d\sqrt{-c})\mathbb{O} = (\mathfrak{q}\gamma)^p.$$

Since the class number of $\mathbb{Q}(\sqrt{-c})$ is not divisible by p, we see that $\mathfrak{q}\gamma$ is a principal ideal. Moreover, as c is positive, the units of $\mathbb{Z}[\sqrt{-c}]$ are ± 1. Hence

$$2^{(p-1)/2}(x + d\sqrt{-c}) = (U + V\sqrt{-c})^p \tag{2.8}$$

for some integers U, V. Since x, d, c are odd, we deduce that U and V are both odd. Moreover, $y = (U^2 + cV^2)/2$. From the coprimality of x and y we see that U, cV are coprime.

In conclusion,

$$\frac{x + d\sqrt{-c}}{\sqrt{2}} = \left(\frac{U + V\sqrt{-c}}{\sqrt{2}}\right)^p,$$

where U, V, c satisfy the conditions of Lemma 2.3.1.

Let α, β be as in (2.4). Let $\{u_n\}$ be the corresponding Lehmer sequence. We note that

$$\alpha^p - \beta^p = d\sqrt{-2c}, \qquad \alpha - \beta = V\sqrt{-2c}.$$

Thus, $V \mid d$ and $u_p \mid d/V$. By Lemma 2.3.1, u_p has a primitive divisor unless $p = 5$ and (c, U^2, V^2) is one of the possibilities listed in (2.5). These possibilities lead to cases given in item (iii) of the theorem. Thus, we may exclude these and so assume that u_p has a primitive divisor q. Our objective now is to show that (iv) holds. Clearly, $q \mid d$, but by the definition of the primitive divisor, $q \nmid (\alpha^2 - \beta^2)^2$ and so, in particular, $q \nmid c$. To complete the proof, let

$$\gamma = U + V\sqrt{-c}, \qquad \delta = U - V\sqrt{-c}.$$

Write $v_n = (\gamma^n - \delta^n)/(\gamma - \delta)$. We note that $q \mid v_p$ but, from the accumulated facts, $q \nmid (\gamma - \delta)\gamma\delta$. We claim that $q \mid v_{q-(-c|q)}$. Given our claim, it follows from [9, Lemma 5], that p divides $q - (-c|q)$. Now let us prove our claim. If $(-c|q) = 1$, then

$$\gamma^{q-1} \equiv \delta^{q-1} \equiv 1 \pmod{q},$$

and hence $q \mid v_{q-1}$. Suppose $(-c|q) = -1$. Then, by the properties of the Frobenius automorphism, we have

$$\gamma^q \equiv \delta \pmod{q}, \qquad \delta^q \equiv \gamma \pmod{q}.$$

Hence,

$$\gamma^{q+1} - \delta^{q+1} \equiv \gamma\delta - \gamma\delta \equiv 0 \pmod{q},$$

proving $q \mid v_{q+1}$ as required. This completes the proof of the theorem.

Remark. In the proof of Theorem 2.1.1, it would have been possible to factorize the left-hand side of (2.1) in $\mathbb{K} = \mathbb{Q}(\sqrt{2}, \sqrt{-c})$. Doing this, the hypothesis that would be needed is that p does not divide the class number of $\mathbb{K}$. By Lemma 2.2.1, the class number of $\mathbb{Q}(\sqrt{-c})$ divides the class number of $\mathbb{K}$, up to powers of 2. Thus, we obtained a stronger result by working in $\mathbb{Q}(\sqrt{-c})$ instead of $\mathbb{K}$.

2.5 Dealing with small exponents

Let $q_1, \ldots, q_k$ be distinct primes. In this section, we explain how to solve the equation

$$x^2 + q_1^{a_1} \ldots q_k^{a_k} = 2y^n, \tag{2.9}$$

for small values of n. The method can be applied more easily to the equation $x^2 + C = 2y^n$. This section is meant to complement Theorem 2.1.1 and Corollary 2.1.

For the cases $n = 3$ and $n = 4$, we show that (2.9) can be reduced to computing $\mathcal{S}$-integral points on a handful of elliptic curves. The problem can now be solved by applying standard algorithms for computing S-integral points on elliptic curves (see, for example, [18]). Fortunately these algorithms are available as an inbuilt functions in the computer package MAGMA [5].

Suppose $n = 4$. We are then dealing with an equation of the form $x^2 + C = 2y^4$. Now write $C = cz^4$, where c is fourth power free and made up only of the primes $q_1, \ldots, q_k$. There are clearly only 4^k possibilities for c. Write

$$Y = \frac{2xy}{z^3}, \qquad X = \frac{2y^2}{z^2}.$$

We immediately see that (X, Y) is an $\mathcal{S}$-integral point on the elliptic curve $Y^2 = X(X^2 - 2c)$, where $\mathcal{S} = \{q_1, \ldots, q_k\}$.

Similarly, if $n = 3$, we are dealing with an equation of the form $x^2 + C = 2y^3$. We then write $C = cz^6$ for some sixth power free integer c made up with the primes $q_1, \ldots, q_k$. There are only 6^k possibilities for c. For each such c, let

$$X = \frac{2y}{z^2}, \qquad Y = \frac{2x}{z^3}.$$

Observe that (X, Y) is an $\mathcal{S}$-integral point on the elliptic curve $Y^2 = X^3 - 4c$.

If $n \geq 5$, then we require $\mathcal{S}$-integral points on finitely many curves of genus ≥ 2. Here it is often—but not always—possible to compute all the rational points on the curves using some variant of the method of Chabauty [7], [15], [17], [20].

2.6 Proof of Theorem 2.1.3

In this section, we prove Theorem 2.1.3. We consider the three Diophantine equations mentioned in the theorem separately.

- The equation $x^2 + 17^{a_1} = 2y^n$. Corollary 2.1 implies that either $(a_1, x, y) = (0, 1, 1)$ or $p \in \{2, 3\}$, where p is a prime divisor of n. Therefore it remains to solve the equations $x^2 + 17^{a_1} = 2y^3$ and $x^2 + 17^{a_1} = 2y^4$. We apply

the method described in Section 5 to determine all integral solutions. We obtain the following solutions

$$1^2 + 17^0 = 2 \cdot 1^3, \quad 1^2 + 17^0 = 2 \cdot 1^4,$$
$$239^2 + 17^0 = 2 \cdot 13^4, \quad 31^2 + 17^2 = 2 \cdot 5^4.$$

- The equation $x^2 + 5^{a_1}13^{a_2} = 2y^n$. In this case, Corollary 2.1 yields that either

$$(a_1, a_2, x, y, n) \in \{(0, 0, 1, 1, n), (3, 0, 19, 3, 5), (3, 0, 183, 7, 5)\},$$

or $p \in \{2, 3, 7\}$, where p is a prime divisor of n. If $p = 2$ or 3, then the method of Section 5 provides all solutions of the corresponding equations. Now we deal with the case $p = 7$. We have that $5^{a_1}13^{a_2} \in \{1\square, 5\square, 13\square, 65\square\}$. Assume that $5^{a_1}13^{a_2} = \square$. Working in the imaginary quadratic field $\mathbb{Q}[i]$, we easily get

$$5^{b_1}13^{b_2} = (U-V)(U^6+8U^5V-13U^4V^2-48U^3V^3-13U^2V^4+8UV^5+V^6).$$

One can obtain all integral solutions of the Thue equations $U^6 + 8U^5V - 13U^4V^2 - 48U^3V^3 - 13U^2V^4 + 8UV^5 + V^6 = \pm 1, \pm 5, \pm 13, \pm 65$. The only solutions are $(U, V) \in \{(\pm 1, 0), (0, \pm 1)\}$. So we may assume that

$$U - V = \pm 5^{c_1}13^{c_2},$$
$$U^6 + 8U^5V - 13U^4V^2 - 48U^3V^3 - 13U^2V^4 + 8UV^5 + V^6 = \pm 5^{b_1-c_1}13^{b_2-c_2},$$

with $b_1 - c_1, b_2 - c_2 \geq 2$. Considering the above system of equations modulo 5 and modulo 13 we get a contradiction. If $5^{a_1}13^{a_2} = 5d^2, 13d^2$ or $65d^2$, then equation (2.8) leads to

$$\begin{aligned} 5d^2 &: 8d = V(7U^6 - 175U^4V^2 + 525U^2V^4 - 125V^6), \\ 13d^2 &: 8d = V(7U^6 - 455U^4V^2 + 3549U^2V^4 - 2197V^6), \\ 65d^2 &: 8d = V(7U^6 - 2275U^4V^2 + 88725U^2V^4 - 274625V^6), \end{aligned}$$

respectively. It follows that V is a divisor of $8d$, so the prime divisors of V belong to the set $\{2, 5, 13\}$. Therefore the above equations can be written as

$$\square = X^3 \pm 175\omega_1 X^2 + 3675\omega_1^2 X \pm 6125\omega_1^3,$$
$$\square = X^3 \pm 455\omega_2 X^2 + 24843\omega_2^2 X \pm 107653\omega_2^3,$$
$$\square = X^3 \pm 2275\omega_3 X^2 + 621075\omega_3^2 X \pm 13456625\omega_3^3,$$

where $\omega_1, \omega_2, \omega_3 \in \{2^{\alpha_1}5^{\alpha_2}13^{\alpha_3} : \alpha_i = 0, 1\}$. We use MAGMA [5] to determine all $\{2, 5, 13\}$-integral points on the above elliptic curves. Then we find (U, V) and the corresponding solutions (x, y, a_1, a_2).

- Equation $x^2+3^{a_1}11^{a_2} = 2y^n$. Note that $x^2+3\square = 2y^p$ and $x^2+11\square = 2y^p$ can be excluded modulo 8. Hence it remains to deal with the equations $x^2+\square = 2y^p$ and $x^2 + 33\square = 2y^p$. We apply Theorem 2.1.1 with $3^{2b_1}11^{2b_2} = C \equiv 1 \pmod 4$ and $33 \cdot 3^{2c_1}11^{2c_2} = C \equiv 1 \pmod 4$. In the former case we obtain that $(x, y, a_1, a_2, n) \in \{(1, 1, 0, 0, n), (79, 5, 2, 0, 5)\}$ or $p \in \{2, 3\}$. In the latter case we get that $p = 2$. If $p = 2$ or 3, then the method of Section 5 provides all solutions of the corresponding equations. The proof of Theorem 3 is completed.

Bibliography

[1] F. S. Abu Muriefah. On the diophantine equation $x^2 + 5^{2k} = y^n$. *Demonstratio Mathematica*, 319:285–289, 2006.

[2] F. S. Abu Muriefah, F. Luca, and A. Togbé. On the Diophantine equation $x^2 + 5^a13^b = y^n$. *Glasg. Math. J.*, 50(1):175–181, 2008.

[3] S. A. Arif and F. S. A. Muriefah. On the Diophantine equation $x^2 + q^{2k+1} = y^n$. *J. Number Theory*, 95(1):95–100, 2002.

[4] Yu. Bilu, G. Hanrot, and P. M. Voutier. Existence of primitive divisors of Lucas and Lehmer numbers. *J. Reine Angew. Math.*, 539:75–122, 2001. With an appendix by M. Mignotte.

[5] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[6] Wieb Bosma and Bart de Smit. Class number relations from a computational point of view. *J. Symbolic Comput.*, 31(1-2):97–112, 2001. Computational algebra and number theory (Milwaukee, WI, 1996).

[7] Nils Bruin. Chabauty methods using elliptic curves. *J. Reine Angew. Math.*, 562:27–49, 2003.

[8] Y. Bugeaud, M. Mignotte, and S. Siksek. Classical and modular approaches to exponential Diophantine equations. II. The Lebesgue-Nagell equation. *Compos. Math.*, 142(1):31–62, 2006.

[9] Yann Bugeaud, Florian Luca, Maurice Mignotte, and Samir Siksek. Perfect powers from products of terms in Lucas sequences. *J. Reine Angew. Math.*, 611:109–129, 2007.

[10] J. H. E. Cohn. On square Fibonacci numbers. *J. London Math. Soc.*, 39:537–540, 1964.

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

[12] J. H. E. Cohn. The Diophantine equation $x^2+C = y^n$. *Acta Arith.*, 65(4):367–381, 1993.

[13] J. H. E. Cohn. Perfect Pell powers. *Glasgow Math. J.*, 38(1):19–20, 1996.

[14] J. H. E. Cohn. The Diophantine equation $x^2 + C = y^n$. II. *Acta Arith.*, 109(2):205–206, 2003.

[15] E. V. Flynn. A flexible method for applying Chabauty's theorem. *Compositio Math.*, 105(1):79–94, 1997.

[16] V.A. Lebesgue. Sur l'impossibilité en nombres entiers de l'équation $x^m = y^2 + 1$. *Nouv. Annal. des Math.*, 9:178–181, 1850.

[17] William Mccallum and Bjorn Poonen. The method of chabauty and coleman. preprint.

[18] Attila Pethő, Horst G. Zimmer, Josef Gebel, and Emanuel Herrmann. Computing all S-integral points on elliptic curves. *Math. Proc. Cambridge Philos. Soc.*, 127(3):383–402, 1999.

[19] Sz. Tengely. On the Diophantine equation $x^2 + q^{2m} = 2y^p$. *Acta Arith.*, 127(1):71–86, 2007.

[20] J. L. Wetherell. *Bounding the Number of Rational Points on Certain Curves of High Rank*. PhD thesis, University of California at Berkeley, 1997.

[21] Kenneth S. Williams. Integers of biquadratic fields. *Canad. Math. Bull.*, 13:519–526, 1970.

3

On the Diophantine Equation $x^2 + C = 4y^n$

*L*uca, F., Tengely, Sz. and Togbé, A.,
Ann. Sci. Math. Québec **33** (2009), 171–184.

Abstract

In this paper, we study the Diophantine equation $x^2 + C = 4y^n$ in nonnegative integers $x, y, n \geq 3$ with x and y coprime for various shapes of the positive integer C.

3.1 Introduction

The Diophantine equation

$$x^2 + C = y^n, \quad x \geq 1, \quad y \geq 1, \quad n \geq 3 \tag{3.1}$$

in integers x, y, n once C is given has a rich history. In 1850, Lebesgue [19] proved that the above equation has no solutions when $C = 1$. In 1965, Chao Ko [16] proved that the only solution of the above equation with $C = -1$ is $x = 3$, $y = 2$. J.H.E. Cohn [14] solved the above equation for several values of the parameter C in the range $1 \leq C \leq 100$. A couple of the remaining values of C in the above range were covered by Mignotte and De Weger in [24], and the remaining ones in the recent paper [13]. In [28], all solutions of the similar looking equation $x^2 + C = 2y^n$, where $n \geq 2$, x and y are coprime, and $C = B^2$ with $B \in \{3, 4, \ldots, 501\}$ were found.

Recently, several authors become interested in the case when only the prime factors of C are specified. For example, the case when $C = p^k$ with a fixed prime number p was dealt with in [5] and [18] for $p = 2$, in [6], [7] and [20] for $p = 3$, and in [8] for $p = 5$ and k odd. Partial results for a general prime p

appear in [10] and [17]. All the solutions when $C = 2^a 3^b$ were found in [21], and when $C = p^a q^b$ where $p, q \in \{2, 5, 13\}$, were found in the sequence of papers [4], [22] and [23]. For an analysis of the case $C = 2^\alpha 3^\beta 5^\gamma 7^\delta$, see [27]. The same Diophantine equation with $C = 2^\alpha 5^\beta 13^\gamma$ was dealt with in [15]. The Diophantine equation $x^2 + C = 2y^n$ was studied in the recent paper [3] for the families of parameters $C \in \{17^a,\ 5^{a_1}13^{a_2},\ 3^{a_1}11^{a_2}\}$. See also [9], [29], as well as the recent survey [2] for further results on equations of this type.

In this paper, we consider the Diophantine equation

$$x^2 + C = 4y^n,\ \ x \geq 1,\ \ y \geq 1,\ \ \gcd(x, y) = 1,\ \ n \geq 3,\ \ C \geq 1. \tag{3.2}$$

We have the following results.

Theorem 3.1.1. *The only integer solutions* (C, n, x, y) *of the Diophantine equation*

$$x^2 + C = 4y^n,\ \ x, y \geq 1,\ \ \gcd(x, y) = 1,\ \ n \geq 3,\ \ C \equiv 3 \mod 4,\ \ 1 \leq C \leq 100 \tag{3.3}$$

are given in the following table:

$(3, n, 1, 1)$	$(3, 3, 37, 7)$	$(7, 3, 5, 2)$	$(7, 5, 11, 2)$
$(7, 13, 181, 2)$	$(11, 5, 31, 3)$	$(15, 4, 7, 2)$	$(19, 7, 559, 5)$
$(23, 3, 3, 2)$	$(23, 3, 29, 6)$	$(23, 3, 45, 8)$	$(23, 3, 83, 12)$
$(23, 3, 7251, 236)$	$(23, 9, 45, 2)$	$(31, 3, 1, 2)$	$(31, 3, 15, 4)$
$(31, 3, 63, 10)$	$(31, 3, 3313, 140)$	$(31, 6, 15, 2)$	$(35, 4, 17, 3)$
$(39, 4, 5, 2)$	$(47, 5, 9, 2)$	$(55, 4, 3, 2)$	$(59, 3, 7, 3)$
$(59, 3, 21, 5)$	$(59, 3, 525, 41)$	$(59, 3, 28735, 591)$	$(63, 4, 1, 2)$
$(63, 4, 31, 4)$	$(63, 8, 31, 2)$	$(71, 3, 235, 24)$	$(71, 7, 21, 2)$
$(79, 3, 265, 26)$	$(79, 5, 7, 2)$	$(83, 3, 5, 3)$	$(83, 3, 3785, 153)$
$(87, 3, 13, 4)$	$(87, 3, 1651, 88)$	$(87, 6, 13, 2)$	$(99, 4, 49, 5)$

Table 3.1: Solutions for $1 \leq C \leq 100$.

Theorem 3.1.2. • *The only integer solutions of the Diophantine equation*

$$x^2 + 7^a \cdot 11^b = 4y^n,\ \ x, y \geq 1,\ \ \gcd(x, y) = 1,\ \ n \geq 3,\ \ a, b \geq 0 \tag{3.4}$$

are:

$5^2 + 7^1 \cdot 11^0 = 4 \cdot 2^3$, $11^2 + 7^1 \cdot 11^0 = 4 \cdot 2^5$, $31^2 + 7^0 \cdot 11^1 = 4 \cdot 3^5$,
$57^2 + 7^1 \cdot 11^2 = 4 \cdot 4^5$, $13^2 + 7^3 \cdot 11^0 = 4 \cdot 2^7$, $57^2 + 7^1 \cdot 11^2 = 4 \cdot 2^{10}$
$181^2 + 7^1 \cdot 11^0 = 4 \cdot 2^{13}$.

- *The only integer solutions of the Diophantine equation*

$$x^2 + 7^a \cdot 13^b = 4y^n, \quad x, y \geq 1, \quad \gcd(x, y) = 1, \quad n \geq 3, \quad a, b \geq 0 \tag{3.5}$$

are:

$5^2 + 7^1 \cdot 13^0 = 4 \cdot 2^3$, $5371655^2 + 7^3 \cdot 13^2 = 4 \cdot 19322^3$, $11^2 + 7^1 \cdot 13^0 = 4 \cdot 2^5$,
$13^2 + 7^3 \cdot 13^0 = 4 \cdot 2^7$, $87^2 + 7^3 \cdot 13^2 = 4 \cdot 4^7$, $181^2 + 7^1 \cdot 13^0 = 4 \cdot 2^{13}$,
$87^2 + 7^3 \cdot 13^2 = 4 \cdot 2^{14}$.

The plan of the paper is the following. In Section 3.2, we prove an important result using the theory of primitive divisors for Lucas sequences that will turn out to be very useful for the rest of the paper. We then find all the solutions of equation (3.2) for $1 \leq C \leq 100$ and $C \equiv 3 \mod 4$ in Section 3.3. In fact, using the results from Section 3.2, for each positive $C \leq 100$ with $C \equiv 3 \mod 4$, we transform equation (3.2) into several elliptic curves that we solve using MAGMA except for the values $C = 47, 71, 79$ for which a class number issue appears. For these remaining cases, we transform equation (3.2) into Thue equations that we solve with PARI/GP. In the last section, we study equations (3.4) and (3.5). We note that taking (3.4) modulo 4 we get that $a+b$ is odd and taking (3.4) modulo 4 we have that a is odd. We will use these facts in the computations. For $n = 3,\ 4$, we turn these equations into elliptic curves on which we need to compute $\mathcal{S}$-integer points for some small sets $\mathcal{S}$ of places of $\mathbb{Q}$. These computations are done with MAGMA. For the remaining values of n, we use the theory of Section 3.2.

3.2 Auxiliary results

Clearly, if (x, y, C, n) is a solution of the Diophantine equation (3.2) and $d \geq 3$ is any divisor of n, then $(x, y^{n/d}, C, d)$ is also a solution of equation (3.2). Since $n \geq 3$, it follows that n either has an odd prime divisor d, or n is a multiple of $d = 4$. We replace n by d and from now on we assume that n is either 4 or an odd prime.

Let α and β be distinct numbers such that $\alpha + \beta = r$ and $\alpha\beta = s$ are coprime nonzero integers. We assume that α/β is not a root of 1, which amounts to $(r, s) \neq (1, -1),\ (-1, -1)$. We write $\Delta = (\alpha - \beta)^2 = r^2 - 4s$. The Lucas sequence of roots $\alpha,\ \beta$ is the sequence of general term

$$u_m = \frac{\alpha^m - \beta^m}{\alpha - \beta} \qquad \text{for all } m \geq 0.$$

Given $m > 3$, a primitive prime factor of u_m is a prime p such that $p \mid u_m$ but $p \nmid \Delta \prod_{1 \leq k \leq m-1} u_k$. Whenever it exists, it is odd and it has the property that

$p \equiv \pm 1 \pmod{m}$. More precisely, $p \equiv \left(\frac{\Delta}{p}\right) \pmod{m}$, where, as usual, $\left(\frac{a}{p}\right)$ stands for the Legendre symbol of a with respect to p. The Primitive Divisor Theorem asserts that if $m \notin \{1, 2, 3, 4, 6\}$, then u_m always has a primitive divisor except for a finite list of triples (α, β, m), all of which are known (see [1] and [11]). One of our work-horses is the following result whose proof is based on the Primitive Divisor Theorem.

Lemma 3.2.1. *Let C be a positive integer satisfying $C \equiv 3 \mod 4$, which we write as $C = cd^2$, where c is square-free. Suppose that (x, y, C, n) is a solution to the equation (3.2), where $n \geq 5$ is prime. Let $\alpha = (x + i\sqrt{c}d)/2$, $\beta = (x - i\sqrt{c}d)/2$ and let $\mathbb{K} = \mathbb{Q}[\alpha]$. Then one of the following holds:*

(i) n divides the class number of $\mathbb{K}$.

(ii) There exist complex conjugated algebraic integers u and v in $\mathbb{K}$ such that the nth term of the Lucas sequence with roots u and v has no primitive divisors.

(iii) There exists a prime $q \mid d$ not dividing c such that $q \equiv \left(\frac{c}{q}\right) \pmod{n}$.

Proof. The proof is immediate. Write (3.2) as

$$\left(\frac{x + i\sqrt{c}d}{2}\right)\left(\frac{x - i\sqrt{c}d}{2}\right) = y^n.$$

Note that since $C \equiv 3 \pmod 4$, it follows that the two numbers α and β appearing in the left hand side of the above inequality are algebraic integers. Their sum is x and their product is $x^2 + C = 4y^n$, and these two integers are coprime. Passing to the level of ideals in $\mathbb{K}$, we get that the product of the two coprime ideals $\langle\alpha\rangle$ and $\langle\beta\rangle$ is an nth power of an ideal in $\mathcal{O}_{\mathbb{K}}$. Here, for $\gamma \in \mathcal{O}_{\mathbb{K}}$ we write $\langle\gamma\rangle$ for the principal ideal $\gamma\mathcal{O}_{\mathbb{K}}$ generated by γ in $\mathcal{O}_{\mathbb{K}}$. By unique factorization at the level of ideals, we get that both $\langle\alpha\rangle$ and $\langle\beta\rangle$ are nth powers of some other ideals. Unless (i) happens, both $\langle\alpha\rangle$ and $\langle\beta\rangle$ are powers of some principal ideals. Write

$$\langle\alpha\rangle = \langle u\rangle^n = \langle u^n\rangle \qquad \text{for some } u \in \mathcal{O}_{\mathbb{K}}.$$

Passing to the levels of elements, we get that α and u^n are associated. Since $\mathbb{K}$ is a complex quadratic field, the group of units in $\mathcal{O}_{\mathbb{K}}$ is finite of orders 2, 4 or 6, all coprime to n. Thus, by replacing u with a suitable associate, we get that $\alpha = u^n$. Conjugating, we get $\beta = v^n$, where $v = \overline{u}$. Thus,

$$u^n - v^n = \alpha - \beta = i\sqrt{c}d.$$

Now clearly, $u - v = i\sqrt{c}d_1$ for some integer d_1. Thus,

$$\frac{u^n - v^n}{u - v} = \frac{d}{d_1} \mid d.$$

The left hand side is the nth term of a Lucas sequence. Unless (ii) happens for this sequence, the left hand side above has a primitive divisor as a Lucas sequence. This primitive divisor q does not divide cd_1 (since c is a divisor of $\Delta = (u-v)^2 = cd_1^2$). It clearly must divide d and it satisfies $q \equiv \left(\frac{c}{q}\right) \pmod{n}$, which is precisely (iii). □

3.3 Proof of Theorem 3.1.1

• First, we suppose that $n = 3$. Then for each positive integer $C \leq 100$ which is congruent to 3 mod 4, equation (3.2) becomes

$$Y^2 = X^3 + C_1, \tag{3.6}$$

where $X = 4y,\ Y = 4x,\ C_1 = -16C$. We use the MAGMA function `IntegralPoints` to find all the solutions in Table 3.1 with $n = 3$.

• Secondly, we suppose that $n = 4$. Then for each positive integer $C \leq 100$ which is congruent to 3 mod 4 we solve equation (3.2) using the MAGMA function
`IntegralQuarticPoints` by transforming it first into

$$Y^2 = X^4 + C_1, \tag{3.7}$$

where $X = 2x,\ Y = 2y,\ C_1 = -4C$. In case (C, n, x, y) is a solution such that y is a power of an integer, i.e. $y = y_1^k$, then (C, nk, x, y_1) is also a solution.

• Thirdly, we consider the case when $n \geq 5$ is prime. For each positive integer $C \leq 100$ which is congruent to 3 mod 4, we write $C = cd^2$ and look at $\mathbb{K} = \mathbb{Q}[ic^{1/2}]$. The class numbers of the resulting fields are $h = 1, 2, 3, 4, 6, 8$ except for $C = 47, 79$ for which $h = 5$, and $C = 71$ for which $h = 7$, respectively. We will study later the equations

$$x^2 + 47 = 4y^5, \qquad x^2 + 79 = 5y^5, \qquad x^2 + 71 = 4y^7. \tag{3.8}$$

For the time being, we assume that item (i) of Lemma 3.2.1 is fulfilled. We next look at items (ii) and (iii) of Lemma 3.2.1. If (iii) holds, then we get some n^{th} member of a Lucas sequence whose prime factors are among the primes in d. But $100 > C = cd^2 \geq 3d^2$, so $d \leq 5$. Since also $n \geq 5$, it is impossible

that this n^{th} member of the Lucas sequence has primitive divisors. So, item (iii) cannot happen. For item (ii) of Lemma 2.1, we checked in the tables in Bilu-Hanrot-Voutier [11] and Abouzaid [1], and we obtain the solutions in Table 3.1. It remains to study the three exceptional equations appearing in (3.8).

3.3.1 The equation $x^2 + 47 = 4y^n$

Here, we reduce the equation $x^2 + 47 = 4y^n$ to some Thue equations.

As we have seen, it suffices to assume that $n = p = 5$. The minimal polynomial of $\theta = (1 + i\sqrt{47})/2$ is

$$(x - (1 - i\sqrt{47})/2)(x - (1 + i\sqrt{47})/2) = x^2 - x + (1 + 47)/4 = x^2 - x + 12.$$

Modulo 2 this polynomial has $x = 0$ and $x = 1$ as solutions. Hence, with $\mathbb{K} = \mathbb{Q}[i\sqrt{47}]$, in $\mathcal{O}_{\mathbb{K}}$ we have

$$\langle 2 \rangle = I_1 I_2,$$

where $I_1 = \langle \theta, 2 \rangle = \langle (1 + i\sqrt{47})/2, 2 \rangle$ and $I_2 = \langle \theta - 1, 2 \rangle = \langle (1 - i\sqrt{47})/2, 2 \rangle$. Note that I_1 is not principal since if it were, then we would have

$$I_1 = \langle \alpha \rangle \qquad \text{for some } \alpha \in \mathcal{O}_{\mathbb{K}}.$$

Write $\alpha = (u + iv\sqrt{47})/2$, where $u \equiv v \pmod 2$. Taking norms, we get that

$$N_{\mathbb{K}}(I_1) = N_{\mathbb{K}}(\langle \alpha \rangle) = N_{\mathbb{K}}(\alpha) = \frac{u^2 + 47v^2}{4},$$

while clearly $N_{\mathbb{K}}(I_1) = 2$. Thus, we get

$$u^2 + 47v^2 = 8,$$

and this has no integer solution (u, v). Since the class number of $\mathbb{K}$ is 5, we get that $I_1^5 = \langle \alpha \rangle$. To compute $\alpha = (u + iv\sqrt{47})/2$, we take again norms and get that

$$2^5 = N_{\mathbb{K}}(I_1^5) = N_{\mathbb{K}}(\alpha) = \frac{u^2 + 47v^2}{4},$$

giving

$$128 = u^2 + 47v^2, \tag{3.9}$$

whose solutions are $(u, v) = (\pm 9, \pm 1)$. Now one checks that if we take $(u, v) = (9, 1)$, then with $\beta = (9 + i\sqrt{47})/2 = \theta + 4$, we have

$$I_1^5 = \langle \beta \rangle.$$

This can also be checked directly as follows:

$$I_1^2 = \langle \theta^2, 2\theta, 4\rangle = \langle \theta - 12, 2(\theta - 12) + 24, 4\rangle = \langle \theta - 12, 4\rangle = \langle \theta, 4\rangle,$$

so

$$I_1^4 \;=\; \langle \theta, 4\rangle^2 = \langle \theta^2, 4\theta, 16\rangle = \langle \theta + 4, 4(\theta + 4) - 16, 16\rangle = \langle \theta + 4, 16\rangle,$$

therefore

$$I_1^5 \;=\; \langle \theta, 2\rangle\langle \theta + 4, 16\rangle = \langle \theta + 4, 32\rangle = \langle \beta\rangle,$$

since $32 = \beta\overline{\beta}$.

Now back to our equation

$$x^2 + 47 = 4y^5,$$

which we rewrite as

$$\left(\frac{x + i\sqrt{47}}{2}\right)\left(\frac{1 - i\sqrt{47}}{2}\right) = y^5.$$

Passing to the level of ideals, we get that if $\alpha = (x + i\sqrt{47})/2$, then $\langle\alpha\rangle = I^5$ for some ideal I. If I sits in the principal class, then $I = \langle\gamma\rangle$ for some $\gamma \in \mathcal{O}_{\mathbb{K}}$. Thus,

$$\langle\alpha\rangle = \langle\gamma^5\rangle.$$

A question of units does not appear since the group of units in $\mathbb{K}$ is $\{\pm 1\}$, so up to replacing γ by $-\gamma$, we get that

$$\alpha = \gamma^5.$$

Conjugating and subtracting the resulting relations we get

$$i\sqrt{47} = \alpha - \overline{\alpha} = \gamma^5 - \overline{\gamma}^5.$$

Since $\gamma = (u + iv\sqrt{47})/2$ for some integers u and v which are congruent modulo 2, we get that $\gamma - \overline{\gamma} = iv\sqrt{47}$. Thus,

$$\frac{1}{v} = \frac{\gamma^5 - \overline{\gamma}^5}{\gamma - \overline{\gamma}}.$$

This leads to $v = \varepsilon \in \{\pm 1\}$, and later to

$$\pm 1 = \frac{(u + i\varepsilon\sqrt{47})^5 - (u - i\varepsilon\sqrt{47})^5}{2^5 i\sqrt{47}} \qquad \varepsilon \in \{\pm 1\},$$

two polynomial equations of degree 4 in u which have no rational root. This case can also be read from the Primitive Divisor Theorem since then $(\gamma^5-\overline{\gamma}^5)/(\gamma-\overline{\gamma}) = \pm 1$ is the 5th member of a Lucas sequence without primitive divisors. We get no solution in this case.

Assume now that I does not sit in the principal class. Since the class number is 5, the class group is $\mathbb{Z}/5\mathbb{Z}$, and a system of representatives for its nonzero elements are I_1, I_1^2, I_2, I_2^2. Indeed, $I_2 = \overline{I_1}$ sits in the class of I_1^{-1} since $I_1 I_2 = \langle 2 \rangle$. Similarly, I_2^2 sits in the class of I_1^{-2}.

Say that the inverse of I sits in the class of I_1. Then

$$I_1^5 \langle \alpha \rangle = (I_1 I)^5 = \langle \gamma^5 \rangle$$

for some $\gamma \in \mathcal{O}_{\mathbb{K}}$. But $I_1^5 = \langle \beta \rangle$, therefore

$$I_1^5 \langle \alpha \rangle = \langle \alpha\beta \rangle = \left\langle \frac{9x - 47 + i(x+9)\sqrt{47}}{4} \right\rangle.$$

Hence, up to replacing γ by $-\gamma$, we get that

$$\frac{9x - 47 + i(x+9)\sqrt{47}}{4} = \gamma^5.$$

With $\gamma = (u + iv\sqrt{47})/2$, we have

$$\frac{9x - 47 + i(x+9)\sqrt{47}}{4} = \left(\frac{u + iv\sqrt{47}}{2} \right)^5.$$

Identifying real and imaginary parts, we have

$$\begin{aligned} \frac{9x - 47}{4} &= \frac{1}{32}(u^5 - 470u^3v^2 + 11045uv^4); \\ \frac{x+9}{4} &= \frac{1}{32}(5u^4v - 470u^2v^3 + 2209v^5). \end{aligned}$$

Multiplying the second equation by 9 and subtracting it from the first one to eliminate x, we get

$$-1024 = u^5 - 45u^4v - 470u^3v^2 + 4230u^2v^3 + 11045uv^4 - 19881v^5. \quad (3.10)$$

Assume now that the inverse of I sits in the class of I_2. Then

$$I_2^5 \langle \alpha \rangle = (I_2 I)^5 = \langle \gamma^5 \rangle.$$

Since $I_2 = \langle \overline{\beta} \rangle$, we get that

$$I_2^5 \langle \alpha \rangle = \langle \alpha \overline{\beta} \rangle = \left\langle \frac{9x + 47 + i(9-x)i\sqrt{47}}{4} \right\rangle.$$

Up to replacing γ by $-\gamma$, we may assume that

$$\frac{9x + 47 + i(9-x)\sqrt{47}}{4} = \gamma^5 = \left(\frac{u + iv\sqrt{47}}{2} \right)^5.$$

Identifying real and imaginary parts, we get

$$\begin{aligned} \frac{9x+47}{4} &= \frac{1}{32}(u^5 - 470u^3v^2 + 11045uv^4); \\ \frac{9-x}{4} &= \frac{1}{32}(5u^4v - 470u^2v^3 + 2209v^5). \end{aligned}$$

Multiplying the second one by 9 and adding it to the first, we get

$$1024 = u^5 + 45u^4v - 470u^3v^2 - 4230u^2v^3 + 11045uv^4 + 19881v^5. \quad (3.11)$$

By replacing v by $-v$, the right hand side above becomes the right hand side of equation (3.10). So, we only need to solve

$$\pm 1024 = u^5 - 45u^4v - 470u^3v^2 + 4230u^2v^3 + 11045uv^4 - 19881v^5. \quad (3.12)$$

We use PARI/GP [25] to solve these Thue equations and the solutions found are $(u, v) = (\pm 4, 0)$. This gives us the solution $(x, y) = (9, 2)$.

Assume now that the inverse of I sits in the class of $I_1^2 = \langle \beta^2 \rangle$. Then, by a similar argument, we get that

$$\alpha\beta^2 = \gamma^5$$

for some $\gamma \in \mathcal{O}_{\mathbb{K}}$. Note that

$$\alpha\beta^2 = \frac{17x - 423 + i(9x+17)\sqrt{47}}{4}.$$

Writing $\gamma = (u + iv\sqrt{47})/2$ and identifying real and imaginary parts, we have

$$\begin{aligned} \frac{17x-423}{4} &= \frac{1}{32}(u^5 - 470u^3v^2 + 11045uv^4); \\ \frac{9x+17}{4} &= \frac{1}{32}(5u^4v - 470u^2v^3 + 2209v^5). \end{aligned}$$

Multiplying the first equation by 9, the second by 17, and subtracting the resulting equations, we get

$$-2^{15} = 9u^5 - 85u^4v - 4230u^3v^2 + 7990u^2v^3 + 99405uv^4 - 37553v^5.$$

Finally, the case when the inverse class of I is in the class of I_2^2 will lead, up to replacing v by $-v$, to the same equation as the last one above except that its right hand side is 2^{15}. Hence, we get

$$\pm 32768 = 9u^5 - 85u^4v - 4230u^3v^2 + 7990u^2v^3 + 99405uv^4 - 37553v^5. \quad (3.13)$$

With PARI/GP, we deduce that these Thue equations have no solutions.

3.3.2 The equation $x^2 + 79 = 4y^n$

The same argument works for 79. We will only sketch the proof without too many details. Here, $2^7 = 7^2 + 79$. We take

$$\alpha = (x + i\sqrt{79})/2 \text{ and } \beta = (7 + i\sqrt{79})/2.$$

If the ideal generated by α in $\mathcal{O}_{\mathbb{K}}$ is the fifth power of a principal ideal, then

$$\alpha = \gamma^5$$

with some $\gamma = (u + iv\sqrt{79})/2$, with $u \equiv v \pmod 2$. We then get that $v = \pm 1$ and

$$\frac{\gamma^5 - \overline{\gamma}^5}{\gamma - \overline{\gamma}} = \pm 1,$$

which is impossible by the Primitive Divisor Theorem and the tables in Bilu-Hanrot-Voutier [11] and Abouzaid [1].

So, we only need to distinguish two remaining cases:

Case 1. $\alpha\beta$ is a fifth power in $\mathbb{K}$.

We then get

$$\alpha\beta = \frac{7x - 79 + i(x+7)\sqrt{79}}{4} = \left(\frac{u + iv\sqrt{79}}{2}\right)^5.$$

Identifying real and imaginary parts, we have

$$\begin{aligned} \frac{7x - 79}{4} &= \frac{1}{32}(u^5 - 790u^3v^2 + 31205uv^4); \\ \frac{x+7}{4} &= \frac{1}{32}(5u^4v - 790u^2v^3 + 6241v^5). \end{aligned}$$

Multiplying the second equation by 7 and subtracting it from the first one leads to

$$-1024 = u^5 - 35u^4v - 790u^3v^2 + 5530u^2v^3 + 31205uv^4 - 43687v^5. \quad (3.14)$$

When $\alpha\overline{\beta}$ is a fifth power in $\mathbb{K}$, one is lead to a similar equation as above but with the positive sign in the left hand side. We use PARI/GP to solve these Thue equations. The resulting solutions are $(u, v) = (\pm 4, 0)$. This gives us the solution $(x, y) = (7, 2)$.

Case 2. $\alpha\beta^2$ is a fifth power in $\mathbb{K}$.

We then get

$$\alpha\beta^2 = \frac{-15x - 553 + i(7x + 15)\sqrt{79}}{4} = \left(\frac{u + iv\sqrt{79}}{2}\right)^5.$$

Identifying real and imaginary parts, we have

$$\begin{aligned} \frac{-15x - 553}{4} &= \frac{1}{32}(u^5 - 790u^3v^2 + 31205uv^4); \\ \frac{7x + 15}{4} &= \frac{1}{32}(5u^4v - 790u^2v^3 + 6241v^5). \end{aligned}$$

Eliminating x gives

$$-32768 = 7u^5 + 75u^4v - 5530u^3v^2 - 1180u^2v^3 + 218435uv^4 + 93615v^5. \quad (3.15)$$

When $\alpha\overline{\beta}^2$ is a fifth power in $\mathbb{K}$, then the resulting Thue equation has the same right hand side but the sign on the left hand side is positive. These Thue equations have no solutions.

3.3.3 The equation $x^2 + 71 = 4y^n$

We use the same method. Here, $21^2 + 71 = 2^9$, so we take

$$\alpha = (x + i\sqrt{71})/2 \text{ and } \beta = (21 + i\sqrt{71})/2.$$

With $\gamma = (u + iv\sqrt{71})/2$, we get again three possibilities.

If

$$\alpha = \gamma^7,$$

then

$$\frac{\gamma^7 - \overline{\gamma}^7}{\gamma - \overline{\gamma}} = \pm 1.$$

This is impossible by the Primitive Divisor Theorem.

Next, assume that

$$\alpha\beta = \frac{21x - 71 + i(x + 21)\sqrt{71}}{4} = \left(\frac{u + iv\sqrt{71}}{2}\right)^7.$$

Identifying real and imaginary parts, we have

$$\begin{aligned} \frac{21x-71}{4} &= \frac{1}{128}(u^7 - 1491u^5v^2 + 176435u^3v^4 - 2505377uv^6); \\ \frac{x+21}{4} &= \frac{1}{128}(7u^6v - 2485u^4v^3 + 105861u^2v^5 - 357911v^7). \end{aligned}$$

To eliminate x, we multiply the second equation by 21 and subtract the resulting equation from the first one. We get

$$\begin{aligned} \pm 16384 = u^7 - 147u^6v - 1491u^5v^2 + 52185u^4v^3 + 176435u^3v^4 \\ -2223081u^2v^5 - 2505377uv^6 + 7516131v^7. \end{aligned} \tag{3.16}$$

The sign + appears in the left hand side when $\alpha\overline{\beta} = \gamma^7$. We use PARI/GP to solve these Thue equations and obtain the solutions $(u, v) = (\pm 4, 0)$. We get the solution $(x, y) = (21, 2)$.

Next, suppose that

$$\alpha\beta^2 = \frac{185x - 1491 + i(21x + 185)\sqrt{71}}{4} = \left(\frac{u + iv\sqrt{71}}{2}\right)^7.$$

Identifying real and imaginary parts, we have

$$\begin{aligned} \frac{185x-1491}{4} &= \frac{1}{128}(u^7 - 1491u^5v^2 + 176435u^3v^4 - 2505377uv^6); \\ \frac{21x+185}{4} &= \frac{1}{128}(7u^6v - 2485u^4v^3 + 105861u^2v^5 - 357911v^7). \end{aligned}$$

We eliminate x to obtain

$$\begin{aligned} \pm 2097152 = 21u^7 - 1295u^6v - 31311u^5v^2 + 459725u^4v^3 \\ +3705135u^3v^4 - 19584285u^2v^5 - 52612917uv^6 + 66213535v^7. \end{aligned} \tag{3.17}$$

The sign + on the left hand side appears when $\alpha\overline{\beta}^2 = \gamma^7$. These Thue equations have no solutions.

Finally, we have

$$\alpha\beta^3 = \frac{1197x - 22223 + i(313x + 1197)\sqrt{71}}{4} = \left(\frac{u + iv\sqrt{71}}{2}\right)^7.$$

Identifying real and imaginary parts, we get

$$\begin{aligned} \frac{1197x-22223}{4} &= \frac{1}{128}(u^7 - 1491u^5v^2 + 176435u^3v^4 - 2505377uv^6); \\ \frac{313x+1197}{4} &= \frac{1}{128}(7u^6v - 2485u^4v^3 + 105861u^2v^5 - 357911v^7). \end{aligned}$$

We eliminate x to obtain

$$\pm 268435456 = 313u^7 - 8379u^6v - 466683u^5v^2 + 2974545u^4v^3 + 55224155u^3v^4 - 126715617u^2v^5 - 784183001uv^6 + 428419467v^7. \tag{3.18}$$

Again the sign + in the left hand side appears when $\alpha\overline{\beta}^3 = \gamma^7$. We checked that these last Thue equations (3.18) are all impossible modulo 43.

This finishes the proof of Theorem 1.1.

3.4 Proof of Theorem 3.1.2

3.4.1 The equation (3.4)

First we deal with the cases $n \in \{3, 4\}$.

- The case $n = 3$. We transform equation (3.4) as follows

$$X^2 = Y^3 - 4^2 \cdot 7^{a_1} \cdot 11^{b_1},$$

where $a_1, b_1 \in \{0, 1, 2, 3, 4, 5\}$. Now we need to determine all the $\{7, 11\}$-points on the above 36 elliptic curves. The coefficients are getting too large making the computations time consuming. Thus, we use a different approach instead. We give the details in case of equation (3.4). We have

$$\frac{x + 7^\alpha 11^\beta\sqrt{-7}}{2} = \left(\frac{u + v\sqrt{-7}}{2}\right)^3, \quad \text{or}$$

$$\frac{x + 7^\alpha 11^\beta\sqrt{-11}}{2} = \left(\frac{u + v\sqrt{-11}}{2}\right)^3.$$

After subtracting the conjugate equation we obtain

$$4 \cdot 7^\alpha 11^\beta = 3u^2v - 7v^3,$$
$$4 \cdot 7^\alpha 11^\beta = 3u^2v - 11v^3.$$

In case of the first equation one can easily see that $11 \mid v$, and in the latter case that $7 \mid v$. Therefore, we have $v \in \{\pm 11^\beta, \pm 4 \cdot 11^\beta, \pm 7^\alpha \cdot 11^\beta, \pm 4 \cdot 7^\alpha \cdot 11^\beta\}$, and $v \in \{\pm 7^\alpha, \pm 4 \cdot 7^\alpha, \pm 7^\alpha \cdot 11^\beta, \pm 4 \cdot 7^\alpha \cdot 11^\beta\}$, respectively.

If $v = \pm 11^\beta$, then we get that $\alpha \in \{0, 1\}$, and it is sufficient to solve the following equations

$$3u^2 = 7V^4 \pm 4,$$
$$3u^2 = 7V^4 \pm 28,$$
$$3u^2 = 7 \cdot 11^2V^4 \pm 4,$$
$$3u^2 = 7 \cdot 11^2V^4 \pm 28,$$

with $V = 11^k$. Here and in what follows, $k = \lfloor \beta/2 \rfloor$. We use the MAGMA [12] software and its function `SIntegralLjunggrenPoints` to determine all integral points on the above curves. We obtain $(u, v) = (\pm 1, \pm 1)$. Thus, $(x, y) = (5, 2)$.

If $v = \pm 4 \cdot 11^\beta$, then we get that $\alpha \in \{0, 1\}$, and it is sufficient to solve the following equations

$$\begin{aligned} 3u^2 &= 7V^4 \pm 1, \\ 3u^2 &= 7V^4 \pm 7, \\ 3u^2 &= 7 \cdot 11^2 V^4 \pm 1, \\ 3u^2 &= 7 \cdot 11^2 V^4 \pm 7, \end{aligned}$$

with $V = 2 \cdot 11^k$. These equations do not yield any solutions.

If $v = \pm 7^\alpha \cdot 11^\beta$, then the equations we need to solve are

$$\begin{aligned} 3u^2 &= 7V^4 \pm 4, \\ 3u^2 &= 7^3 V^4 \pm 4, \\ 3u^2 &= 7 \cdot 11^2 V^4 \pm 4, \\ 3u^2 &= 7^3 \cdot 11^2 V^4 \pm 4, \end{aligned}$$

with $V = 11^k$. We do not get new solutions.

If $v = \pm 4 \cdot 7^\alpha \cdot 11^\beta$, then the equations we need to solve are

$$\begin{aligned} 3u^2 &= 7V^4 \pm 1, \\ 3u^2 &= 7^3 V^4 \pm 1, \\ 3u^2 &= 7 \cdot 11^2 V^4 \pm 1, \\ 3u^2 &= 7^3 \cdot 11^2 V^4 \pm 1, \end{aligned}$$

with $V = 2 \cdot 11^k$. We do not get new solutions.

The cases $v \in \{\pm 7^\alpha, \pm 4 \cdot 7^\alpha, \pm 7^\alpha \cdot 11^\beta, \pm 4 \cdot 7^\alpha \cdot 11^\beta\}$ can be handled in a similar way. The only solution of equation (3.4) with $n = 3$ is

$$5^2 + 7^1 \cdot 11^0 = 4 \cdot 2^3.$$

- The case $n = 4$. We can rewrite equation (3.4) as follows:

$$x^2 = 4y^4 - 7^\alpha 11^\beta, \quad \text{where } \alpha, \beta \in \{0, 1, 2, 3\}, \quad \mathcal{S} = \{7, 11\}.$$

The problem can now be solved by applying standard algorithms for computing $\mathcal{S}$-integral points on elliptic curves (see, for example, [26]). We use the MAGMA

[12] function `SIntegralLjunggrenPoints` to determine all $\mathcal{S}$-integral points on the above curves. No solution of equation (3.4) was found.

- If $n \geq 5$ is a prime, then by Lemma 3.2.1, it follows easily that $n = 5$, or

$$(y, n) \in \{(2,7), (2,13), (3,7), (4,7), (5,7)\}.$$

A short calculation assures that the class number of $\mathbb{K}$ belongs to $\{1\}$, where $\mathbb{K} = \mathbb{Q}[i\sqrt{d}]$ with $d \in \{7, 11\}$.

- The case $n = 5$. We describe the method in case of equation (3.4). We have

$$\frac{x + 7^{\alpha}11^{\beta}\sqrt{-7}}{2} = \left(\frac{u + v\sqrt{-7}}{2}\right)^5, \quad \text{or}$$
$$\frac{x + 7^{\alpha}11^{\beta}\sqrt{-11}}{2} = \left(\frac{u + v\sqrt{-11}}{2}\right)^5.$$

After subtracting the conjugate equation we obtain

$$16 \cdot 7^{\alpha}11^{\beta} = v(5u^4 - 70u^2v^2 + 49v^4),$$
$$16 \cdot 7^{\alpha}11^{\beta} = v(5u^4 - 110u^2v^2 + 121v^4).$$

Therefore v is composed by the primes $2, 7$ and 11. We rewrite the above equations as follows

$$Y^2 = \pm 2^{a_1}7^{a_2}11^{a_3}(5X^4 - 70X^2 + 49),$$
$$Y^2 = \pm 2^{a_1}7^{a_2}11^{a_3}(5X^4 - 110X^2 + 121),$$

where $a_i \in \{0, 1\}$. Many of these equations do not have solutions in $\mathbb{Q}_p$ for some prime p. We use the MAGMA [12] function `SIntegralLjunggrenPoints` to determine all $\{2, 7, 11\}$-integral points on the remaining curves. We obtain the following solutions

curve	$\{2,7,11\}$-integral points
$Y^2 = -11(5X^4 - 70X^2 + 49)$	$(\pm 3, \pm 44), (\pm\frac{3}{2}, \pm\frac{121}{4})$
$Y^2 = -(5X^4 - 70X^2 + 49)$	$(\pm 1, \pm 4)$
$Y^2 = 5X^4 - 70X^2 + 49$	$(0, 7)$
$Y^2 = 11(5X^4 - 70X^2 + 49)$	$(\pm 7, \pm 308)$
$Y^2 = 5X^4 - 110X^2 + 121$	$(0, \pm 11), (\pm 1, \pm 4)$

We use the above points on the elliptic curves to find the corresponding solutions of equation (3.4). For example, the solution $(X, Y) = (3, 44)$ of the

first elliptic curve gives the solution $(n, a, b, x, y) = (5, 1, 2, 57, 4)$. The solution $(X, Y) = (1, 4)$ of the second elliptic curve yields the solution $(n, a, b, x, y) = (5, 1, 0, 11, 2)$. The solution $(n, a, b, x, y) = (5, 0, 1, 31, 3)$ is obtained from the solution $(X, Y) = (1, 4)$ of the last elliptic curve, while the solution $(n, a, b, x, y) = (10, 1, 2, 57, 2)$ is obtained easily from the solution $(n, a, b, x, y) = (5, 1, 2, 57, 4)$.

- The case $n > 5$. Here, by Lemma 3.2.1, we have

$$(y, n) \in \{(2, 7), (2, 13), (3, 7), (4, 7), (5, 7)\}.$$

We provide the details of the computations in case of equation (3.4). It remains to find all integral points on the following elliptic curves

$$Y^2 = X^3 + 4 \cdot 7^{2\alpha} 11^{2\beta} y^n,$$

where $0 \leq \alpha, \beta \leq 2$ and $(y, n) \in \{(2, 7), (2, 13), (3, 7), (4, 7), (5, 7)\}$. Using MAGMA, we get the following solutions.

(α, β)	$(2, 7)$	$(2, 13)$	$(3, 7)$
$(0, 0)$	$X \in \{\pm 8, -7, 4, 184\}$	$X \in \{\pm 32, -28, 16, 736\}$	$X \in \{-18, 117\}$
$(0, 1)$	$X \in \{-28\}$	$X \in \{-112\}$	$X \in \{-99, -18, 22, 198\}$
$(0, 2)$	$\emptyset$	$\emptyset$	$\emptyset$
$(1, 0)$	$X \in \{-28, 8, 56, 497\}$	$X \in \{-112, -7, 32, 224, 1988\}$	$X \in \{198\}$
$(1, 1)$	$X \in \{-28, 56, 1736, 61037816\}$	$X \in \{-112, 224, 6944, 244151264\}$	$X \in \{198, 333, 15598\}$
$(1, 2)$	$\emptyset$	$\emptyset$	$\emptyset$
$(2, 0)$	$X \in \{392\}$	$X \in \{1568\}$	$X \in \{-234\}$
$(2, 1)$	$X \in \{-503, -392, 49, 2744\}$	$X \in \{-2012, -1568, 196, 5537, 10976\}$	$X \in \{198, 37566\}$
$(2, 2)$	$\emptyset$	$\emptyset$	$\emptyset$

(α, β)	$(4, 7)$	$(5, 7)$
$(0, 0)$	$X \in \{0\}$	$\emptyset$
$(0, 1)$	$X \in \{0\}$	$X \in \{-275\}$
$(0, 2)$	$X \in \{0\}$	$\emptyset$
$(1, 0)$	$X \in \{-112, 0, 128, 420, 896\}$	$\emptyset$
$(1, 1)$	$X \in \{0\}$	$\emptyset$
$(1, 2)$	$X \in \{0, 21669648\}$	$\emptyset$
$(2, 0)$	$X \in \{0, 25872\}$	$\emptyset$
$(2, 1)$	$X \in \{-1536, 0, 1617\}$	$\emptyset$
$(2, 2)$	$X \in \{0\}$	$\emptyset$

One can check, for example, that $(y, n, \alpha, \beta, X) = (2, 7, 0, 0, -7)$ yields the solution $13^2 + 7^3 \cdot 11^0 = 4 \cdot 2^7$, while the solution $181^2 + 7^1 \cdot 11^0 = 4 \cdot 2^{13}$ is obtained from $(y, n, \alpha, \beta, X) = (2, 13, 1, 0, -7)$.

3.4.2 The equation (3.5)

We use a similar method as for equation (3.4).

- The case $n = 3$. We transform equation (3.5) as follows

$$X^2 = Y^3 - 4^2 \cdot 7^{a_1} \cdot 13^{b_1},$$

where $a_1 \in \{1,3,5\}, b_1 \in \{0,1,2,3,4,5\}$. Now we need to determine all the $\{7,13\}$-points on the above 18 elliptic curves. Among the 18 curves there are only 6 curves having rank greater than 0. MAGMA determined the appropriate Mordell-Weil groups except in case $(a_1, b_1) = (5,4)$. We deal with this case separately. The $\{7,13\}$-points on the 5 curves are as follows.

curve	(X, Y)
$X^2 = Y^3 - 4^2 \cdot 7^1 \cdot 13^0$	$(\pm 20, 8)$
$X^2 = Y^3 - 4^2 \cdot 7^1 \cdot 13^3$	$(\pm 169, 65)$
$X^2 = Y^3 - 4^2 \cdot 7^3 \cdot 13^2$	$(\pm 21486620, 77288)$
$X^2 = Y^3 - 4^2 \cdot 7^3 \cdot 13^5$	$\emptyset$
$X^2 = Y^3 - 4^2 \cdot 7^5 \cdot 13^1$	$\emptyset$

This leads to the solutions $(x, y, a, b) = (5, 2, 1, 0), (5371655, 19322, 3, 2)$.

If $(a_1, b_1) = (5, 4)$, then we obtain

$$4 \cdot 7^{3\alpha_1+2} 13^{3\beta_1+2} = v(3u^2 - 7v^2).$$

One can easily see that $13 \mid v$ and $7 \nmid u$. So, we have $v \in \{\pm 7^{3\alpha_1+2} \cdot 13^{3\beta_1+2}, \pm 4 \cdot 7^{3\alpha_1+2} \cdot 13^{3\beta_1+2}\}$.

If $v = \pm 7^{3\alpha_1+2} \cdot 13^{3\beta_1+2}$, then the equations we need to solve are

$$\begin{aligned} 3u^2 &= 7V^4 \pm 4, \\ 3u^2 &= 7^3 V^4 \pm 4, \\ 3u^2 &= 7 \cdot 13^2 V^4 \pm 4, \\ 3u^2 &= 7^3 \cdot 13^2 V^4 \pm 4. \end{aligned}$$

We do not get new solutions.

If $v = \pm 4 \cdot 7^{3\alpha_1+2} \cdot 13^{3\beta_1+2}$, then the equations we need to solve are

$$\begin{aligned} 3u^2 &= 7V^4 \pm 1, \\ 3u^2 &= 7^3 V^4 \pm 1, \\ 3u^2 &= 7 \cdot 13^2 V^4 \pm 1, \\ 3u^2 &= 7^3 \cdot 13^2 V^4 \pm 1, \end{aligned}$$

We do not get new solutions.

- The case $n = 4$. We can rewrite equation (3.5) as follows:

$$x^2 = 4y^4 - 7^\alpha 13^\beta, \quad \text{where } \alpha, \beta \in \{0,1,2,3\}, \quad \mathcal{S} = \{7,13\}.$$

As previously, we use the MAGMA [12] function `SIntegralLjunggrenPoints` to determine all the $\mathcal{S}$-integral points on the above curves. We find no solution of equation (3.5) with $n = 4$.

• If $n \geq 5$ is a prime, then by Lemma 3.2.1, we have that $n = 5$ or $(y, n) \in \{(2, 7), (2, 13), (3, 7), (4, 7), (5, 7)\}$. A short calculation assures that the class number of $\mathbb{K}$ belongs to $\{1, 2\}$, where $\mathbb{K} = \mathbb{Q}[i\sqrt{d}]$ with $d \in \{7, 91\}$.

• The case $n = 5$. Here we have

$$16 \cdot 7^{\alpha} 13^{\beta} = v(5u^4 - 70u^2v^2 + 49v^4),$$
$$16 \cdot 7^{\alpha} 13^{\beta} = v(5u^4 - 910u^2v^2 + 8281v^4).$$

Therefore v is composed by the primes $2, 7$ and 13. We rewrite the above equations as follows

$$Y^2 = \pm 2^{a_1} 7^{a_2} 13^{a_3} (5X^4 - 70X^2 + 49),$$
$$Y^2 = \pm 2^{a_1} 7^{a_2} 13^{a_3} (5X^4 - 910X^2 + 8281),$$

where $a_i \in \{0, 1\}$. Many of these equations do not have solutions in $\mathbb{Q}_p$ for some prime p. We use the MAGMA [12] function `SIntegralLjunggrenPoints` to determine all $\{2, 7, 13\}$-integral points on the remaining curves. We obtain the following solutions

curve	$\{2, 7, 13\}$-integral points
$Y^2 = 5X^4 - 70X^2 + 49$	$(0, \pm 7)$
$Y^2 = -(5X^4 - 70X^2 + 49)$	$(\pm 1, \pm 4)$
$Y^2 = 5X^4 - 910X^2 + 8281$	$(0, \pm 91)$
$Y^2 = -(5X^4 - 910X^2 + 8281)$	$(\pm 13, \pm 52)$

• The case $n > 5$. By Lemma 3.2.1, we have

$$(y, n) \in \{(2, 7), (2, 13), (3, 7), (4, 7), (5, 7)\}.$$

We find all integral points on the following elliptic curves

$$Y^2 = X^3 + 4 \cdot 7^{2\alpha} 13^{2\beta} y^n,$$

where $0 \leq \alpha, \beta \leq 2$ and $(y, n) \in \{(2, 7), (2, 13), (3, 7), (4, 7), (5, 7)\}$. Using MAGMA, we get all the solutions.

(α, β)	$(2, 7)$	$(2, 13)$	$(3, 7)$
$(0, 0)$	$X \in \{\pm 8, -7, 4, 184\}$	$X \in \{\pm 32, -28, 16, 736\}$	$X \in \{-18, 117\}$
$(0, 1)$	$X \in \{56\}$	$X \in \{224\}$	$X \in \{117\}$
$(0, 2)$	$\emptyset$	$\emptyset$	$X \in \{-338\}$
$(1, 0)$	$X \in \{-28, 8, 56, 497\}$	$X \in \{-112, -7, 32, 224, 1988\}$	$X \in \{198\}$
$(1, 1)$	$X \in \{-56\}$	$X \in \{-224\}$	$X \in \{-234\}$
$(1, 2)$	$\emptyset$	$\emptyset$	$\emptyset$
$(2, 0)$	$X \in \{392\}$	$X \in \{1568\}$	$X \in \{-234\}$
$(2, 1)$	$\emptyset$	$\emptyset$	$\emptyset$
$(2, 2)$	$X \in \{3332\}$	$X \in \{13328\}$	$\emptyset$

(α, β)	$(4, 7)$	$(5, 7)$
$(0, 0)$	$X \in \{0\}$	$\emptyset$
$(0, 1)$	$X \in \{0, 4368\}$	$\emptyset$
$(0, 2)$	$X \in \{-1183, 0, 3584\}$	$\emptyset$
$(1, 0)$	$X \in \{-112, 0, 128, 420, 896\}$	$\emptyset$
$(1, 1)$	$X \in \{-768, 0, 144, 1092, 1920, 104832\}$	$\emptyset$
$(1, 2)$	$X \in \{0\}$	$\emptyset$
$(2, 0)$	$X \in \{0, 25872\}$	$\emptyset$
$(2, 1)$	$X \in \{-2560, 0, 3185\}$	$\emptyset$
$(2, 2)$	$X \in \{0\}$	$\emptyset$

Bibliography

[1] M. Abouzaid. Les nombres de Lucas et Lehmer sans diviseur primitif. *J. Théor. Nombres Bordeaux*, 18(2):299–313, 2006.

[2] F. S. Abu Muriefah and Y. Bugeaud. The Diophantine equation $x^2 + c = y^n$: a brief overview. *Rev. Colombiana Mat.*, 40(1):31–37, 2006.

[3] F. S. Abu Muriefah, F. Luca, S. Siksek, and Sz. Tengely. On the Diophantine equation $x^2 + C = 2y^n$. *Int. J. Number Theory*, 5(6):1117–1128, 2009.

[4] F. S. Abu Muriefah, F. Luca, and A. Togbé. On the Diophantine equation $x^2 + 5^a 13^b = y^n$. *Glasg. Math. J.*, 50(1):175–181, 2008.

[5] S. A. Arif and F. S. A. Muriefah. On the Diophantine equation $x^2 + 2^k = y^n$. *Internat. J. Math. Math. Sci.*, 20(2):299–304, 1997.

[6] S. A. Arif and F. S. A. Muriefah. The Diophantine equation $x^2 + 3^m = y^n$. *Internat. J. Math. Math. Sci.*, 21(3):619–620, 1998.

[7] S. A. Arif and F. S. A. Muriefah. On a Diophantine equation. *Bull. Austral. Math. Soc.*, 57(2):189–198, 1998.

[8] S. A. Arif and F. S. A. Muriefah. The Diophantine equation $x^2 + 5^{2k+1} = y^n$. *Indian J. Pure Appl. Math.*, 30(3):229–231, 1999.

[9] S. A. Arif and F. S. A. Muriefah. The Diophantine equation $x^2 + q^{2k} = y^n$. *Arab. J. Sci. Eng. Sect. A Sci.*, 26(1):53–62, 2001.

[10] S. A. Arif and F. S. A. Muriefah. On the Diophantine equation $x^2 + q^{2k+1} = y^n$. *J. Number Theory*, 95(1):95–100, 2002.

[11] Yu. Bilu, G. Hanrot, and P. M. Voutier. Existence of primitive divisors of Lucas and Lehmer numbers. *J. Reine Angew. Math.*, 539:75–122, 2001. With an appendix by M. Mignotte.

[12] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[13] Y. Bugeaud, M. Mignotte, and S. Siksek. Classical and modular approaches to exponential Diophantine equations. II. The Lebesgue-Nagell equation. *Compos. Math.*, 142(1):31–62, 2006.

[14] J. H. E. Cohn. The Diophantine equation $x^2+C = y^n$. *Acta Arith.*, 65(4):367–381, 1993.

[15] Edray Goins, Florian Luca, and Alain Togbé. On the Diophantine equation $x^2 + 2^\alpha 5^\beta 13^\gamma = y^n$. In *Algorithmic number theory*, volume 5011 of *Lecture Notes in Comput. Sci.*, pages 430–442. Springer, Berlin, 2008.

[16] Chao Ko. On the Diophantine equation $x^2 = y^n + 1$, $xy \neq 0$. *Sci. Sinica*, 14:457–460, 1965.

[17] Maohua Le. An exponential Diophantine equation. *Bull. Austral. Math. Soc.*, 64(1):99–105, 2001.

[18] Maohua Le. On Cohn's conjecture concerning the Diophantine equation $x^2 + 2^m = y^n$. *Arch. Math. (Basel)*, 78(1):26–35, 2002.

[19] V.A. Lebesgue. Sur l'impossibilité en nombres entiers de l'équation $x^m = y^2 + 1$. *Nouv. Annal. des Math.*, 9:178–181, 1850.

[20] F. Luca. On a Diophantine equation. *Bull. Austral. Math. Soc.*, 61(2):241–246, 2000.

[21] F. Luca. On the equation $x^2 + 2^a \cdot 3^b = y^n$. *Int. J. Math. Math. Sci.*, 29(4):239–244, 2002.

[22] Florian Luca and Alain Togbé. On the Diophantine equation $x^2+2^a\cdot 5^b = y^n$. *Int. J. Number Theory*, 4(6):973–979, 2008.

[23] Florian Luca and Alain Togbé. On the Diophantine equation $x^2 + 2^\alpha 13^\beta = y^n$. *Colloq. Math.*, 116(1):139–146, 2009.

[24] M. Mignotte and B.M.M. De Weger. On the Diophantine equations $x^2 + 74 = y^5$ and $x^2 + 86 = y^5$. *Glasgow Math. J.*, 38:77–85, 1996.

[25] The PARI Group, Bordeaux. *PARI/GP, version 2.2.8*, 2004. available from http://pari.math.u-bordeaux.fr/.

[26] Attila Pethő, Horst G. Zimmer, Josef Gebel, and Emanuel Herrmann. Computing all S-integral points on elliptic curves. *Math. Proc. Cambridge Philos. Soc.*, 127(3):383–402, 1999.

[27] István Pink. On the Diophantine equation $x^2+2^\alpha 3^\beta 5^\gamma 7^\delta = y^n$. *Publ. Math. Debrecen*, 70(1-2):149–166, 2007.

[28] Sz. Tengely. On the Diophantine equation $x^2 + a^2 = 2y^p$. *Indag. Math. (N.S.)*, 15(2):291–304, 2004.

[29] Sz. Tengely. On the Diophantine equation $x^2 + q^{2m} = 2y^p$. *Acta Arith.*, 127(1):71–86, 2007.

4

Note on a paper "An Extension of a Theorem of Euler" by Hirata-Kohno et al.

*T*engely, Sz.,
Acta Arithmetica **134** (2008), 329–335.

Abstract

In this paper we extend a result of Hirata-Kohno, Laishram, Shorey and Tijdeman on the Diophantine equation $n(n+d)\cdots(n+(k-1)d) = by^2$, where $n, d, k \geq 2$ and y are positive integers such that $\gcd(n,d) = 1$.

4.1 Introduction

Let $n, d, k > 2$ and y be positive integers such that $\gcd(n,d) = 1$. For an integer $v > 1$, we denote by $P(v)$ the greatest prime factor of v and we put $P(1) = 1$. Let b be a squarefree positive integer such that $P(b) \leq k$. We consider the equation

$$n(n+d)\cdots(n+(k-1)d) = by^2 \tag{4.1}$$

in n, d, k and y.

A celebrated theorem of Erdős and Selfridge [7] states that the product of consecutive positive integers is never a perfect power. An old, difficult conjecture states that even a product of consecutive terms of arithmetic progression of length $k > 3$ and difference $d \geq 1$ is never a perfect power. Euler proved (see [6] pp. 440 and 635) that a product of four terms in arithmetic progression is never a square solving equation (7.1) with $b = 1$ and $k = 4$. Obláth [10] obtained a similar statement for $b = 1, k = 5$. Bennett, Bruin, Győry and Hajdu [1] solved (7.1) with $b = 1$ and $6 \leq k \leq 11$. For more results on this topic see [1], [8] and the references given there.

We write

$$n + id = a_i x_i^2 \text{ for } 0 \leq i < k \tag{4.2}$$

where a_i are squarefree integers such that $P(a_i) \leq \max(P(b), k-1)$ and x_i are positive integers. Every solution to (7.1) yields a k-tuple $(a_0, a_1, \ldots, a_{k-1})$. Recently Hirata-Kohno, Laishram, Shorey and Tijdeman [8] proved the following theorem.

Theorem A (Hirata-Kohno, Laishram, Shorey,Tijdeman)**.** Equation (7.1) with $d > 1, P(b) = k$ and $7 \leq k \leq 100$ implies that $(a_0, a_1, \ldots, a_{k-1})$ is among the following tuples or their mirror images.

$$\begin{aligned}
k = 7: &\quad (2,3,1,5,6,7,2),(3,1,5,6,7,2,1),(1,5,6,7,2,1,10),\\
k = 13: &\quad (3,1,5,6,7,2,1,10,11,3,13,14,15),\\
&\quad (1,5,6,7,2,1,10,11,3,13,14,15,1),\\
k = 19: &\quad (1,5,6,7,2,1,10,11,3,13,14,15,1,17,2,19,5,21,22),\\
k = 23: &\quad (5,6,7,2,1,10,11,3,13,14,15,1,17,2,19,5,21,22,23,6,1,26,3),\\
&\quad (6,7,2,1,10,11,3,13,14,15,1,17,2,19,5,21,22,23,6,1,26,3,7).
\end{aligned}$$

In case of $k = 5$ Mukhopadhyay and Shorey [9] proved the following result.

Theorem B (Mukhopadhyay, Shorey)**.** If n and d are coprime nonzero integers, then the Diophantine equation

$$n(n+d)(n+2d)(n+3d)(n+4d) = by^2$$

has no solutions in nonzero integers b, y and $P(b) \leq 3$.

In this article we solve (7.1) with $k = 5$ and $P(b) = 5$, moreover we handle the 8 special cases mentioned in Theorem A. We prove the following theorems.

Theorem 4.1.1. *Equation* (7.1) *with* $d > 1, P(b) = k$ *and* $7 \leq k \leq 100$ *has no solutions.*

Theorem 4.1.2. *Equation* (7.1) *with* $d > 1, k = 5$ *and* $P(b) = 5$ *implies that* $(n, d) \in \{(-12, 7), (-4, 3)\}$.

4.2 Preliminary lemmas

In the proofs of Theorem 4.1.2 and 4.1.1 we need several results using elliptic Chabauty's method (see [4],[5]). Bruin's routines related to elliptic Chabauty's method are contained in MAGMA [2]. Here we only indicate the main steps without explaining the background theory. To see how the method works in

practice, in particular by the help of Magma, [3] is an excellent source. To have the method work, the rank of the elliptic curve (defined over the number field K) should be strictly less than the degree of K. In the present cases it turns out that the ranks of the elliptic curves are either 0 or 1, so elliptic Chabauty's method is applicable. Further, the procedure `PseudoMordellWeilGroup` of Magma is able to find a subgroup of the Mordell-Weil group of finite odd index. We also need to check that the index is not divisible by some prime numbers provided by the procedure `Chabauty`. This last step can be done by the inbuilt function `IsPSaturated`.

Lemma 4.2.1. *Equation* (7.1) *with* $k = 7$ *and* $(a_0, a_1, \ldots, a_6) = (1, 5, 6, 7, 2, 1, 10)$ *implies that* $n = 2, d = 1$.

Proof. Using that $n = x_0^2$ and $d = (x_5^2 - x_0^2)/5$ we obtain the following system of equations

$$\begin{aligned} x_5^2 + 4x_0^2 &= 25x_1^2, \\ 4x_5^2 + x_0^2 &= 10x_4^2, \\ 6x_5^2 - x_0^2 &= 50x_6^2. \end{aligned}$$

The second equation implies that x_0 is even, that is there exists a $z \in \mathbb{Z}$ such that $x_0 = 2z$. By standard factorization argument in the Gaussian integers we get that

$$(x_5 + 4iz)(x_5 + iz) = \delta\square,$$

where $\delta \in \{-3 \pm i, -1 \pm 3i, 1 \pm 3i, 3 \pm i\}$. Thus putting $X = x_5/z$ it is sufficient to find all points (X, Y) on the curves

$$C_\delta : \quad \delta(X + i)(X + 4i)(3X^2 - 2) = Y^2, \tag{4.3}$$

where $\delta \in \{-3 \pm i, -1 \pm 3i, 1 \pm 3i, 3 \pm i\}$, for which $X \in \mathbb{Q}$ and $Y \in \mathbb{Q}(i)$. Note that if (X, Y) is a point on C_δ then (X, iY) is a point on $C_{-\delta}$. We will use this isomorphism later on to reduce the number of curves to be examined. Hence we need to consider the curve C_δ for $\delta \in \{1 - 3i, 1 + 3i, 3 - i, 3 + i\}$.

I. $\delta = 1 - 3i$. In this case C_{1-3i} is isomorphic to the elliptic curve

$$E_{1-3i} : \quad y^2 = x^3 + ix^2 + (-17i - 23)x + (2291i + 1597).$$

Using MAGMA we get that the rank of E_{1-3i} is 0 and there is no point on C_{1-3i} for which $X \in \mathbb{Q}$.

II. $\delta = 1 + 3i$. Here we obtain that $E_{1+3i} : y^2 = x^3 - ix^2 + (17i - 23)x + (-2291i + 1597)$. The rank of this curve is 0 and there is no point on C_{1+3i} for which $X \in \mathbb{Q}$.

III. $\delta = 3 - i$. The elliptic curve in this case is $E_{3-i} : y^2 = x^3 + x^2 + (-17i + 23)x + (-1597i - 2291)$. We have $E_{3-i}(\mathbb{Q}(i)) \simeq \mathbb{Z}_2 \oplus \mathbb{Z}$ as an Abelian group. Applying elliptic Chabauty with $p = 13$, we get that $x_5/z = -3$. Thus $n = 2$ and $d = 1$.

IV. $\delta = 3 + i$. The curve C_{3+i} is isomorphic to $E_{3+i} : y^2 = x^3 + x^2 + (17i + 23)x + (1597i - 2291)$. The rank of this curve is 1 and applying elliptic Chabauty again with $p = 13$ we obtain that $x_5/z = 3$. This implies that $n = 2$ and $d = 1$. □

Lemma 4.2.2. *Equation* (7.1) *with* $k = 7$ *and* $(a_0, a_1, \ldots, a_6) = (2, 3, 1, 5, 6, 7, 2)$ *implies that* $n = 2, d = 1$.

Proof. In this case we have the following system of equations

$$\begin{aligned} x_4^2 + x_0^2 &= 2x_1^2, \\ 9x_4^2 + x_0^2 &= 10x_3^2, \\ 9x_4^2 - x_0^2 &= 2x_6^2. \end{aligned}$$

Using the same argument as in the proof of Theorem 1 it follows that it is sufficient to find all points (X, Y) on the curves

$$C_\delta : \quad 2\delta(X + i)(3X + i)(9X^2 - 1) = Y^2, \tag{4.4}$$

where $\delta \in \{-4 \pm 2i, -2 \pm 4i, 2 \pm 4i, 4 \pm 2i\}$, for which $X \in \mathbb{Q}$ and $Y \in \mathbb{Q}(i)$. We summarize the results obtained by elliptic Chabauty in the following table. In each case we used $p = 29$.

δ	curve	x_4/x_0
$2 - 4i$	$y^2 = x^3 + (-12i - 9)x + (-572i - 104)$	$\{-1, \pm 1/3\}$
$2 + 4i$	$y^2 = x^3 + (12i - 9)x + (-572i + 104)$	$\{1, \pm 1/3\}$
$4 - 2i$	$y^2 = x^3 + (-12i + 9)x + (-104i - 572)$	$\{\pm 1/3\}$
$4 + 2i$	$y^2 = x^3 + (12i + 9)x + (-104i + 572)$	$\{\pm 1/3\}$

Thus $x_4/x_0 \in \{\pm 1, \pm 1/3\}$. From $x_4/x_0 = \pm 1$ it follows that $n = 2, d = 1$, while $x_4/x_0 = \pm 1/3$ does not yield any solutions. □

Lemma 4.2.3. *Equation* (7.1) *with* $k = 7$ *and* $(a_0, a_1, \ldots, a_6) = (3, 1, 5, 6, 7, 2, 1)$ *implies that* $n = 3, d = 1$.

Proof. Here we get the following system of equations

$$\begin{aligned} 2x_3^2 + 2x_0^2 &= x_1^2, \\ 4x_3^2 + x_0^2 &= 5x_2^2, \\ 12x_3^2 - 3x_0^2 &= x_6^2. \end{aligned}$$

Using the same argument as in the proof of Theorem 1 it follows that it is sufficient to find all points (X, Y) on the curves

$$C_\delta : \quad \delta(X+i)(2X+i)(12X^2-3) = Y^2, \tag{4.5}$$

where $\delta \in \{-3 \pm i, -1 \pm 3i, 1 \pm 3i, 3 \pm i\}$ for which $X \in \mathbb{Q}$ and $Y \in \mathbb{Q}(i)$. We summarize the results obtained by elliptic Chabauty in the following table. In each case we used $p = 13$.

δ	curve	x_3/x_0
$1-3i$	$y^2 = x^3 + (27i+36)x + (243i-351)$	$\{-1, \pm 1/2\}$
$1+3i$	$y^2 = x^3 + (-27i+36)x + (243i+351)$	$\{1, \pm 1/2\}$
$3-i$	$y^2 = x^3 + (27i-36)x + (-351i+243)$	$\{\pm 1/2\}$
$3+i$	$y^2 = x^3 + (-27i-36)x + (-351i-243)$	$\{\pm 1/2\}$

Thus $x_3/x_0 \in \{\pm 1, \pm 1/2\}$. From $x_4/x_0 = \pm 1$ it follows that $n = 3, d = 1$, while $x_3/x_0 = \pm 1/2$ does not yield any solutions. □

Lemma 4.2.4. *Equation* (7.1) *with* $(a_0, a_1, \ldots, a_4) = (-3, -5, 2, 1, 1)$ *and* $k = 5, d > 1$ *implies that* $n = -12, d = 7$.

Proof. From the system of equations (2) we have

$$\begin{aligned}
\frac{1}{4}x_4^2 - \frac{9}{4}x_0^2 &= -5x_1^2, \\
\frac{1}{2}x_4^2 - \frac{3}{2}x_0^2 &= 2x_2^2, \\
\frac{3}{4}x_4^2 - \frac{3}{4}x_0^2 &= x_3^2.
\end{aligned}$$

Clearly, $\gcd(x_4, x_0) = 1$ or 2. In both cases we get the following system of equations

$$\begin{aligned}
X_4^2 - 9X_0^2 &= -5\square, \\
X_4^2 - 3X_0^2 &= \square, \\
X_4^2 - X_0^2 &= 3\square,
\end{aligned}$$

where $X_4 = x_4/\gcd(x_4, x_0)$ and $X_0 = x_0/\gcd(x_4, x_0)$. The curve in this case is

$$C_\delta : \quad \delta(X+\sqrt{3})(X+3)(X^2-1) = Y^2,$$

where δ is from a finite set. Elliptic Chabauty's method applied with $p = 11, 37$ and 59 provides all points for which the first coordinate is rational. These coordinates are $\{-3, -2, -1, 1, 2\}$. We obtain the arithmetic progression with $(n, d) = (-12, 7)$. □

Lemma 4.2.5. *Equation* (7.1) *with* $(a_0, a_1, \dots, a_4) = (2, 5, 2, -1, -1)$ *and* $k = 5, d > 1$ *implies that* $n = -4, d = 3$.

Proof. We use x_3 and x_2 to get a system of equations as in the previous lemmas. Elliptic Chabauty's method applied with $p = 13$ yields that $x_3/x_2 = \pm 1$, hence $(n, d) = (-4, 3)$. □

Lemma 4.2.6. *Equation* (7.1) *with* $(a_0, a_1, \dots, a_4) = (6, 5, 1, 3, 2)$ *and* $k = 5, d > 1$ *has no solutions.*

Proof. In this case we have

$$\delta(x_3 + \sqrt{-1}x_0)(x_3 + 2\sqrt{-1}x_0)(2x_3^2 - x_0^2) = \square,$$

where $\delta \in \{1 \pm 3\sqrt{-1}, 3 \pm \sqrt{-1}\}$. Chabauty's argument gives $x_3/x_0 = \pm 1$, which corresponds to arithmetic progressions with $d = \pm 1$. □

4.3 Remaining cases of Theorem A

In this section we prove Theorem 4.1.1.

Proof. First note that Lemmas 4.2.1, 4.2.2 and 4.2.3 imply the statement of the theorem in cases of $k = 7, 13$ and 19. The two remaining possibilities can be eliminated in a similar way, we present the argument working for the tuple

$$(5, 6, 7, 2, 1, 10, 11, 3, 13, 14, 15, 1, 17, 2, 19, 5, 21, 22, 23, 6, 1, 26, 3).$$

We have the system of equations

$$\begin{aligned}
n + d &= 6x_1^2, \\
n + 3d &= 2x_3^2, \\
n + 5d &= 10x_5^2, \\
n + 7d &= 3x_7^2, \\
n + 9d &= 14x_9^2, \\
n + 11d &= x_{11}^2, \\
n + 13d &= 2x_{13}^2.
\end{aligned}$$

We find that x_7, x_{11} and $(n + d)$ are even integers. Dividing all equations by 2 we obtain an arithmetic progression of length 7 and $(a_0, a_1, \dots, a_6) = (3, 1, 5, 6, 7, 2, 1)$. This is not possible by Lemma 4.2.3 and the theorem is proved. □

4.4 the case $k = 5$

In this section we prove Theorem 4.1.2.

Proof. Five divides one of the terms and by symmetry we may assume that $5 \mid n+d$ or $5 \mid n+2d$. First we compute the set of possible tuples $(a_0, a_1, a_2, a_3, a_4)$ for which appropriate congruence conditions hold ($\gcd(a_i, a_j) \in \{1, P(j-i)\}$ for $0 \le i < j \le 4$) and the number of sign changes are at most 1 and the product $a_0a_1a_2a_3a_4$ is positive. After that we eliminate tuples by using elliptic curves of rank 0. We consider elliptic curves $(n+\alpha_1 d)(n+\alpha_2 d)(n+\alpha_3 d)(n+\alpha_4 d) = \prod_i a_{\alpha_i}\square$, where $\alpha_i, i \in \{1,2,3,4\}$ are distinct integers belonging to the set $\{0,1,2,3,4\}$. If the rank is 0, then we obtain all possible values of n/d. Since $\gcd(n,d) = 1$ we get all possible values of n and d. It turns out that it remains to deal with the following tuples

$$(-3,-5,2,1,1),$$
$$(-2,-5,3,1,1),$$
$$(-1,-15,-1,-2,3),$$
$$(2,5,2,-1,-1),$$
$$(6,5,1,3,2).$$

In case of $(-3,-5,2,1,1)$ Lemma 4.2.4 implies that $(n,d) = (-12,7)$.

If $(a_0, a_1, \ldots, a_4) = (-2,-5,3,1,1)$, then by $\gcd(n,d) = 1$ we have that $\gcd(n,3) = 1$. Since $n = -2x_0^2$ we obtain that $n \equiv 1 \pmod 3$. From the equation $n + 2d = 3x_2^2$ we get that $d \equiv 1 \pmod 3$. Finally, the equation $n + 4d = x_4^2$ leads to a contradiction.

If $(a_0, a_1, \ldots, a_4) = (-1,-15,-1,-2,3)$, then we obtain that $\gcd(n,3) = 1$. From the equations $n = -x_0^2$ and $n+d = -15x_1^2$ we get that $n \equiv 2 \pmod 3$ and $d \equiv 1 \pmod 3$. Now the contradiction follows from the equation $n + 2d = -x_2^2$.

In case of the tuple $(2,5,2,-1,-1)$ Lemma 4.2.5 implies that $(n,d) = (-4,3)$. The last tuple is eliminated by Lemma 4.2.6. □

Bibliography

[1] M. A. Bennett, N. Bruin, K. Győry, and L. Hajdu. Powers from products of consecutive terms in arithmetic progression. *Proc. London Math. Soc. (3)*, 92(2):273–306, 2006.

[2] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[3] N. Bruin. Some ternary diophantine equations of signature $(n, n, 2)$. In Wieb Bosma and John Cannon, editors, *Discovering Mathematics with Magma — Reducing the Abstract to the Concrete*, volume 19 of *Algorithms and Computation in Mathematics*, pages 63–91. Springer, Heidelberg, 2006.

[4] N. R. Bruin. *Chabauty methods and covering techniques applied to generalized Fermat equations*, volume 133 of *CWI Tract*. Stichting Mathematisch Centrum Centrum voor Wiskunde en Informatica, Amsterdam, 2002. Dissertation, University of Leiden, Leiden, 1999.

[5] Nils Bruin. Chabauty methods using elliptic curves. *J. Reine Angew. Math.*, 562:27–49, 2003.

[6] L.E. Dickson. *History of the theory of numbers. Vol II: Diophantine analysis*. Chelsea Publishing Co., New York, 1966.

[7] P. Erdős and J. L. Selfridge. The product of consecutive integers is never a power. *Illinois J. Math.*, 19:292–301, 1975.

[8] N. Hirata-Kohno, S. Laishram, T. N. Shorey, and R. Tijdeman. An extension of a theorem of Euler. *Acta Arith.*, 129(1):71–102, 2007.

[9] Anirban Mukhopadhyay and T. N. Shorey. Almost squares in arithmetic progression. II. *Acta Arith.*, 110(1):1–14, 2003.

[10] Richard Obláth. Über das Produkt fünf aufeinander folgender Zahlen in einer arithmetischen Reihe. *Publ. Math. Debrecen*, 1:222–226, 1950.

5

Squares in products in arithmetic progression with at most one term omitted and common difference a prime power

*L*aishram, S., Shorey, T. N. and Tengely, Sz.,
Acta Arithmetica **135** (2008), 143–158.

Abstract

It is shown that a product of $k-1$ terms out of $k \geq 7$ terms in arithmetic progression with common difference a prime power > 1 is not a square. In fact it is not of the form by^2 where the greatest prime factor of b is less than or equal to k. Also, we show that product of 11 or more terms in an arithmetic progression with common difference a prime power > 1 is not of the form by^2 where the greatest prime factor of b is less than or equal to $p_{\pi(k)+2}$.

5.1 Introduction

For an integer $x > 1$, we denote by $P(x)$ and $\omega(x)$ the greatest prime factor of x and the number of distinct prime divisors of x, respectively. Further we put $P(1) = 1$ and $\omega(1) = 0$. Let p_i be the $i-$th prime number. Let $k \geq 4, t \geq k-2$ and $\gamma_1 < \gamma_2 < \cdots < \gamma_t$ be integers with $0 \leq \gamma_i < k$ for $1 \leq i \leq t$. Thus $t \in \{k, k-1, k-2\}$, $\gamma_t \geq k-3$ and $\gamma_i = i-1$ for $1 \leq i \leq t$ if $t = k$. We put $\psi = k - t$. Let b be a positive squarefree integer and we shall always assume, unless otherwise specified, that $P(b) \leq k$. We consider the equation

$$\Delta = \Delta(n, d, k) = (n + \gamma_1 d) \cdots (n + \gamma_t d) = by^2 \tag{5.1}$$

in positive integers n, d, k, b, y, t. It has been proved (see [9] and [8]) that (5.1) with $\psi = 1, k \geq 9$, $d \nmid n$, $P(b) < k$ and $\omega(d) = 1$ does not hold. Further it

has been shown in [10] that the assertion continues to be valid for $6 \leq k \leq 8$ provided $b = 1$. We show

Theorem 5.1.1. *Let $\psi = 1, k \geq 7$ and $d \nmid n$. Then* (5.1) *with $\omega(d) = 1$ does not hold.*

Thus the assumption $P(b) < k$ and $k \geq 9$ (in [9] and [8]) has been relaxed to $P(b) \leq k$ and $k \geq 7$, respectively, in Theorem 5.1.1. As an immediate consequence of Theorem 5.1.1, we see that (5.1) with $\psi = 0, k \geq 7$, $d \nmid n$, $P(b) \leq p_{\pi(k)+1}$ and $\omega(d) = 1$ is not possible. If $k \geq 11$, we relax the assumption $P(b) \leq p_{\pi(k)+1}$ to $P(b) \leq p_{\pi(k)+2}$ in the next result.

Theorem 5.1.2. *Let $\psi = 0, k \geq 11$ and $d \nmid n$. Assume that $P(b) \leq p_{\pi(k)+2}$ Then* (5.1) *with $\omega(d) = 1$ does not hold.*

For related results on (5.1), we refer to [6].

5.2 Notations and Preliminaries

We assume (5.1) with $\gcd(n, d) = 1$ in this section. Then we have

$$n + \gamma_i d = a_{\gamma_i} x_{\gamma_i}^2 \quad \text{for } 1 \leq i \leq t \tag{5.2}$$

with a_{γ_i} squarefree such that $P(a_{\gamma_i}) \leq \max(k-1, P(b))$. Thus (5.1) with b as the squarefree part of $a_{\gamma_1} \cdots a_{\gamma_t}$ is determined by the $t-$tuple $(a_{\gamma_1}, \cdots, a_{\gamma_t})$. Further we write

$$b_i = a_{\gamma_i}, \ y_i = x_{\gamma_i}.$$

Since $\gcd(n, d) = 1$, we see from (5.2) that

$$(b_i, d) = (y_i, d) = 1 \quad \text{for } 1 \leq i \leq t. \tag{5.3}$$

Let

$$R = \{b_i : 1 \leq i \leq t\}.$$

Lemma 5.2.1. (*[6]*)

Equation (5.1) *with $\omega(d) = 1$ and $k \geq 9$ implies that $t - |R| \leq 1$.*

Lemma 5.2.2. *Let $\psi = 0, k \geq 4$ and $d \nmid n$. Then* (5.1) *with $\omega(d) = 1$ implies $(n, d, k, b) = (75, 23, 4, 6)$.*

This is proved in [9] and [7] unless $k = 5, P(b) = 5$ and then it is a particular case of a result of Tengely [12].

Lemma 5.2.3. *([9, Theorem 4] and [8])*

Let $\psi = 1, k \geq 9$ and $d \nmid n$. Assume that $P(b) < k$. Then (5.1) *with $\omega(d) = 1$ does not hold.*

Lemma 5.2.4. *([6])*

Let $\psi = 2, k \geq 15$ and $d \nmid n$. Then (5.1) *with $\omega(d) = 1$ does not hold.*

Lemma 5.2.5. *Let $\psi = 1, k = 7$ and $d \nmid n$. Then $(a_0, a_1, \cdots, a_6)$ is different from the ones given by the following tuples or their mirror images.*

$$\begin{aligned} k = 7 : &(1,2,3,-,5,6,7),(2,1,6,-,10,3,14),(2,1,14,3,10,-,6),\\ &(-,3,1,5,6,7,2),(3,1,5,6,7,2,-),(3,-,5,6,7,2,1),\\ &(1,5,6,7,2,-,10),(-,5,6,7,2,1,10),(5,6,7,2,1,10,-),\\ &(6,7,2,1,10,-,3),(10,3,14,1,2,5,-),\\ &(-,10,3,14,1,2,5),(5,2,1,14,3,10,-),(-,5,2,1,14,3,10). \end{aligned} \tag{5.4}$$

Further $(a_1, \cdots, a_6)$ is different from $(1,2,3,-,5,6),(2,1,6,-,10,3)$ and their mirror images.

The proof of Lemma 5.2.5 is given in Section 3.

The following result is contained in [1, Lemma 4.1].

Lemma 5.2.6. *There are no coprime positive integers n', d' satisfying the diophantine equations*

$$\prod(0,1,2,3) = by^2,\ b \in \{1,2,3,5,15\}$$
$$\prod(0,1,3,4) = by^2,\ b \in \{1,2,3,6,30\}$$

where $\prod(0,i,j,l) = n'(n'+id')(n'+jd')(n'+ld')$.

Lemma 5.2.7. *Equation* (5.1) *with $\psi = 1, k = 7$ is not possible if*

(i) $a_1 = a_4 = 1, a_6 = 6$ *and either* $a_3 = 3$ *or* $a_2 = 2$

(ii) $a_1 = a_6 = 1$ *and at least two of* $a_2 = 2, a_4 = 6, a_5 = 5$ *holds.*

(iii) $a_0 = a_6 = 2$, $a_5 = 3$ *and either* $a_2 = 6$ *or* $a_4 = 1$

(iv) $a_0 = a_5 = 1$ *and at least two of* $a_1 = 5, a_2 = 6$, $a_4 = 2$ *holds.*

(v) $a_3 = a_6 = 1$, $a_1 = 6$ *and* $a_2 = 5$

(vi) $a_0 = a_4 = 1$, $a_3 = 3$ *and* $a_6 = 2$

(vii) $a_0 = a_5 = 1$ *and at least two of* $a_1 = 2, a_3 = 6, a_6 = 3$ *holds.*

Proof. The proof of Lemma 5.2.7 uses MAGMA to compute integral points on Quartic curves. For this we first make a Quartic curve and find a integral point on it. Then we compute all integral points on the curve by using MAGMA command *IntegralQuarticPoints* and we exclude them.

We illustrate this with one example and others are similar. Consider (*ii*). Then from $x_6^2 - x_1^2 = n + 6d - (n + d) = 5d$ and $\gcd(x_6 - x_1, x_6 + x_1) = 1$, we get either

$$x_6 - x_1 = 5, x_6 + x_1 = d \tag{5.5}$$

or

$$x_6 - x_1 = 1, x_6 + x_1 = 5d. \tag{5.6}$$

Assume (5.5). Then $d = 2x_1 + 5$. This with $n + d = x_1^2$, we get

$$\begin{aligned} 2x_2^2 &= n + 2d = n + d + d = x_1^2 + 2x_1 + 5 = (x_1 + 1)^2 + 4 \text{ if } a_2 = 2 \\ 6x_4^2 &= n + 4d = n + d + 3d = x_1^2 + 6x_1 + 15 = (x_1 + 3)^2 + 6 \text{ if } a_4 = 6 \\ 5x_5^2 &= n + 5d = n + d + 4d = x_1^2 + 8x_1 + 20 = (x_1 + 4)^2 + 4 \text{ if } a_5 = 5. \end{aligned}$$

When $a_2 = 2, a_4 = 6$, by putting $X = x_1 + 1$, $Y = 3(2x_2)(6x_4)$, we get the Quartic curve $Y^2 = 3(X^2+4)((X+2)^2+6) = 3X^4+12X^3+42X^2+48X+120$ in positive integers X and Y with $X = x_1 + 1 \geq 2$. Observing that $(X, Y) = (1, 15)$ is an integral point on this curve, we obtain by MAGMA command

$$IntegralQuarticPoints([3, 12, 42, 48, 120], [1, 15]);$$

that all integral points on the curve are given by

$$(X, Y) \in \{(1, \pm 15), (-2, \pm 12), (-14, \pm 300), (-29, \pm 1365).$$

Since none of the points (X, Y) satisfy $X \geq 2$, we exclude the case $a_2 = 2, a_4 = 6$. Further when $a_2 = 2, a_5 = 5$, by putting $X = x_1 + 1$ and $Y = 10(2x_2)(5x_5)$, we get the curve $Y^2 = 10(X^2+4)((X+3)^2+4) = 10X^4+60X^3+170X^2+240X+520$ for which an integral point is $(X, Y) = (-1, 20)$ and all the integral points have $X \leq 1$ and it is excluded. When $a_4 = 6, a_5 = 5$, by puting $X = x_1 + 3$ and $Y = 30(6x_4)(5x_5)$, we get the curve $Y^2 = 30(X^2 + 6)((X + 1)^2 + 4) =$

$30X^4 + 60X^3 + 330X^2 + 360X + 900$ for which $(X, Y) = (0, 30)$ is an integral point and all the integral points other than $(X, Y) = (11, 500)$ satisfy $X \leq 1$. Since $30|Y$ and $30 \nmid 500$, this case is also excluded. When (5.6) holds, we get $5d = 2x_1 + 1$ and this with $n + d = x_1^2$ implies

$$2(5x_2)^2 = 25(n + d) + 25d = 25x_1^2 + 10x_1 + 5 = (5x_1 + 1)^2 + 4 \text{ if } a_2 = 2$$
$$6(5x_4)^2 = 25(n + d) + 75d = 25x_1^2 + 30x_1 + 15 = (5x_1 + 3)^2 + 6 \text{ if } a_4 = 6$$
$$5(5x_5)^2 = 25(n + d) + 100d = 25x_1^2 + 40x_1 + 20 = (5x_1 + 4)^2 + 4 \text{ if } a_5 = 5.$$

As in the case (5.5), these gives rise to the same Quartic curves $Y^2 = 3X^4 + 12X^3 + 42X^2 + 48X + 120$; $Y^2 = 10X^4 + 60X^3 + 170X^2 + 240X + 520$ and $Y^2 = 30X^4 + 60X^3 + 330X^2 + 360X + 900$ when $a_2 = 2, a_3 = 6$; $a_2 = 2, a_5 = 5$ and $a_4 = 6, a_5 = 5$, respectively. This is not possible.

Similarly all the other cases are excluded. In the case (iii), we have $n = 2x_0^2$ and obtain either $d = 2x_0 + 3$ or $3d = 2x_0 + 1$. Then we use $2a_i x_i^2 = 2(n + id) = (2x_0)^2 + 2i(2x_0 + 3) = (2x_0 + i)^2 + 6i - i^2$ if $d = 2x_0 + 3$ and $2a_i(3x_i)^2 = 18(n + id) = (6x_0)^2 + 6i(2x_0 + 1) = (6x_0 + i)^2 + 6i - i^2$ if $3d = 2x_0 + 1$ to get Quartic equations. In the case (vi), we obtain the Quartic equation $Y^2 = 6X^4 + 36X^3 + 108X - 54 = 6(X^4 + 6X^3 + 18X - 9)$. For any integral point (X, Y) on this curve, we obtain $3|(X^4 + 6X^3 + 18X - 9)$ giving $3|X$. Then $\mathrm{ord}_3(X^4 + 6X^3 + 18X - 9) = 2$ giving $\mathrm{ord}_3(Y^2) = \mathrm{ord}_3(6) + 2 = 3$, a contradiction. □

5.3 Proof of Lemma 5.2.5

For the proof of Lemma 5.2.5, we use the so-called elliptic Chabauty's method (see [3],[4]). Bruin's routines related to elliptic Chabauty's method are contained in MAGMA [2], so here we indicate the main steps only and a MAGMA routine which can be used to verify the computations. Note that in case of rank 0 elliptic curves one can compute the finitely many torsion points and check each of them if they correspond to any solutions. Therefore this case is not included in the routine. The input C is a hyperelliptic curve defined over a number field and p is a prime.

```
APsol:=function(C,p)
P1:=ProjectiveSpace(Rationals(),1);
E,toE:=EllipticCurve(C);
Em,EtoEm:=MinimalModel(E);
two:= MultiplicationByMMap(Em,2);
mu,tor:= DescentMaps(two);
S,AtoS:= SelmerGroup(two);
```

```
RB:=RankBound(Em: Isogeny:=two);
umap:=map<C->P1|[C.1,C.3]>;
U:=Expand(Inverse(toE*EtoEm)*umap);
if RB eq 0 then
    print "Rank 0 case";
    return true;
else
    success,G,mwmap:=PseudoMordellWeilGroup(Em: Isogeny:=two);
    if success then
        NC,VC,RC,CC:=Chabauty(mwmap,U,p);
        print "NC,#VC,RC:",NC,#VC,RC;
        PONTOK:={EvaluateByPowerSeries(U,mwmap(gp)): gp in VC};
        print "Saturated:",
            forall{pr: pr in PrimeDivisors(RC)|IsPSaturated(mwmap,pr)};
        return PONTOK;
    else return false;
    end if;
end if;
end function;
```

First consider the tuple $(6, 7, 2, 1, 10, -, 3)$. Using that $n = 6x_3^2 - 2x_2^2$ and $d = -2x_3^2 + x_2^2$ we obtain the following system of equations

$$\begin{aligned} -x_3^2 + 3x_2^2 &= 3x_0^2, \\ -x_3^2 + 4x_2^2 &= 7x_1^2, \\ x_3^2 - x_2^2 &= 5x_4^2, \\ 4x_3^2 - 6x_2^2 &= 3x_6^2. \end{aligned}$$

The first equation implies that x_3 is divisible by 3, that is there exists a $z \in \mathbb{Z}$ such that $x_3 = 3z$. By standard factorization argument we get that

$$(\sqrt{3}z + x_2)(3z + x_2)(12z^2 - 2x_2^2) = \delta\square,$$

where $\delta \in \{\pm 2 + \sqrt{3}, \pm 10 + 5\sqrt{3}\}$. Thus putting $X = z/x_2$ it is sufficient to find all points (X, Y) on the curves

$$C_\delta : \quad \delta(\sqrt{3}X + 1)(3X + 1)(12X^2 - 2) = Y^2, \tag{5.7}$$

for which $X \in \mathbb{Q}$ and $Y \in \mathbb{Q}(\sqrt{3})$. For all possible values of δ the point $(X, Y) = (-1/3, 0)$ is on the curves, therefore we can transform them to elliptic curves. We note that $X = z/x_2 = -1/3$ does not yield appropriate arithmetic progressions.

I. $\delta = 2+\sqrt{3}$. In this case $C_{2+\sqrt{3}}$ is isomorphic to the elliptic curve

$$E_{2+\sqrt{3}}: \quad y^2 = x^3 + (-\sqrt{3}-1)x^2 + (6\sqrt{3}-9)x + (11\sqrt{3}-19).$$

Using MAGMA we get that the rank of $E_{2+\sqrt{3}}$ is 0 and the only point on $C_{2+\sqrt{3}}$ for which $X \in \mathbb{Q}$ is $(X, Y) = (-1/3, 0)$.

II. $\delta = -2+\sqrt{3}$. Applying elliptic Chabauty with $p = 7$, we get that $z/x_2 \in \{-1/2, -1/3, -33/74, 0\}$. Among these values $z/x_2 = -1/2$ gives $n = 6, d = 1$.

III. $\delta = 10+5\sqrt{3}$. Applying again elliptic Chabauty with $p = 23$, we get that $z/x_2 \in \{1/2, -1/3\}$. Here $z/x_2 = 1/2$ corresponds to $n = 6, d = 1$.

IV. $\delta = -10+5\sqrt{3}$. The elliptic curve $E_{-10+5\sqrt{3}}$ is of rank 0 and the the only point on $C_{-10+5\sqrt{3}}$ for which $X \in \mathbb{Q}$ is $(X, Y) = (-1/3, 0)$.

We proved that there is no arithmetic progression for which $(a_0, a_1, \ldots, a_6) = (6, 7, 2, 1, 10, -, 3)$ and $d \nmid n$.

Now consider the tuple $(1, 5, 6, 7, 2, -, 10)$. The system of equation we use is

$$\begin{aligned} x_6^2 - 3x_1^2 &= -2x_0^2, \\ x_6^2 + 2x_1^2 &= 3x_2^2, \\ 4x_6^2 + 3x_1^2 &= 7x_3^2, \\ 3x_6^2 + x_1^2 &= x_4^2. \end{aligned}$$

We factor the first equation over $\mathbb{Q}(\sqrt{3})$ and the fourth over $\mathbb{Q}(\sqrt{-3})$. We obtain

$$\begin{aligned} x_6 + \sqrt{3}x_1 &= \delta_1\square, \\ \sqrt{-3}x_6 + x_1 &= \delta_2\square, \end{aligned}$$

where δ_1, δ_2 are from some finite sets (see e.g. [11], pp. 50-51). The curves for which we apply elliptic Chabaty's method are

$$C_\delta: \quad 3\delta(X+\sqrt{3})(\sqrt{-3}X+1)(X^2+2) = Y^2,$$

defined over $Q(\alpha)$, where $\alpha^4 + 36 = 0$. It turnes out that there is no arithmetic progression with $(a_0, a_1, \ldots, a_6) = (1, 5, 6, 7, 2, -, 10)$ and $d \nmid n$.

Note that in the remaining cases one can obtain the same system of equations for several tuples, these are

$(-, 3, 1, 5, 6, 7, 2)$ and $(3, 1, 5, 6, 7, 2, -)$,

$(1, 2, 3, -, 5, 6)$ and $(2, 1, 6, -, 10, 3)$,

$(-, 5, 6, 7, 2, 1, 10)$ and $(5, 6, 7, 2, 1, 10, -)$,

$(-, 5, 2, 1, 14, 3, 10)$ and $(-, 10, 3, 14, 1, 2, 5)$ and

$(5, 2, 1, 14, 3, 10, -)$ and $(10, 3, 14, 1, 2, 5, -)$.

In the table below we indicate the relevant quartic polynomials. These are as follows.

tuple	polynomial
$(-,3,1,5,6,7,2)$	$\delta_{A1}(X+\sqrt{-1})(2X+\sqrt{-1})(5X^2-1)$
$(-,5,2,1,14,3,10)$	$\delta_{A2}(X+\sqrt{-2})(2\sqrt{-2}X+1)(4X^2+3)$
$(-,5,6,7,2,1,10)$	$\delta_{A3}(X+\sqrt{-2})(2\sqrt{-2}X+1)(3X^2+1)$
$(1,2,3,-,5,6)$	$2\delta_{A4}(X+\sqrt{-1})(X+3\sqrt{-1})(5X^2-3)$
$(2,1,14,3,10,-,6)$	$\delta_{A5}(2X+\sqrt{-1})(3X+\sqrt{-1})(-3X^2+3)$
$(3,-,5,6,7,2,1)$	$5\delta_{A6}(2X+3\sqrt{-1})(X+\sqrt{-1})(12X^2-3)$

□

5.4 Proof of Theorem 5.1.1

Suppose that the assumptions of Theorem 5.1.1 are satisfied and assume (5.1) with $\omega(d)=1$. Let $k\geq 15$. We may suppose that $P(b)=k$ otherwise it follows from (5.2) and Lemma 5.2.4. Then we delete the term divisible by k on the left hand side of (5.1) and the the assertion follows from Lemma 5.2.4. Thus it suffices to prove the assertion for $k\in\{7,8,11,13\}$ by Lemma 5.2.3. Therefore we always restrict to $k\in\{7,8,11,13\}$. In view of Lemma 5.2.1, we arrive at a contradiction by showing $t-|R|\geq 2$ when $k\in\{11,13\}$. Further Lemma 5.2.1 also implies that $p\nmid d$ for $p\leq k$ whenever $k\in\{11,13\}$.

For a prime $p\leq k$ and $p\nmid d$, let i_p be such that $0\leq i_p<p$ and $p|n+i_pd$. For any subset $\mathcal{I}\subseteq[0,k)\cap\mathbb{Z}$ and primes p_1, p_2 with $p_i\leq k$ and $p_i\nmid d$, $i=1,2$, we define

$$\mathcal{I}_1=\{i\in\mathcal{I}:\left(\tfrac{i-i_{p_1}}{p_1}\right)=\left(\tfrac{i-i_{p_2}}{p_2}\right)\}\ and\ \mathcal{I}_2=\{i\in\mathcal{I}:\left(\tfrac{i-i_{p_1}}{p_1}\right)\neq\left(\tfrac{i-i_{p_2}}{p_2}\right)\}.$$

Then from $\left(\frac{a_i}{p}\right)=\left(\frac{i-i_p}{p}\right)\left(\frac{d}{p}\right)$, we see that either

$$\left(\frac{a_i}{p_1}\right)\neq\left(\frac{a_i}{p_2}\right)\ \text{ for all } i\in\mathcal{I}_1\ \text{ and }\ \left(\frac{a_i}{p_1}\right)=\left(\frac{a_i}{p_2}\right)\ \text{ for all } i\in\mathcal{I}_2 \tag{5.8}$$

or

$$\left(\frac{a_i}{p_1}\right)\neq\left(\frac{a_i}{p_2}\right)\ \text{ for all } i\in\mathcal{I}_2\ \text{ and }\ \left(\frac{a_i}{p_1}\right)=\left(\frac{a_i}{p_2}\right)\ \text{ for all } i\in\mathcal{I}_1. \tag{5.9}$$

We define $(\mathcal{M},\mathcal{B})=(\mathcal{I}_1,\mathcal{I}_2)$ in the case (5.8) and $(\mathcal{M},\mathcal{B})=(\mathcal{I}_2,\mathcal{I}_1)$ in the case (5.9). We call $(\mathcal{I}_1,\mathcal{I}_2,\mathcal{M},\mathcal{B})=(\mathcal{I}_1^k,\mathcal{I}_2^k,\mathcal{M}^k,\mathcal{B}^k)$ when $\mathcal{I}=[0,k)\cap\mathbb{Z}$. Then for any $\mathcal{I}\subseteq[0,k)\cap\mathbb{Z}$, we have

$$\mathcal{I}_1\subseteq\mathcal{I}_1^k,\mathcal{I}_2\subseteq\mathcal{I}_2^k,\mathcal{M}\subseteq\mathcal{M}^k,\mathcal{B}\subseteq\mathcal{B}^k$$

and

$$|\mathcal{M}| \geq |\mathcal{M}^k| - (k - |\mathcal{I}|),\ |\mathcal{B}| \geq |\mathcal{B}^k| - (k - |\mathcal{I}|). \tag{5.10}$$

By taking $m = n + \gamma_t d$ and $\gamma_i' = \gamma_t - \gamma_{t-i+1}$, we re-write (5.1) as

$$(m - \gamma_1' d) \cdots (m - \gamma_t' d) = by^2. \tag{5.11}$$

The equation (5.11) is called the mirror image of (5.1). The corresponding t-tuple $(a_{\gamma_1'}, a_{\gamma_2'}, \cdots, a_{\gamma_t'})$ is called the mirror image of $(a_{\gamma_1}, \cdots, a_{\gamma_t})$.

5.4.1 The case $k = 7, 8$

We may assume that $k = 7$ since the case $k = 8$ follows from that of $k = 7$.

In this subsection, we take $d \in \{2^\alpha, p^\alpha, 2p^\alpha\}$ where p is any odd prime and α is a positive integer. In fact, we prove

Lemma 5.4.1. *Let $\psi = 1, k = 7$ and $d \nmid n$. Then* (5.1) *with $d \in \{2^\alpha, p^\alpha, 2p^\alpha\}$ does not hold.*

First we check that (5.1) does not hold for $d \leq 23$ and $n + 5d \leq 324$. Thus we assume that either $d > 23$ or $n + 5d > 324$. Hence $n + 5d > 5 \cdot 26 = 130$. Then (5.1) with $\psi = 0$, $k \geq 4$ and $\omega(d) = 1$ has no solution by Lemma 5.2.2. Let $d = 2$ or $d = 4$. Suppose $a_i = a_j$ with $i > j$. Then $x_i - x_j = r_1$ and $x_i + x_j = r_2$ with r_1, r_2 even and $\gcd(r_1, r_2) = 2$. Now from $n + id > 26i$, we get

$$i - j \geq \frac{a_i(x_i + x_j)}{2} \geq \frac{(a_i x_i^2)^{\frac{1}{2}} + (a_j a_j^2)^{\frac{1}{2}}}{2} > \frac{\sqrt{26(i+j)}}{2} > j,$$

a contradiction. Therefore $a_i \neq a_j$ whenever $i \neq j$ giving $|R| = k - 1$. But $|\{a_i : P(a_i) \leq 5\}| \leq 4$ implying $|R| \leq 4 + 1 < k - 1$, a contradiction. Let $8|d$. Then $|\{a_i : P(a_i) \leq 5\}| \leq 1$ and $|\{j : a_j = a_i\}| \leq 2$ for each $a_i \in R$ giving $|\{i : P(a_i) \leq 5\}| \leq 2$. This is a contradiction since $|\{i : P(a_i) \leq 5\}| \geq 7 - 2 = 5$. Thus $d \neq 2^\alpha$. Let $t - |R| \geq 2$. Then we observe from [5, Lemma] that $d_2 = d < 24$ and $n + 5d < 324$. This is not possible.

Therefore $t - |R| \leq 1$ implying $|R| \geq k - 2 = 5$. If $7|d$, then we get a contradiction since $7 \nmid a_i$ for any i and $|\{a_i : P(a_i) \leq 5\}| \leq 4$ implying $|R| \leq 4 < k - 2$. If $3|d$ or $5|d$, then also we obtain a contradiction since $|\{a_i : P(a_i) \leq 5\}| \leq 2$ implying $|R| \leq 2 + 1 < k - 2$.

Thus $\gcd(p, d) = 1$ for each prime $p \leq 7$. Therefore $5|n + i_5 d$ and $7|n + i_7 d$ with $0 \leq i_5 < 5$ and $0 \leq i_7 < 7$. By taking the mirror image (5.11) of (5.1), we may suppose that $0 \leq i_7 \leq 3$.

Let $p_1 = 5$, $p_2 = 7$ and $\mathcal{I} = \{\gamma_1, \gamma_2, \cdots, \gamma_6\}$. We observe that $P(a_i) \leq 3$ for $i \in \mathcal{M} \cup \mathcal{B}$. Since $\left(\frac{2}{5}\right) \neq \left(\frac{2}{7}\right)$ but $\left(\frac{3}{5}\right) = \left(\frac{3}{7}\right)$, we observe that $a_i \in \{2, 6\}$ whenever $i \in \mathcal{M}$ and $a_i \in \{1, 3\}$ whenever $i \in \mathcal{B}$.

We now define four sets

$$\mathcal{I}_{++}^k = \{i : 0 \leq i < k, \left(\frac{i - i_{p_1}}{p_1}\right) = \left(\frac{i - i_{p_2}}{p_2}\right) = 1\},$$
$$\mathcal{I}_{--}^k = \{i : 0 \leq i < k, \left(\frac{i - i_{p_1}}{p_1}\right) = \left(\frac{i - i_{p_2}}{p_2}\right) = -1\},$$
$$\mathcal{I}_{+-}^k = \{i : 0 \leq i < k, \left(\frac{i - i_{p_1}}{p_1}\right) = 1, \left(\frac{i - i_{p_2}}{p_2}\right) = -1\},$$
$$\mathcal{I}_{-+}^k = \{i : 0 \leq i < k, \left(\frac{i - i_{p_1}}{p_1}\right) = -1, \left(\frac{i - i_{p_2}}{p_2}\right) = 1\}.$$

and let $\mathcal{I}_{++} = \mathcal{I}_{++}^k \cap \mathcal{I}$, $\mathcal{I}_{--} = \mathcal{I}_{--}^k \cap \mathcal{I}$, $\mathcal{I}_{+-} = \mathcal{I}_{+-}^k \cap \mathcal{I}$, $\mathcal{I}_{-+} = \mathcal{I}_{-+}^k \cap \mathcal{I}$. We observe here that $\mathcal{I}_1 = \mathcal{I}_{++} \cup \mathcal{I}_{--}$ and $\mathcal{I}_2 = \mathcal{I}_{+-} \cup \mathcal{I}_{-+}$. Since $a_i \in \{1, 2, 3, 6\}$ for $i \in \mathcal{I}_1 \cup \mathcal{I}_2$ and $\left(\frac{a_i}{p}\right) = \left(\frac{i - i_p}{p}\right)\left(\frac{d}{p}\right)$, we obtain four possibilities *I*, *II*, *III* and *IV* according as $\left(\frac{d}{5}\right) = \left(\frac{d}{7}\right) = 1$; $\left(\frac{d}{5}\right) = \left(\frac{d}{7}\right) = -1$; $\left(\frac{d}{5}\right) = 1, \left(\frac{d}{7}\right) = -1$; $\left(\frac{d}{5}\right) = -1, \left(\frac{d}{7}\right) = 1$, respectively.

	$\{a_i : i \in \mathcal{I}_{++}\}$	$\{a_i : i \in \mathcal{I}_{--}\}$	$\{a_i : i \in \mathcal{I}_{+-}\}$	$\{a_i : i \in \mathcal{I}_{-+}\}$
I	{1}	{3}	{6}	{2}
II	{3}	{1}	{2}	{6}
III	{2}	{6}	{3}	{1}
IV	{6}	{2}	{1}	{3}

In the case *I*, we have $\left(\frac{a_i}{p}\right) = \left(\frac{i - i_p}{p}\right)$ for $p \in \{5, 7\}$ which together with $\left(\frac{a_i}{5}\right) = 1$ for $a_i \in \{1, 6\}$, $\left(\frac{a_i}{5}\right) = -1$ for $a_i \in \{2, 3\}$, $\left(\frac{a_i}{7}\right) = 1$ for $a_i \in \{1, 2\}$ and $\left(\frac{a_i}{7}\right) = -1$ for $a_i \in \{3, 6\}$ implies the assertion. The assertion for the cases *II*, *III* and *IV* follows similarly. For simplicity, we write $\mathcal{A}_7 = (a_0, a_1, a_2, a_3, a_4, a_5, a_6)$.

For each possibility $0 \leq i_5 < 5$ and $0 \leq i_7 \leq 3$, we compute $\mathcal{I}_{++}^k, \mathcal{I}_{--}^k, \mathcal{I}_{+-}^k, \mathcal{I}_{+-}^k$ and restrict to those pairs (i_5, i_7) for which $\max(|\mathcal{I}_1^k|, |\mathcal{I}_2^k|) \leq 4$. Then we check for the possibilities *I*, *II*, *III* or *IV*.

Suppose $d = 2p^\alpha$. Then $b_i \in \{1, 3\}$ whenever $P(b_i) \leq 3$. If $i_5 \neq 0, 1$, then $|R| \leq 2 + 2 = 4$ giving $t - |R| \geq 7 - 1 - 4 = 2$, a contradiction. Thus $i_5 \in \{0, 1\}$. Further $\mathcal{M} = \emptyset$ and $a_i \in \{1, 3\}$ for $i \in \mathcal{B}$. Therefore either $|\mathcal{I}_1^k| \leq 1$ or $|\mathcal{I}_1^k| \leq 2$. We find that this is the case only when $(i_5, i_7) \in \{(0, 1), (1, 2)$. Let $(i_5, i_7) = (0, 1)$. We get $\mathcal{I}_{++}^k = \mathcal{I}_{--}^k = \emptyset$, $\mathcal{I}_{+-}^k = \{4, 6\}$ and $\mathcal{I}_{-+}^k = \{2, 3\}$. It suffices to consider the cases *III* and *IV* since $b_i \in \{1, 3\}$ whenever $P(b_i) \leq 3$. Suppose *III* holds. Then by modulo 3, we obtain $4 \notin \mathcal{I}$, $a_6 = 3$ and $a_2 = a_3 = 1$. By modulo 3

again, we get $a_1 \notin \{1,7,3\}$ which is not possible since $5 \nmid a_1$. Suppose *IV* holds. Then by modulo 3, we obtain $2 \notin \mathcal{I}$, $a_4 = a_6 = 1$ and $a_3 = 3$. We now get $a_1 \in \{1,7\}$ and by $t - |R| \leq 1$, we get $a_1 = 7$. This is not possible since $-1 = \left(\frac{a_1 a_4}{5}\right) = \left(\frac{(1-0)(4-0)}{5}\right) = 1$. Similarly $(i_5, i_7) = (1,2)$ is excluded. Hence $d = p^\alpha$ from now on.

Let $(i_5, i_7) = (0,0)$. We obtain $\mathcal{I}^k_{++} = \{1,4\}, \mathcal{I}^k_{--} = \{3\}$, $\mathcal{I}^k_{+-} = \{6\}$ and $\mathcal{I}^k_{-+} = \{2\}$. We may assume that $1 \in \mathcal{I}$ otherwise $P(a_2a_3a_4a_5a_6) \leq 5$ and this is excluded by Lemma 5.2.2 with $k = 5$. Further $i \notin \mathcal{I}$ for exactly one of $i \in \{2,3,4\}$ otherwise $P(a_1a_2a_3a_4) \leq 3$ and this is not possible by Lemma 5.2.2 with $k = 4$ since $d > 23$. Consider the possibilities *II* and *IV*. By modulo 3, we obtain $2 \notin \mathcal{I}$, $3 | a_1a_4$ and $a_3a_6 = 2$. This is not possible by modulo 3 since $-1 = \left(\frac{a_3a_6}{3}\right) = \left(\frac{(3-1)(6-1)}{3}\right) = 1$, a contradiction. Suppose *I* holds. Then $a_1 = 1$ and $a_6 = 6$. If $4 \in \mathcal{I}$, then $a_1 = a_4 = 1$ and at least one of $a_3 = 3, a_2 = 2$ holds and this is excluded by Lemma 5.2.7 (i). Assume that $4 \notin \mathcal{I}$. Then $a_1 = 1, a_2 = 2, a_3 = 3, a_6 = 6$ giving $a_5 = 5$ by modulo 2 and 3. Thus we have $(a_1, \cdots, a_5, a_6) = (1,2,3,-,5,6)$. This is not possible by Lemma 5.2.5. Suppose *III* holds. Then $4 \notin \mathcal{I}$, $a_1 = 2, a_2 = 1, a_3 = 6, a_6 = 3$ giving $a_5 = 10$ by modulo 2 and 3. Thus $(a_1, \cdots, a_5, a_6) = (2,1,6,-,10,3)$ which is also excluded by Lemma 5.2.5.

Let $(i_5, i_7) = (0,1)$. We obtain $\mathcal{I}^k_{++} = \mathcal{I}^k_{--} = \emptyset$, $\mathcal{I}^k_{+-} = \{4,6\}$ and $\mathcal{I}^k_{-+} = \{2,3\}$. The possibility *I* is excluded by parity and modulo 3. The possibility *II* implies that $3 \notin \mathcal{I}$, $a_4 = a_6 = 2$ and $a_2 = 3$. This is not possible by modulo 3. Suppose *III* holds. Then $a_2 = a_3 = 1$ and either $4 \notin \mathcal{I}, a_6 = 3$ or $6 \notin \mathcal{I}, a_4 = 3$. By modulo 3, we obtain $4 \notin \mathcal{I}, a_6 = 3$ and $\left(\frac{a_5}{3}\right) = \left(\frac{a_2}{3}\right) = 1$. This gives $a_5 \in \{1,10\}$ which together with $t - |R| \leq 1$ implies $a_5 = 10$. But this is not possible by Lemma 5.2.6 with $n' = n + 2d, d' = d$ and $(i,j,l) = (1,3,4)$. Hence *III* is excluded. Suppose *IV* holds. Then $a_4 = a_6 = 1$ and $2 \notin \mathcal{I}, a_3 = 3$ by modulo 3. By modulo 3, we get $a_5 \in \{2,5\}$ and we may take $a_5 = 5$ otherwise we get a contradiction from $d > 23$ and Lemma 5.2.2 with $k = 4$ applied to $(n+3d)(n+4d)(n+5d)(n+6d)$. This is again not possible by Lemma 5.2.6 with $n' = n + 3d, d' = d$ and $(i,j,l) = (1,2,3)$.

Let $(i_5, i_7) = (0,3)$. We obtain $\mathcal{I}^k_{++} = \{4\}, \mathcal{I}^k_{--} = \{2\}$, $\mathcal{I}^k_{+-} = \{1,6\}$ and $\mathcal{I}^k_{-+} = \emptyset$. By modulo 3, we observe that the possibilities *I* and *III* are excluded. Suppose *II* happens. Then $a_2 = 1, a_4 = 3$ and either $a_6 = 2, 1 \notin \mathcal{I}$ or $a_1 = 2, 6 \notin \mathcal{I}$. If $a_6 = 2, 1 \notin \mathcal{I}$, then $a_5 \in \{1,5\}$ which gives $a_5 = 1$ by modulo 3. This is not possible by modulo 7 since $-1 = \left(\frac{a_4a_5}{7}\right) = \left(\frac{(4-3)(5-3)}{7}\right) = 1$. Thus $a_1 = 2, 6 \notin \mathcal{I}$. Then $a_0 = 5, a_5 = 10, a_3 = 14$ by modulo 3 giving $(a_0, a_1, \cdots, a_5, a_6) = (5,2,1,14,3,10,-)$. Suppose *IV* happens. Let $1, 6 \in \mathcal{I}$. Then $a_1 = a_6 = 1$ and either $a_2 = 2$ or $a_4 = 6$. By Lemma 5.2.7 (ii), we may

assume that either $2 \notin \mathcal{I}$ or $4 \notin \mathcal{I}$. If $2 \notin \mathcal{I}$, then $a_4 = 6$, $a_3 = 7$ and $a_5 = 5$ which is excluded by Lemma 5.2.7 (ii). Thus $4 \notin \mathcal{I}$, $a_2 = 2$ and $a_5 = 5$ since $3 \nmid a_5$. This is also excluded by Lemma 5.2.7 (ii). Therefore $a_2 = 2, a_4 = 6$ and either $6 \notin \mathcal{I}, a_1 = 1$ or $1 \notin \mathcal{I}, a_6 = 1$. Now $7|a_3$ otherwise $P(a_1a_2\cdots a_5) \leq 5$ if $1 \in \mathcal{I}$ or $P(a_2a_3\cdots a_6) \leq 5$ if $6 \in \mathcal{I}$ and this is excluded by Lemma 5.2.2 with $k = 5$. Further by modulo 3, we get $a_3 = 7$, $a_0 = 10$ and $a_5 = 5$. Hence we obtain $\mathcal{A}_7 = (10, -, 2, 7, 6, 5, 1)$ or $\mathcal{A}_7 = (10, 1, 2, 7, 6, 5, -)$.

Let $(i_5, i_7) = (1, 0)$. We obtain $\mathcal{I}^k_{++} = \{2\}, \mathcal{I}^k_{--} = \{3\}$, $\mathcal{I}^k_{+-} = \{5\}$ and $\mathcal{I}^k_{-+} = \{4\}$. We consider the possibility *I*. By parity argument, we have either $5 \notin \mathcal{I}$ or $4 \notin \mathcal{I}$. Again by modulo 3, either $3 \notin \mathcal{I}$ or $5 \notin \mathcal{I}$. Thus $5 \notin \mathcal{I}$ giving $a_2 = 1, a_3 = 3, a_4 = 2$. Now $5|a_1$ otherwise we get a contradiction from $P(a_1a_2a_3a_4) \leq 3$, Lemma 5.2.2 with $k = 4$ and $d > 23$. Hence $a_1 = 5$. This is a again a contradiction since $-1 = \left(\frac{a_1a_2}{7}\right) = \left(\frac{(1-0)(2-0)}{7}\right) = 1$. Thus the possibility *I* is excluded. If the possibility *III* holds, then $3 \notin \mathcal{I}$, $a_2 = 2, a_5 = 3, a_4 = 1$ giving $a_1 \in \{1, 5\}$ and $a_6 = 5$. By modulo 3, we get $a_1 = 1$. But this is not possible by Lemma 5.2.6 with $n' = n + 2d, d' = d$ and $(i, j, l) = (1, 3, 4)$. Similarly, the possibilities *II* and *IV* are also excluded. If *II* holds, then $4 \notin \mathcal{I}, a_2 = 3, a_3 = 1, a_5 = 2$. Now $a_6 \in \{1, 5\}$ and further by modulo 3, we get $a_6 = 1$. This is not possible by Lemma 5.2.6 with $n' = n + 2d, d' = d$ and $(i, j, l) = (1, 3, 4)$. If *IV* holds, then $2 \notin \mathcal{I}$, $a_3 = 2$, $a_5 = 1, a_4 = 3$. Then $a_6 \in \{1, 5\}$ giving $a_6 = 5$ by modulo 3. This is not possible modulo 7.

Let $(i_5, i_7) = (1, 1)$. We obtain $\mathcal{I}^k_{++} = \{2, 5\}, \mathcal{I}^k_{--} = \{4\}$, $\mathcal{I}^k_{+-} = \{0\}$ and $\mathcal{I}^k_{-+} = \{3\}$. We consider the possibilities *III* and *IV*. By parity, we obtain $5 \notin \mathcal{I}$. But then we get a contradiction modulo 3 since $a_4 = 6, a_0 = 3$ if *III* holds and $a_2 = 6, a_3 = 3$ if *IV* holds are not possible. Next we consider the possibility *I*. Then $0 \notin \mathcal{I}$ by modulo 2 and 3 and we get $P(a_2a_3\cdots a_6) \leq 5$ and this is excluded by Lemma 5.2.2 with $k = 5$. Let *II* holds. Then $3 \notin \mathcal{I}$ by modulo 2 and 3 and $a_2 = a_5 = 3, a_4 = 1, a_0 = 2$. Further $a_6 \in \{5, 10\}$ which together with modulo 3 gives $a_6 = 5$. Now we get a contradiction modulo 7 from $a_5 = 3, a_6 = 5$.

Let $(i_5, i_7) = (3, 1)$. We obtain $\mathcal{I}^k_{++} = \{2\}, \mathcal{I}^k_{--} = \{0, 6\}$, $\mathcal{I}^k_{+-} = \{4\}$ and $\mathcal{I}^k_{-+} = \{5\}$. We may assume that $i \notin \mathcal{I}$ for exactly one of $i \in \{0, 2, 4, 6\}$ otherwise n is even, $P(a_0a_2a_4a_6) \leq 3$ and this is excluded by $k = 4$ of Lemma 5.2.2 applied to $\frac{n}{2}(\frac{n}{2} + d)(\frac{n}{2} + 2d)(\frac{n}{2} + 3d)$. We consider the possibilities *I* and *III*. By modulo 3, we get $4 \notin \mathcal{I}$, $a_0 = a_6$, $3|a_0$ and $a_2a_5 = 2$. This is not possible by modulo 3. Next we consider the possibility *II*. Then $4 \notin \mathcal{I}$ by parity argument. Further $a_0 = a_6 = 1$, $a_2 = 3, a_5 = 6$. This is not possible since $8|x_6^2 - x_0^2 = n + 6d - n = 6d$ and d is odd. Finally we consider the possibility *IV*. If $2 \notin \mathcal{I}$ or $4 \notin \mathcal{I}$, then $a_0 = a_6 = 2, a_5 = 3$ and one of $a_2 = 6$ or $a_4 = 1$.

This is excluded by Lemma 5.2.7 (iii). Thus $a_2 = 6, a_4 = 1, a_5 = 3$ and either $a_0 = 2, 6 \notin \mathcal{I}$ or $a_6 = 2, 0 \notin \mathcal{I}$. Then $a_1 = 7, a_3 = 5$ by parity and modulo 3. Hence $\mathcal{A}_7 = (2, 7, 6, 5, 1, 3, -)$ or $\mathcal{A}_7 = (-, 7, 6, 5, 1, 3, 2)$.

All the other pairs are excluded similarly. For $(i_5, i_7) = (0, 2)$, we obtain either $\mathcal{A}_7 = (1, 2, 3, -, 5, 6)$ or $(5, 6, 7, 2, 1, 10, -)$ or $(10, 3, 14, 1, 2, 5, -)$ which are excluded by Lemma 5.2.5. For $(i_5, i_7) = (1, 3)$, we obtain $\mathcal{A}_7 = (1, 5, 6, 7, 2, -, 10)$, $(-, 5, 6, 7, 2, 1, 10)$ or $(-, 10, 3, 14, 1, 2, 5)$ which is not possible by Lemma 5.2.5 or $a_0 = a_5 = 1$ and at least two of $a_1 = 5, a_2 = 6$, $a_4 = 2$ holds which is again excluded by Lemma 5.2.7 (iv). For $(i_5, i_7) = (2, 0)$, we obtain $\mathcal{A}_7 = (14, 3, 10, -, 6, 1, 2), (7, 6, 5, -, 3, 2, 1)$ or $a_3 = a_6 = 1, a_0 = 7, a_1 = 6, a_2 = 5$, $a_4 = 3$ or $a_5 = 2$. These are Lemma 5.2.7 (v). For $(i_5, i_7) = (2, 1)$, we obtain $a_0 = a_4 = 1, a_3 = 3, a_6 = 2$ which is not possible by Lemma 5.2.7 (vi). For $(i_5, i_7) = (4, 1)$, we obtain $\mathcal{A}_7 = (6, 7, 2, 1, 10, -, 3)$ which is also excluded. For $(i_5, i_7) = (4, 2)$, we obtain $\mathcal{A}_7 = (2, 1, 14, 3, 10, -, 6), (1, 2, 7, 6, 5, -, 3), (-, 2, 7, 6, 5, 1, 3)$ or $a_0 = a_5 = 1$ and at least two of $a_1 = 2, a_3 = 6, a_6 = 3$ holds. The previous possibility is excluded by Lemma 5.2.5 and the latter by Lemma 5.2.7 (*vii*).

5.4.2 The case $k = 11$

We may assume that $11 | a_i$ for some i but $11 \nmid a_0a_1a_2a_3a_7a_8a_9a_{10}$ otherwise the assertion follows from Lemma 5.4.1. Further we may also suppose that $i \in \{4, 5, 6\}$ whenever $i \notin \mathcal{I}$ otherwise the assertion follows from Lemma 5.4.1.

Let $p_1 = 5$, $p_2 = 11$ and $\mathcal{I} = \{\gamma_1, \gamma_2, \cdots, \gamma_t\}$. We observe that $P(a_i) \leq 7$ for $i \in \mathcal{M} \cup \mathcal{B}$. Since $\left(\frac{3}{5}\right) \neq \left(\frac{3}{11}\right)$ but $\left(\frac{q}{5}\right) = \left(\frac{q}{11}\right)$ for a prime $q < k$ other than $3, 5, 11$, we observe that $3 | a_i$ whenever $i \in \mathcal{M}$. Since $\sigma_3 \leq 4$ and $|\mathcal{I}| = k-1$, we obtain from (5.10) that $|\mathcal{M}^k| \leq 5$ and $3 | a_i$ for at least $|\mathcal{M}^k| - 1$ i's with $i \in \mathcal{M}^k$. Further $a_i \in \{1, 2, 7, 14\}$ for $i \in \mathcal{B}$ giving $|\mathcal{B}| \leq 5$ otherwise $t - |R| \geq 2$. Hence $|\mathcal{B}^k| \leq 6$ by (5.10).

By taking the mirror image (5.11) of (5.1), we may suppose that $4 \leq i_{11} \leq 5$. For each possibility $0 \leq i_5 < 5$ and $4 \leq i_{11} \leq 5$, we compute $|\mathcal{I}_1^k|, |\mathcal{I}_2^k|$ and restrict to those pairs (i_5, i_{11}) for which $\max(|\mathcal{I}_1^k|, |\mathcal{I}_2^k|) \leq 6$. Further we restrict to those pairs (i_5, i_{11}) for which either

$$3 | a_i \text{ for at least } |\mathcal{I}_1^k| - 1 \text{ elements } i \in \mathcal{I}_1^k \tag{5.12}$$

or

$$3 | a_i \text{ for at least } |\mathcal{I}_2^k| - 1 \text{ elements } i \in \mathcal{I}_2^k. \tag{5.13}$$

We find that exactly one of (5.12) or (5.13) happens. We have $\mathcal{M}^k = \mathcal{I}_1^k, \mathcal{B}^k = \mathcal{I}_2^k$ when (5.12) holds and $\mathcal{M}^k = \mathcal{I}_2^k, \mathcal{B}^k = \mathcal{I}_1^k$ when (5.13) holds. If $3 | a_i$ for exactly

$|\mathcal{M}^k|-1$ elements $i \in \mathcal{M}^k$, then $\mathcal{B} = \mathcal{B}^k$ and we restrict to such pairs (i_5, i_{11}) for which there are at most 3 elements $i \in \mathcal{B}^k$ with $P(a_i) \leq 2$ otherwise $t-|R| \geq 2$. Now all the pairs (i_5, i_{11}) are excluded other than

$$(0,4), (1,5), (4,5). \tag{5.14}$$

For these pairs, we find that $|\mathcal{B}^k| \geq 5$. Hence we may suppose that $7|a_i$ for some $i \in \mathcal{B}$ otherwise $a_i \in \{1,2\}$ for $i \in \mathcal{B}$ which together with $|\mathcal{B}| \geq 4$ gives $t-|R| \geq 2$. Further if $|\mathcal{B}^k| = 6$, then we may assume that $7|a_i, 7|a_{i+7}$ for some $0 \leq i \leq 3$.

Let $(i_5, i_{11}) = (0,4)$. Then $\mathcal{M}^k = \{3,9\}$ and $\mathcal{B}^k = \{1,2,6,7,8\}$ giving $i_3 = 0$. If $7|a_6a_7$, then $|\mathcal{B}| = |\mathcal{B}^k| - 1$ and $a_i \in \{3,6\}$ for $i \in \mathcal{M} = \mathcal{M}^k$ but $\left(\frac{a_3a_9}{7}\right) = \left(\frac{(3-i_7)(9-i_7)}{7}\right) = -1$ for $i_7 = 6,7$, a contradiction. If $7|a_2$, then $a_i \in \{5,10\}$ for $i \in \{5,10\} \subseteq \mathcal{I}$ but $\left(\frac{a_5a_{10}}{7}\right) = \left(\frac{(5-2)(10-2)}{7}\right) = -1$, a contradiction again. Thus $7|a_1a_8$ and $a_i \in \{1,2\}$ for $\{2,6,7\} \cap \mathcal{B}^k$. From $\left(\frac{a_i}{7}\right) = \left(\frac{i-1}{7}\right)\left(\frac{d}{7}\right)$, $\left(\frac{6-1}{7}\right) = \left(\frac{7-1}{7}\right) = -1$ and $\left(\frac{2-1}{7}\right) = 1$, we find that $2 \notin \mathcal{I}$. This is not possible.

Let $(i_5, i_{11}) = (1,5)$. Then $\mathcal{M}^k = \{4,10\}$ and $\mathcal{B}^k = \{0,2,3,7,8,9\}$ giving $i_3 = 1$. Thus $\mathcal{M} = \mathcal{M}^k$, $a_i \in \{3,6\}$ for $i \in \mathcal{M}$ and $|\mathcal{B}| = |\mathcal{B}^k| - 1$, $a_i \in \{1,2,7,14\}$ for $i \in \mathcal{B}$. Further we have either $7|a_0a_7$ or $7|a_2a_9$. Taking modulo $\left(\frac{a_i}{7}\right)$ for $i \in \{4,10,0,2,3,7,8,9\}$, we find that $7|a_2a_9$ and $3 \notin \mathcal{B}$. This is not possible.

Let $(i_5, i_{11}) = (4,5)$. Then $\mathcal{M}^k = \{0,6\}$ and $\mathcal{B}^k = \{1,2,3,7,8,10\}$ giving $\mathcal{M} = \mathcal{M}^k$ and $i_3 = 0$. Further $7|a_1a_8$ or $7|a_3a_{10}$. Taking modulo $\left(\frac{a_i}{7}\right)$ for $i \in \mathcal{M} \cup \mathcal{B}^k$, we find that $7|a_1a_8$ and $\mathcal{B} = \mathcal{B}^k \setminus \{7\}$. This is not possible since $7 \in \mathcal{I}$.

5.4.3 The case $k = 13$

We may assume that $13 \nmid a_0a_1a_2a_{10}a_{11}a_{12}$ otherwise the assertion follows from Theorem 5.1.1 with $k = 11$.

Let $p_1 = 11$, $p_2 = 13$ and $\mathcal{I} = \{\gamma_1, \gamma_2, \cdots, \gamma_t\}$. Since $\left(\frac{5}{11}\right) \neq \left(\frac{5}{13}\right)$ but $\left(\frac{q}{11}\right) = \left(\frac{q}{13}\right)$ for $q = 2,3,7$, we observe that for $5|a_i$ for $i \in \mathcal{M}$ and $P(a_i) \leq 7$, $5 \nmid a_i$ for $i \in \mathcal{B}$. Since $\sigma_5 \leq 3$, we obtain $|\mathcal{M}^k| \leq 4$ and $5|a_i$ for at least $|\mathcal{M}^k|-1$ i's with $i \in \mathcal{M}^k$.

By taking the mirror image (5.11) of (5.1), we may suppose that $3 \leq i_{13} \leq 6$ and $0 \leq i_{11} \leq 10$. We may suppose that $i_{13} \geq 4,5$ if $i_{11} = 0,1$, respectively and $\max(i_{11}, i_{13}) \geq 6$ if $i_{11} \geq 2$ otherwise the assertion follows from Lemma 5.4.1.

Since $\max(|\mathcal{I}_1^k|, |\mathcal{I}_2^k|) \geq 5$ and $|\mathcal{M}^k| \leq 4$, we restrict to those pairs satisfying $\min(|\mathcal{I}_1^k|, |\mathcal{I}_2^k|) \leq 4$ and further $\mathcal{M}^k$ is exactly one of $\mathcal{I}_1^k$ or $\mathcal{I}_2^k$ with minimum

cardinality and hence $\mathcal{B}^k$ is the other one. Now we restrict to those pairs (i_{11}, i_{13}) for which $5|a_i$ for at least $|\mathcal{M}^k| - 1$ elements $i \in \mathcal{M}^k$. If $5|a_i$ for exactly $|\mathcal{M}^k| - 1$ elements $i \in \mathcal{M}^k$, then $\mathcal{B} = \mathcal{B}^k$ and hence we may assume that $|\mathcal{B}| = |\mathcal{B}^k| \leq 7$ otherwise there are at least 6 elements $i \in \mathcal{B}$ for which $a_i \in \{1, 2, 3, 6\}$ giving $t - |R| \geq 2$. Therefore we now exclude those pairs (i_{11}, i_{13}) for which $5|a_i$ for exactly $|\mathcal{M}^k| - 1$ elements $i \in \mathcal{M}^k$ and $|\mathcal{B}^k| > 7$. We find that all the pairs (i_{11}, i_{13}) are excluded other than

$$(1, 3), (2, 4), (3, 5), (4, 2), (5, 3), (6, 4). \tag{5.15}$$

From $i_{13} \geq 5$ if $i_{11} = 1$ and $\max(i_{11}, i_{13}) \geq 6$ if $i_{11} \geq 2$, we find that all these pairs are excluded other than $(6, 4)$.

Let $(i_{11}, i_{13}) = (6, 4)$. Then $\mathcal{M}^k = \{0, 2, 7, 12\}$ and $\mathcal{B}^k = \{1, 3, 5, 8, 9, 10, 11\}$ giving $i_5 = 1$, $\mathcal{M} = \{2, 7, 12\}$ and $0 \notin \mathcal{I}$. This is excluded by applying Lemma 5.4.1 to $\prod_{i=0}^{5}(n + d + 2i)$. □

5.5 Proof of Theorem 5.1.2

By Lemma 5.2.2, we may suppose that $P(b) > k$. If $P(b) = p_{\pi(k)+1}$ or $P(b) = p_{\pi(k)+2}$ with $p_{\pi(k)+1} \nmid b$, then the assertion follows from Theorem 5.1.1. Thus we may suppose that $P(b) = p_{\pi(k)+2}$ and $p_{\pi(k)+1}|b$. Then we delete the terms divisible by $p_{\pi(k)+1}, p_{\pi(k)+2}$ on the left hand side of (5.1) and the assertion for $k \geq 15$ follows from Lemma 5.2.4. Thus $11 \leq k \leq 14$ and it suffices to prove the assertion for $k = 11$ and $k = 13$. After removing the i's for which $p|a_i$ with $p \in \{13, 17\}$ when $k = 11$ and $p|a_i$ with $p \in \{17, 19\}$ when $k = 13$, we observe that from Lemma 5.2.1 that $k - |R| \leq 1$ and $p \nmid d$ for each $p \leq k$.

5.5.1 The case $k = 11$

Let $p_1 = 11, p_2 = 13$ and $\mathcal{I} = \{0, 1, 2, \cdots, 10\}$. Since $\left(\frac{5}{11}\right) \neq \left(\frac{5}{13}\right)$, $\left(\frac{17}{11}\right) \neq \left(\frac{17}{13}\right)$ but $\left(\frac{q}{11}\right) = \left(\frac{q}{13}\right)$ for $q = 2, 3, 7$, we observe that either $5|a_i$ or $17|a_i$ for $i \in \mathcal{M}$ and either $5 \cdot 17|a_i$ or $P(a_i) \leq 7$ for $i \in \mathcal{B}$. Since $\sigma_5 \leq 3$, we obtain $|\mathcal{M}| \leq 4$.

By taking the mirror image (5.11) of (5.1), we may suppose that $0 \leq i_{13} \leq 5$ and $0 \leq i_{11} \leq 10$. If both i_{11}, i_{13} are odd, then we may suppose that i_{17} is even otherwise we get a contradiction from Lemma 5.4.1 applied to $\prod_{i=0}^{5} a_{n+i(2d)}$. Also we may suppose that $\max(i_{11}, i_{13}) \geq 4$ otherwise we get a contradiction from Lemma 5.4.1 applied to $\prod_{i=0}^{6} a_{n+4d+id}$. Further from Lemma 5.4.1, we may assume $i_{17} > 4$ if $\max(i_{11}, i_{13}) = 4$.

Since $\max(|\mathcal{I}_1^k|, |\mathcal{I}_2^k|) \geq 5$ and $|\mathcal{M}^k| \leq 4$, we restrict to those pairs satisfying $\min(|\mathcal{I}_1^k|, |\mathcal{I}_2^k|) \leq 4$ and further $\mathcal{M}^k$ is exactly one of $\mathcal{I}_1^k$ or $\mathcal{I}_2^k$ with minimum

cardinality and hence $\mathcal{B}^k$ is the other one. Now we restrict to those pairs (i_{11}, i_{13}) for which either $5|a_i$ or $17|a_i$ whenever $i \in \mathcal{M}$. Let $\mathcal{B}' = \mathcal{B} \setminus \{i : 5 \cdot 17|a_i\}$. If $|\mathcal{B}'| \geq 8$, then there are at least 6 elements $i \in \mathcal{B}'$ such that $P(a_i) \leq 3$ giving $k - |R| \geq 2$. Thus we restrict to those pairs for which $|\mathcal{B}'| \leq 7$. Further we observe that $7|a_i$ and $7|a_{i+7}$ for some $i, i+7 \in \mathcal{B}'$ if $|\mathcal{B}'| = 7$.

Let $(i_{11}, i_{13}) = (2, 4)$. Then $\mathcal{M}^k = \{1, 6, 8\}$ and $\mathcal{B}^k = \{0, 3, 5, 7, 9, 10\}$ giving $i_5 = 1$, $17|a_8$ and $P(a_i) \leq 7$ for $i \in \mathcal{B}$. For each possibility $i_7 \in \{0, 3, 4, 5\}$, and $i_{17} = 8$, we take $p_1 = 7, p_2 = 17$, $\mathcal{I} = \mathcal{B}^k$ and compute $\mathcal{I}_1$ and $\mathcal{I}_2$. Since $\left(\frac{p}{7}\right) = \left(\frac{p}{17}\right)$ for $p \in \{2, 3\}$, we should have either $\mathcal{I}_1 = \emptyset$ or $\mathcal{I}_2 = \emptyset$. We find that $\min(|\mathcal{I}_1|, |\mathcal{I}_2|) > 0$ for each possibility $i_7 \in \{0, 3, 4, 5\}$. Hence $(i_{11}, i_{13}) = (2, 4)$ is excluded. Similarly all pairs (i_{11}, i_{13}) are excluded except $(i_{11}, i_{13}) \in \{(4, 2), (6, 4)\}$. When $(i_{11}, i_{13}) = (3, 5)$, we get $\mathcal{M}^k = \{2, 7, 9\}$ giving $5|a_2a_7$, $17|a_9$ and hence it is excluded. When $(i_{11}, i_{13}) = (1, 4)$, we obtain $\mathcal{M}^k = \{5, 9\}$ and $\mathcal{B}^k = \{0, 2, 3, 6, 7, 8, 10\}$ giving either $5|a_5, 17|a_9$ or $17|a_5, 5|a_9$. Also $i_7 \in \{0, 3\}$. Thus we have $(i_7, i_{17}) \in \{(0, 5), (0, 9), (3, 5), (3, 9)\}$ and apply the procedure for each of these possibilities.

Let $(i_{11}, i_{13}) = (6, 4)$. Then $\mathcal{M}^k = \{0, 2, 7\}$ and $\mathcal{B}^k = \{1, 3, 5, 8, 9, 10\}$ giving $i_5 = 2$, $17|a_0$ and $P(a_i) \leq 7$ for $i \in \mathcal{B}$. For each possibility $i_7 \in \{1, 3, 4, 5\}$, and $i_{17} = 0$, we take $p_1 = 7, p_2 = 17$ and $\mathcal{I} = \mathcal{B}^k$. Since $\left(\frac{p}{7}\right) = \left(\frac{p}{17}\right)$ for $p \in \{2, 3\}$, we observe that either $\mathcal{I}_1 = \emptyset$ or $\mathcal{I}_2 = \emptyset$. We find that this happens only when $i_7 = 3$ where we get $\mathcal{I}_1 = \emptyset$ and $\mathcal{I}_2 = \{1, 5, 8, 9\}$. By taking modulo 7, we get $a_i \in \{1, 2\}$ for $i \in \{1, 8, 9\}$ and $a_5 \in \{3, 6\}$. Further by modulo 5, we obtain $a_1 = a_8 = 1, a_9 = 2, a_5 = 3$, $a_14, a_{10} = 7$ and this is excluded by Runge's method. When $(i_{11}, i_{13}) = (4, 2)$, we get $\mathcal{M}^k = \{0, 5, 10\}$ and $\mathcal{B}^k = \{1, 3, 6, 7, 8, 9\}$ giving $5|a_0a_5a_{10}$ and $i_{17} \in \{5, 10\}$. Here we obtain $i_{17} = 10, i_7 = 3$ where $\mathcal{I}_1 = \emptyset$ and $\mathcal{I}_2 = \{1, 6, 7, 8, 9\}$. This is not possible by Lemma 5.2.2 with $k = 4$ applied to $(n+6d)(n+6d+d)(n+6d+2d)(n+6d+3d)$.

5.5.2 The case $k = 13$

Let $p_1 = 11$, $p_2 = 13$ and $\mathcal{I} = \{0, 1, 2, \cdots, 12\}$. Since $\left(\frac{5}{11}\right) \neq \left(\frac{5}{13}\right)$, $\left(\frac{17}{11}\right) \neq \left(\frac{17}{13}\right)$ but $\left(\frac{q}{11}\right) = \left(\frac{q}{13}\right)$ for $q = 2, 3, 7$, we observe that either $5|a_i$ or $17|a_i$ for $i \in \mathcal{M}^k$ and either $5 \cdot 17|a_i$ or $19|a_i$ or $P(a_i) \leq 7$ for $i \in \mathcal{B}^k$. Since $\sigma_5 \leq 3$, we obtain $|\mathcal{M}^k| \leq 4$.

By taking the mirror image (5.11) of (5.1), we may suppose that $0 \leq i_{13} \leq 6$ and $0 \leq i_{11} \leq 10$. We may assume that $i_{11}, a_{13}, i_{17}, i_{19}$ are not all even otherwise $P(\prod_{i=0}^{5} a_{2i+1}) \leq 7$ which is excluded by Lemma 5.4.1. Further exactly two of $i_{11}, a_{13}, i_{17}, i_{19}$ are even and other two odd otherwise this is excluded again by Lemma 5.4.1 applied to $\prod^6 i = 0(n + i(2d))$ if n is odd and $\prod^6 i = 0(\frac{n}{2} + id)$ if

$n$is even. Also exactly two of $i_{11}, a_{13}, i_{17}, i_{19}$ lie in each set $\{2,3,4,5,6,7,8\}$, $\{3,4,5,6,7,8,9\}$ and $\{3,4,5,6,7,8,9\}$ otherwise this is excluded by Lemma 5.4.1.

Since $\max(|\mathcal{I}_1^k|, |\mathcal{I}_2^k|) \geq 5$ and $|\mathcal{M}^k| \leq 4$, we restrict to those pairs satisfying $\min(|\mathcal{I}_1^k|, |\mathcal{I}_2^k|) \leq 4$ and further $\mathcal{M}^k$ is exactly one of $\mathcal{I}_1^k$ or $\mathcal{I}_2^k$ with minimum cardinality and hence $\mathcal{B}^k$ is the other one. Now we restrict to those pairs (i_{11}, i_{13}) for which either $5|a_i$ or $17|a_i$ whenever $i \in \mathcal{M}$. Let $\mathcal{B}' = \mathcal{B}^k \setminus \{i : 5 \cdot 17|a_i\}$. If $|\mathcal{B}'| \geq 9$, then there are at least 6 elements $i \in \mathcal{B}'$ such that $P(a_i) \leq 3$ giving $k - |R| \geq 2$. Thus we restrict to those pairs for which $|\mathcal{B}'| \leq 8$. For instance, let $(i_{11}, i_{13}) = (0,0)$. We obtain $\mathcal{M}^k = \{5, 10\}$ and $\mathcal{B}^k = \{1,2,3,4,6,7,8,9,12\}$ giving $i_5 = 0$, $i_{17} \in \{5, 10\}$, $\mathcal{B}' = \mathcal{B}^k$ and $|\mathcal{B}^k| = 9$. This is excluded.

Let $(i_{11}, i_{13}) = (1,1)$. Then $\mathcal{M}^k = \{0, 6, 11\}$ and $\mathcal{B}^k = \{2,3,4,5,7,8,9,10\}$ giving $i_5 = 1$, $i_{17} = 0$. This is excluded. Similarly $(i_{11}, i_{13}) \in \{(1,3),(2,4),(3,5),(4,6),(6,4),(7,5),(8,6)$ are excluded where we find that i_{17} is of the same parity as i_{11}, i_{13}.

Let $(i_{11}, i_{13}) = (4,2)$. Then $\mathcal{M}^k = \{0,5,10\}$ and $\mathcal{B}^k = \{1,3,6,7,8,9,11,12\}$ giving $5|a_0, 5|a_{10}$ and $i_{17} = 5$. Further for $i \in \mathcal{B}^k$, we have either $19|a_i$ or $P(a_i) \leq 7$. Also $7|a_1$ and $7|a_8$ otherwise $k - |R| \geq 2$. We now take $(i_7, i_{17}) = (1,5)$, $p_1 = 7, p_2 = 17$, $\mathcal{I} = \mathcal{B}^k$ and compute $\mathcal{I}_1$ and $\mathcal{I}_2$. Since $\left(\frac{p}{7}\right) = \left(\frac{p}{17}\right)$ for $p \in \{2,3\}$, and $\left(\frac{19}{7}\right) = \left(\frac{19}{17}\right)$, we should have either $|\mathcal{I}_1| = 1$ or $|\mathcal{I}_2| = 1$. We find that $\mathcal{I}_1 = \{3,9,11\}$ $\mathcal{I}_2 = \{6,7,12\}$ which is a contradiction. Similarly $(i_{11}, i_{13}) \in \{(5,3),(8,4)\}$ are also excluded. When $(i_{11}, i_{13}) = (5,3)$, we find that $i_{17} = 6$ and $i_7 \in \{0,2\}$ and this is excluded. □

5.6 A Remark

We consider (5.1) with $\psi = 0, \omega(d) = 2$ and the assumption $\gcd(n,d) = 1$ replaced by $d \nmid n$ if $b > 1$. It is proved in [5] that (5.1) with $\psi = 0, b = 1$ and $k \geq 8$ is not possible. We show that (5.1) with $\psi = 0, k \geq 6$ and $\omega(d) = 2$ is not possible. The case $k = 6$ has already been solved in [1]. Let $k \geq 7$. As in [5] and since $d \nmid n$, the assertion follows if (5.1) with $\psi = 1$, $k \geq 7$, $\omega(d) = 1$ and $\gcd(n,d) = 1$ does not hold. This follows from Theorem 5.1.1.

Bibliography

[1] M. A. Bennett, N. Bruin, K. Győry, and L. Hajdu. Powers from products of consecutive terms in arithmetic progression. *Proc. London Math. Soc. (3)*, 92(2):273–306, 2006.

[2] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[3] N. R. Bruin. *Chabauty methods and covering techniques applied to generalized Fermat equations*, volume 133 of *CWI Tract*. Stichting Mathematisch Centrum Centrum voor Wiskunde en Informatica, Amsterdam, 2002. Dissertation, University of Leiden, Leiden, 1999.

[4] Nils Bruin. Chabauty methods using elliptic curves. *J. Reine Angew. Math.*, 562:27–49, 2003.

[5] Shanta Laishram and T. N. Shorey. The equation $n(n+d)\cdots(n+(k-1)d) = by^2$ with $\omega(d) \leq 6$ or $d \leq 10^{10}$. *Acta Arith.*, 129(3):249–305, 2007.

[6] Shanta Laishram and T. N. Shorey. Squares in arithmetic progression with at most two terms omitted. *Acta Arith.*, 134(4):299–316, 2008.

[7] Anirban Mukhopadhyay and T. N. Shorey. Almost squares in arithmetic progression. II. *Acta Arith.*, 110(1):1–14, 2003.

[8] Anirban Mukhopadhyay and T. N. Shorey. Almost squares in arithmetic progression. III. *Indag. Math. (N.S.)*, 15(4):523–533, 2004.

[9] N. Saradha and T. N. Shorey. Almost squares in arithmetic progression. *Compositio Math.*, 138(1):73–111, 2003.

[10] T. N. Shorey. Powers in arithmetic progressions. III. In *The Riemann zeta function and related themes: papers in honour of Professor K. Ramachandra*, volume 2 of *Ramanujan Math. Soc. Lect. Notes Ser.*, pages 131–140. Ramanujan Math. Soc., Mysore, 2006.

[11] N. P. Smart. *The algorithmic resolution of Diophantine equations*, volume 41 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1998.

[12] Sz. Tengely. Note on the paper: "An extension of a theorem of Euler" [Acta Arith. 129 (2007), no. 1, 71–102; mr2326488] by N. Hirata-Kohno, S. Laishram, T. N. Shorey and R. Tijdeman. *Acta Arith.*, 134(4):329–335, 2008.

6

Cubes in products of terms in arithmetic progression

*H*ajdu, L., Tengely, Sz. and Tijdeman, R.,
Publ. Math. Debrecen **74** (2009), 215–232.

Abstract

Euler proved that the product of four positive integers in arithmetic progression is not a square. Győry, using a result of Darmon and Merel, showed that the product of three coprime positive integers in arithmetic progression cannot be an l-th power for $l \geq 3$. There is an extensive literature on longer arithmetic progressions such that the product of the terms is an (almost) power. In this paper we extend the range of k's such that the product of k coprime integers in arithmetic progression cannot be a cube when $2 < k < 39$. We prove a similar result for almost cubes.

6.1 Introduction

In this paper we consider the problem of almost cubes in arithmetic progressions. This problem is closely related to the Diophantine equation

$$n(n+d)\dots(n+(k-1)d) = by^l \tag{6.1}$$

in positive integers n, d, k, b, y, l with $l \geq 2$, $k \geq 3$, $\gcd(n, d) = 1$, $P(b) \leq k$, where for $u \in \mathbb{Z}$ with $|u| > 1$, $P(u)$ denotes the greatest prime factor of u, and $P(\pm 1) = 1$.

This equation has a long history, with an extensive literature. We refer to the research and survey papers [3], [10], [11], [14], [16], [18], [19], [20], [23], [25], [26], [27], [29], [31], [32], [33], [34], [35], [36], [37], [38], [41], [39], the references given there, and the other papers mentioned in the introduction.

In this paper we concentrate on results where all solutions of (6.1) have been determined, under some assumptions for the unknowns. We start with results concerning squares, so in this paragraph we assume that $l = 2$. Already Euler proved that in this case equation (6.1) has no solutions with $k = 4$ and $b = 1$ (see [7] pp. 440 and 635). Obláth [21] extended this result to the case $k = 5$. Erdős [8] and Rigge [22] independently proved that equation (6.1) has no solutions with $b = d = 1$. Saradha and Shorey [28] proved that (6.1) has no solutions with $b = 1$, $k \geq 4$, provided that d is a power of a prime number. Later, Laishram and Shorey [19] extended this result to the case where either $d \leq 10^{10}$, or d has at most six prime divisors. Finally, most importantly from the viewpoint of the present paper, Hirata-Kohno, Laishram, Shorey and Tijdeman [17] completely solved (6.1) with $3 \leq k < 110$ for $b = 1$. Combining their result with those of Tengely [40] all solutions of (6.1) with $3 \leq k \leq 100$, $P(b) < k$ are determined.

Now assume for this paragraph that $l \geq 3$. Erdős and Selfridge [9] proved the celebrated result that equation (6.1) has no solutions if $b = d = 1$. In the general case $P(b) \leq k$ but still with $d = 1$, Saradha [24] for $k \geq 4$ and Győry [12], using a result of Darmon and Merel [6], for $k = 2, 3$ proved that (6.1) has no solutions with $P(y) > k$. For general d, Győry [13] showed that equation (6.1) has no solutions with $k = 3$, provided that $P(b) \leq 2$. Later, this result has been extended to the case $k < 12$ under certain assumptions on $P(b)$, see Győry, Hajdu, Saradha [15] for $k < 6$ and Bennett, Bruin, Győry, Hajdu [1] for $k < 12$.

In this paper we consider the problem for cubes, that is equation (6.1) with $l = 3$. We solve equation (6.1) nearly up to $k = 40$. In the proofs of our results we combine the approach of [17] with results of Selmer [30] and some new ideas.

6.2 Notation and results

As we are interested in cubes in arithmetic progressions, we take $l = 3$ in (6.1). That is, we consider the Diophantine equation

$$n(n + d) \dots (n + (k - 1)d) = by^3 \tag{6.2}$$

in integers n, d, k, b, y where $k \geq 3$, $d > 0$, $\gcd(n, d) = 1$, $P(b) \leq k$, $n \neq 0, y \neq 0$. (Note that similarly as e.g. in [1] we allow $n < 0$, as well.)

In the standard way, by our assumptions we can write

$$n + id = a_i x_i^3 \quad (i = 0, 1, \dots, k - 1) \tag{6.3}$$

with $P(a_i) \leq k$, a_i is cube-free. Note that (6.3) also means that in fact $n + id$ $(i = 0, 1, \dots, k - 1)$ is an arithmetic progression of almost cubes.

In case of $b = 1$ we prove the following result.

Theorem 6.2.1. *Suppose that* (n, d, k, y) *is a solution to equation* (6.2) *with* $b = 1$ *and* $k < 39$. *Then we have*

$$(n, d, k, y) = (-4, 3, 3, 2), (-2, 3, 3, -2), (-9, 5, 4, 6) \text{ or } (-6, 5, 4, 6).$$

We shall deduce Theorem 6.2.1 from the following theorem.

Theorem 6.2.2. *Suppose that* (n, d, k, b, y) *is a solution to equation* (6.2) *with* $k < 32$ *and that* $P(b) < k$ *if* $k = 3$ *or* $k \geq 13$. *Then* (n, d, k) *belongs to the following list:*

$$(n, 1, k) \text{ with } -30 \leq n \leq -4 \text{ or } 1 \leq n \leq 5,$$
$$(n, 2, k) \text{ with } -29 \leq n \leq -3,$$
$$(-10, 3, 7), (-8, 3, 7), (-8, 3, 5), (-4, 3, 5), (-4, 3, 3), (-2, 3, 3),$$
$$(-9, 5, 4), (-6, 5, 4), (-16, 7, 5), (-12, 7, 5).$$

Note that the above statement follows from Theorem 1.1 of Bennett, Bruin, Győry, Hajdu [1] in case $k < 12$ and $P(b) \leq P_k$ with $P_3 = 2$, $P_4 = P_5 = 3$, $P_6 = P_7 = P_8 = P_9 = P_{10} = P_{11} = 5$.

6.3 Lemmas and auxiliary results

We need some results of Selmer [30] on cubic equations.

Lemma 6.3.1. *The equations*

$$x^3 + y^3 = cz^3, \quad c \in \{1, 2, 4, 5, 10, 25, 45, 60, 100, 150, 225, 300\},$$
$$ax^3 + by^3 = z^3, \ (a, b) \in \{(2, 9), (4, 9), (4, 25), (4, 45), (12, 25)\}$$

have no solution in non-zero integers x, y, z.

As a lot of work will be done modulo 13, the following lemma will be very useful. Before stating it, we need to introduce a new notation. For $u, v, m \in \mathbb{Z}$, $m > 1$ by $u \overset{c}{\equiv} v \pmod{m}$ we mean that $uw^3 \equiv v \pmod{m}$ holds for some integer w with $\gcd(m, w) = 1$. We shall use this notation throughout the paper, without any further reference.

Lemma 6.3.2. *Let* n, d *be integers. Suppose that for five values* $i \in \{0, 1, ..., 12\}$ *we have* $n + id \overset{c}{\equiv} 1 \pmod{13}$. *Then* $13 \mid d$, *and* $n + id \overset{c}{\equiv} 1 \pmod{13}$ *for all* $i = 0, 1, \ldots, 12$.

Proof. Suppose that $13 \nmid d$. Then there is an integer r such that $n \equiv rd \pmod{13}$. Consequently, $n + id \equiv (r+i)d \pmod{13}$. A simple calculation yields that the cubic residues of the numbers $(r+i)d$ $(i = 0, 1, \ldots, 12)$ modulo 13 are given by a cyclic permutation of one of the sequences

$$0, 1, 2, 2, 4, 1, 4, 4, 1, 4, 2, 2, 1,$$
$$0, 2, 4, 4, 1, 2, 1, 1, 2, 1, 4, 4, 2,$$
$$0, 4, 1, 1, 2, 4, 2, 2, 4, 2, 1, 1, 4.$$

Thus the statement follows. □

Lemma 6.3.3. *Let $\alpha = \sqrt[3]{2}$ and $\beta = \sqrt[3]{3}$. Put $K = \mathbb{Q}(\alpha)$ and $L = \mathbb{Q}(\beta)$. Then the only solution of the equation*

$$\mathcal{C}_1 : \quad X^3 - (\alpha+1)X^2 + (\alpha+1)X - \alpha = (-3\alpha+6)Y^3$$

in $X \in \mathbb{Q}$ and $Y \in K$ is $(X, Y) = (2, 1)$. Further, the equation

$$\mathcal{C}_2 : \quad 4X^3 - (4\beta+2)X^2 + (2\beta+1)X - \beta = (-3\beta+3)Y^3$$

has the single solution $(X, Y) = (1, 1)$ in $X \in \mathbb{Q}$ and $Y \in L$.

Proof. Using the point $(2, 1)$ we can transform the genus 1 curve $\mathcal{C}_1$ to Weierstrass form

$$E_1 : \quad y^2 + (\alpha^2+\alpha)y = x^3 + (26\alpha^2 - 5\alpha - 37).$$

We have $E_1(K) \simeq \mathbb{Z}$ as an Abelian group and $(x, y) = (-\alpha^2-\alpha+3, -\alpha^2-3\alpha+4)$ is a non-torsion point on this curve. Applying elliptic Chabauty (cf. [4], [5]), in particular the procedure "Chabauty" of MAGMA (see [2]) with $p = 5$, we obtain that the only point on $\mathcal{C}_1$ with $X \in \mathbb{Q}$ is $(2, 1)$.

Now we turn to the second equation $\mathcal{C}_2$. We can transform this equation to an elliptic one using its point $(1, 1)$. We get

$$E_2 : \quad y^2 = x^3 + \beta^2 x^2 + \beta x + (41\beta^2 - 58\beta - 4).$$

We find that $E_2(L) \simeq \mathbb{Z}$ and $(x, y) = (4\beta - 2, -2\beta^2 + \beta + 12)$ is a non-torsion point on E_2. Applying elliptic Chabauty (as above) with $p = 11$, we get that the only point on $\mathcal{C}_2$ with $X \in \mathbb{Q}$ is $(1, 1)$. □

6.4 Proofs

In this section we provide the proofs of our results. As Theorem 6.2.1 follows from Theorem 6.2.2 by a simple inductive argument, first we give the proof of the latter result.

Proof of Theorem 6.2.2. As we mentioned, for $k = 3, 4$ the statement follows from Theorem 1.1 of [1]. Observe that the statement for every

$$k \in \{6, 8, 9, 10, 12, 13, 15, 16, 17, 19, 21, 22, 23, 25, 26, 27, 28, 29, 31\}$$

is a simple consequence of the result obtained for some smaller value of k. Indeed, for any such k let p_k denote the largest prime with $p_k < k$. Observe that in case of $k \leq 13$ $P(a_0a_1 \dots a_{p_k-1}) \leq p_k$ holds, and for $k > 13$ we have $P(a_0a_1 \dots a_{p_k}) < p_k+1$. Hence, noting that we assume $P(b) \leq k$ for $3 < k \leq 11$ and $P(b) < k$ otherwise, the theorem follows inductively from the case of p_k-term products and $p_k + 1$-term products, respectively. Hence in the sequel we deal only with the remaining values of k.

The cases $k = 5, 7$ are different from the others. In most cases a "brute force" method suffices. In the remaining cases we apply the elliptic Chabauty method (see [4], [5]).

The case $k = 5$.

In this case a very simple algorithm works already. Note that in view of Theorem 1.1 of [1], by symmetry it is sufficient to assume that $5 \mid a_2a_3$. We look at all the possible distributions of the prime factors $2, 3, 5$ of the coefficients a_i ($i = 0, \dots, 4$) one-by-one. Using that if x is an integer, then x^3 is congruent to ± 1 or 0 both (mod 7) and (mod 9), almost all possibilities can be excluded. For example,

$$(a_0, a_1, a_2, a_3, a_4) = (1, 1, 1, 10, 1)$$

is impossible modulo 7, while

$$(a_0, a_1, a_2, a_3, a_4) = (1, 1, 15, 1, 1)$$

is impossible modulo 9. (Note that the first choice of the a_i cannot be excluded modulo 9, and the second one cannot be excluded modulo 7.)

In case of the remaining possibilities, taking the linear combinations of three appropriately chosen terms of the arithmetic progression on the left hand side of (6.2) we get all solutions by Lemma 6.3.1. For example,

$$(a_0, a_1, a_2, a_3, a_4) = (2, 3, 4, 5, 6)$$

obviously survives the above tests modulo 7 and modulo 9. However, in this case using the identity $4(n + d) - 3n = n + 4d$, Lemma 6.3.1 implies that the only corresponding solution is given by $n = 2$ and $d = 1$.

After having excluded all quintuples which do not pass the above tests we are left with the single possibility

$$(a_0, a_1, a_2, a_3, a_4) = (2, 9, 2, 5, 12).$$

Here we have

$$x_0^3 + x_2^3 = 9x_1^3 \text{ and } x_0^3 - 2x_2^3 = -6x_4^3. \tag{6.4}$$

Factorizing the first equation of (6.4), a simple consideration yields that $x_0^2 - x_0x_2 + x_2^2 = 3u^3$ holds for some integer u. Put $K = \mathbb{Q}(\alpha)$ with $\alpha = \sqrt[3]{2}$. Note that the ring O_K of integers of K is a unique factorization domain, $\alpha - 1$ is a fundamental unit and $1, \alpha, \alpha^2$ is an integral basis of K, and $3 = (\alpha - 1)(\alpha + 1)^3$, where $\alpha + 1$ is a prime in O_K. A simple calculation shows that $x_0 - \alpha x_2$ and $x_0^2 + \alpha x_0x_2 + \alpha^2 x_2^2$ can have only the prime divisors α and $\alpha + 1$ in common. Hence checking the field norm of $x_0 - \alpha x_2$, by the second equation of (6.4) we get that

$$x_0 - \alpha x_2 = (\alpha - 1)^\varepsilon(\alpha^2 + \alpha)y^3$$

with $y \in O_K$ and $\varepsilon \in \{0, 1, 2\}$. Expanding the right hand side, we deduce that $\varepsilon = 0, 2$ yields $3 \mid x_0$, which is a contradiction. Thus we get that $\varepsilon = 1$, and we obtain the equation

$$(x_0 - \alpha x_2)(x_0^2 - x_0x_2 + x_2^2) = (-3\alpha + 6)z^3$$

for some $z \in O_K$. Hence after dividing both sides of this equation by x_2^3, the theorem follows from Lemma 6.3.3 in this case.

The case $k = 7$.

In this case by similar tests as for $k = 5$, we get that the only remaining possibilities are given by

$$(a_0, a_1, a_2, a_3, a_4, a_5, a_6) = (4, 5, 6, 7, 1, 9, 10), (10, 9, 1, 7, 6, 5, 4).$$

By symmetry it is sufficient to deal with the first case. Then we have

$$x_1^3 + 8x_6^3 = 9x_5^3 \text{ and } x_6^3 - 3x_1^3 = -2x_0^3. \tag{6.5}$$

Factorizing the first equation of (6.5), just as in case of $k = 5$, a simple consideration gives that $4x_6^2 - 2x_1x_6 + x_1^2 = 3u^3$ holds for some integer u. Let $L = \mathbb{Q}(\beta)$ with $\beta = \sqrt[3]{3}$. As is well-known, the ring O_L of integers of L is a unique factorization domain, $2 - \beta^2$ is a fundamental unit and $1, \beta, \beta^2$ is an integral basis of L. Further, $2 = (\beta - 1)(\beta^2 + \beta + 1)$, where $\beta - 1$ and $\beta^2 + \beta + 1$ are primes in O_L,

with field norms 2 and 4, respectively. A simple calculation yields that $x_6 - \beta x_1$ and $x_6^2 + \beta x_1 x_6 + \beta^2 x_1^2$ are relatively prime in O_L. Moreover, as $\gcd(n, d) = 1$ and x_4 is even, x_0 should be odd. Hence as the field norm of $\beta^2 + \beta + 1$ is 4, checking the field norm of $x_6 - \beta x_1$, the second equation of (6.5) yields

$$x_6 - \beta x_1 = (2 - \beta^2)^\varepsilon (1 - \beta) y^3$$

for some $y \in O_L$ and $\varepsilon \in \{0, 1, 2\}$. Expanding the right hand side, a simple computation shows that $\varepsilon = 1, 2$ yields $3 \mid x_6$, which is a contradiction. Thus we get that $\varepsilon = 0$, and we obtain the equation

$$(x_6 - \beta x_1)(4x_6^2 - 2x_1 x_6 + x_1^2) = (-3\beta + 3)z^3$$

for some $z \in O_L$. We divide both sides of this equation by x_1^3 and apply Lemma 6.3.3 to complete the case $k = 7$.

Description of the general method

So far we have considered all the possible distributions of the prime factors $\leq k$ among the coefficients a_i. For larger values of k we use a more efficient procedure similar to that in [17]. We first outline the main ideas. We explain the important case that 3, 7, and 13 are coprime to d first.

The case $\gcd(3 \cdot 7 \cdot 13, d) = 1$.

Suppose we have a solution to equation (6.2) with $k \geq 11$ and $\gcd(3 \cdot 7, d) = 1$. Then there exist integers r_7 and r_9 such that $n \equiv r_7 d \pmod 7$ and $n \equiv r_9 d \pmod 9$. Further, we can choose the integers r_7 and r_9 to be equal; put $r := r_7 = r_9$. Then $n + id \equiv (r + i)d \pmod q$ holds for $q \in \{7, 9\}$ and $i = 0, 1 \ldots, k - 1$. In particular, we have $r + i \overset{c}{\equiv} a_i s_q \pmod q$, where $q \in \{7, 9\}$ and s_q is the inverse of d modulo q. Obviously, we may assume that $r + i$ takes values only from the set $\{-31, -30, \ldots, 31\}$.

First we make a table for the residues of h modulo 7 and 9 up to cubes for $|h| < 32$, but here we present only the part with $0 \leq h < 11$.

h	0	1	2	3	4	5	6	7	8	9	10
h mod 7	0	1	2	4	4	2	1	0	1	2	4
h mod 9	0	1	2	3	4	4	3	2	1	0	1

In the first row of the table we give the values of h and in the second and third rows the corresponding residues of h modulo 7 and modulo 9 up to cubes,

respectively, where the classes of the relation $\overset{c}{\equiv}$ are represented by $0, 1, 2, 4$ modulo 7, and by $0, 1, 2, 3, 4$ modulo 9.

Let $a_{i_1}, \ldots, a_{i_t}$ be the coefficients in (6.3) which do not have prime divisors greater than 2. Put

$$E = \{(u_{i_j}, v_{i_j}) : r + i_j \overset{c}{\equiv} u_{i_j} \pmod 7, r + i_j \overset{c}{\equiv} v_{i_j} \pmod 9, 1 \le j \le t\}$$

and observe that E is contained in one of the sets

$$E_1 := \{(1,1), (2,2), (4,4)\},\ E_2 := \{(1,2), (2,4), (4,1)\},$$

$$E_3 := \{(2,1), (4,2), (1,4)\}.$$

We use this observation in the following tests which we shall illustrate by some examples.

In what follows we assume k and r to be fixed. In our method we apply the following tests in the given order. By each test some cases are eliminated.

Class cover. Let $u_i \overset{c}{\equiv} r + i \pmod 7$ and $v_i \overset{c}{\equiv} r + i \pmod 9$ $(i = 0, 1, \ldots, k-1)$. For $l = 1, 2, 3$ put

$$C_l = \{i \ :\ (u_i, v_i) \in E_l,\ i = 0, 1, \ldots, k-1\}.$$

Check whether the sets $C_1 \cup C_2$, $C_1 \cup C_3$, $C_2 \cup C_3$ can be covered by the multiples of the primes p with $p < k$, $p \neq 2, 3, 7$. If this is not possible for $C_{l_1} \cup C_{l_2}$, then we know that $E \subseteq E_{l_3}$ is impossible and E_{l_3} is excluded. Here $\{l_1, l_2, l_3\} = \{1, 2, 3\}$.

The forthcoming procedures are applied separately for each case where $E \subseteq E_l$ remains possible for some l. From this point on we also assume that the odd prime factors of the a_i are fixed.

Parity. Define the sets

$$I_e = \{(u_i, v_i) \in E_l \ :\ r + i \text{ is even},\ P(a_i) \le 2\},$$

$$I_o = \{(u_i, v_i) \in E_l \ :\ r + i \text{ is odd},\ P(a_i) \le 2\}.$$

As the only odd power of 2 is 1, $\min(|I_e|, |I_o|) \le 1$ must be valid. If this does not hold, the corresponding case is excluded.

Test modulo 13. Suppose that after the previous tests we can decide whether a_i is even for the even values of i. Assume that $E \subseteq E_l$ with fixed $l \in \{1, 2, 3\}$. Further, suppose that based upon the previous tests we can decide whether a_i can be even for the even or the odd values of i. For $t = 0, 1, 2$ put

$$U_t = \{i \ :\ a_i = \pm 2^t,\ i \in \{0, 1, \ldots, k-1\}\}$$

and let

$$U_3 = \{i \,:\, a_i = \pm 5^\gamma,\ i \in \{0,1,\dots,k-1\}, \gamma \in \{0,1,2\}\}.$$

Assume that $13 \mid n + i_0 d$ for some i_0. Recall that $13 \nmid d$ and $5 \overset{c}{\equiv} 1 \pmod{13}$. If $i, j \in U_t$ for some $t \in \{0,1,2,3\}$, then $i - i_0 \overset{c}{\equiv} j - i_0 \pmod{13}$. If $i \in U_{t_1}$, $j \in U_{t_2}$ with $0 \le t_1 < t_2 \le 2$, then $i - i_0 \overset{c}{\not\equiv} j - i_0 \pmod{13}$. We exclude all the cases which do not pass these tests.

Test modulo 7. Assume again that $E \subseteq E_l$ with fixed $l \in \{1,2,3\}$. Check whether the actual distribution of the prime divisors of the a_i yields that for some i with $7 \nmid n + id$, both $a_i = \pm t$ and $|r + i| = t$ hold for some positive integer t with $7 \nmid t$. Then

$$t \overset{c}{\equiv} n + id \overset{c}{\equiv} (r+i)d \overset{c}{\equiv} td \pmod{7}$$

implies that $d \overset{c}{\equiv} 1 \pmod{7}$. Now consider the actual distribution of the prime factors of the coefficients a_i $(i = 0,1,\dots,k-1)$. If in any a_i we know the exponents of all primes with one exception, and this exceptional prime p satisfies $p \overset{c}{\equiv} 2,3,4,5 \pmod{7}$, then we can fix the exponent of p using the above information on n. As an example, assume that $7 \mid n$, and $a_1 = \pm 5^\gamma$ with $\gamma \in \{0,1,2\}$. Then $d \overset{c}{\equiv} 1 \pmod{7}$ immediately implies $\gamma = 0$. Further, if $7 \mid n$ and $a_2 = \pm 13^\gamma$ with $\gamma \in \{0,1,2\}$, then $d \overset{c}{\equiv} 1 \pmod{7}$ gives a contradiction. We exclude all cases yielding a contradiction. Moreover, in the remaining cases we fix the exponents of the prime factors of the a_i-s whenever it is possible.

We remark that we used this procedure for $0 \ge r \ge -k+1$. In almost all cases it turned out that a_i is even for $r+i$ even. Further, we could prove that with $|r+i| = 1$ or 2 we have $a_i = \pm 1$ or ± 2, respectively, to conclude $d \overset{c}{\equiv} 1 \pmod{7}$. The test is typically effective in case when r is "around" $-k/2$. The reason for this is that then in the sequence $r, r+1, \dots, -1, 0, 1, \dots, k-r-2, k-r-1$ several powers of 2 occur.

Induction. For fixed distribution of the prime divisors of the coefficients a_i, search for arithmetic sub-progressions of length l with $l \in \{3,5,7\}$ such that for the product Π of the terms of the sub-progression $P(\Pi) \le L_l$ holds, with $L_3 = 2$, $L_5 = 5$, $L_7 = 7$. If there is such a sub-progression, then in view of Theorem 1.1 of [1], all such solutions can be determined.

An example. Now we illustrate how the above procedures work. For this purpose, take $k = 24$ and $r = -8$. Then, using the previous notation, we work with the following stripe (with $i \in \{0,1,\dots,23\}$):

$r+i$	−8	−7	−6	−5	−4	−3	−2	−1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
mod 7	1	0	1	2	4	4	2	1	0	1	2	4	4	2	1	0	1	2	4	4	2	1	0	1
mod 9	1	2	3	4	4	3	2	1	0	1	2	3	4	4	3	2	1	0	1	2	3	4	4	3

.

In the procedure Class cover we get the following classes:

$$C_1 = \{0, 4, 6, 7, 9, 10, 12, 16\}, \quad C_2 = \{3, 13, 18\}, \quad C_3 = \{19, 21\}.$$

For $p = 5, 11, 13, 17, 19, 23$ put

$$m_p = |\{i \ : \ i \in C_1 \cup C_2, \ p \mid n + id\}|,$$

respectively. Using the condition $\gcd(n, d) = 1$, one can easily check that

$$m_5 \leq 3, \ m_{11} \leq 2, \ m_{13} \leq 2, \ m_{17} \leq 1, \ m_{19} \leq 1, \ m_{23} \leq 1.$$

Hence, as $|C_1 \cup C_2| = 11$, we get that $E \subseteq E_3$ cannot be valid in this case. By a similar (but more sophisticated) calculation one gets that $E \subseteq E_2$ is also impossible. So after the procedure Class cover only the case $E \subseteq E_1$ remains.

From this point on, the odd prime divisors of the coefficients a_i are fixed, and we look at each case one-by-one. Observe that $p \mid n + id$ does not imply $p \mid a_i$. Further, $p \mid n + id$ implies $p \mid n + jd$ whenever $i \equiv j \pmod{p}$.

We consider two subcases. Suppose first that we have

$$3 \mid n + 2d, \ 5 \mid n + d, \ 7 \mid n + d, \ 11 \mid n + 7d, \ 13 \mid n + 7d,$$
$$17 \mid n + 3d, \ 19 \mid n, \ 23 \mid n + 13d.$$

Then by a simple consideration we get that in Test modulo 13 either

$$4 \in U_1 \text{ and } 10 \in U_2,$$

or

$$10 \in U_1 \text{ and } 4 \in U_2.$$

In the first case, using $13 \mid n + 7d$ we get

$$-3d \overset{c}{\equiv} 2 \pmod{13} \text{ and } 3d \overset{c}{\equiv} 4 \pmod{13},$$

which by $-3d \overset{c}{\equiv} 3d \pmod{13}$ yields a contradiction. In the second case we get a contradiction in a similar manner.

Consider now the subcase where

$$3 \mid n + 2d, \ 5 \mid n + d, \ 7 \mid n + d, \ 11 \mid n + 7d, \ 13 \mid n + 8d,$$
$$17 \mid n + 3d, \ 19 \mid n, \ 23 \mid n + 13d.$$

This case survives the Test modulo 13. However, using the strategy explained in Test modulo 7, we can easily check that if a_i is even then i is even, which yields $a_9 = \pm 1$. This immediately gives $d \overset{c}{\equiv} 1 \pmod{7}$. Further, we have $a_7 = \pm 11^{\varepsilon_7}$ with $\varepsilon_7 \in \{0, 1, 2\}$. Hence we get that

$$\pm 11^{\varepsilon_7} \overset{c}{\equiv} n + 7d \overset{c}{\equiv} d \overset{c}{\equiv} 1 \pmod{7}.$$

This gives $\varepsilon_7 = 0$, thus $a_7 = \pm 1$. Therefore $P(a_4 a_7 a_{10}) \leq 2$. Now we apply the test Induction.

The case $\gcd(3 \cdot 7 \cdot 13, d) \neq 1$.

In this case we shall use the fact that almost half of the coefficients are odd. With a slight abuse of notation, when $k > 11$ we shall assume that the coefficients $a_1, a_3, \ldots, a_{k-1}$ are odd, and the other coefficients are given either by $a_0, a_2, \ldots, a_{k-2}$ or by $a_2, a_4, \ldots, a_k$. Note that in view of $\gcd(n, d) = 1$ this can be done without loss of generality. We shall use this notation in the corresponding parts of our arguments without any further reference.

Now we continue the proof, considering the remaining cases $k \geq 11$.

The case $k = 11$.

When $\gcd(3 \cdot 7, d) = 1$, the procedures Class cover, Test modulo 7 and Induction suffice. Hence we may suppose that $\gcd(3 \cdot 7, d) > 1$.

Assume that $7 \mid d$. Observe that $P(a_0 a_1 \ldots a_4) \leq 5$ or $P(a_5 a_6 \ldots a_9) \leq 5$. Hence the statement follows by induction.

Suppose next that $3 \mid d$. Observe that if $11 \nmid a_4 a_5 a_6$ then $P(a_0 a_1 \ldots a_6) \leq 7$ or $P(a_4 a_5 \ldots a_{10}) \leq 7$. Hence by induction and symmetry we may assume that $11 \mid a_5 a_6$. Assume first that $11 \mid a_6$. If $7 \mid a_0 a_6$ then we have $P(a_1 a_2 a_3 a_4 a_5) \leq 5$. Further, in case of $7 \mid a_5$ we have $P(a_0 a_1 a_2 a_3 a_4) \leq 5$. Thus by induction we may suppose that $7 \mid a_1 a_2 a_3 a_4$. If $7 \mid a_1 a_2 a_4$ and $5 \nmid n$, we have $P(a_0 a_5 a_{10}) \leq 2$, whence by applying Lemma 6.3.1 to the identity $n + (n + 10d) = 2(n + 5d)$ we get all the solutions of (6.2). Assume next that $7 \mid a_1 a_2 a_4$ and $5 \mid n$. Hence we deduce that one among $P(a_2 a_3 a_4) \leq 2$, $P(a_1 a_4 a_7) \leq 2$, $P(a_1 a_2 a_3) \leq 2$ is valid, and the statement follows in each case in a similar manner as above. If $7 \mid a_3$, then a simple calculation yields that one among $P(a_0 a_1 a_2) \leq 2$, $P(a_0 a_4 a_8) \leq 2$, $P(a_1 a_4 a_7) \leq 2$ is valid, and we are done. Finally, assume that $11 \mid a_5$. Then by symmetry we may suppose that $7 \mid a_0 a_1 a_4 a_5$. If $7 \mid a_4 a_5$ then $P(a_6 a_7 a_8 a_9 a_{10}) \leq 5$, and the statement follows by induction. If $7 \mid a_0$ then we have $P(a_2 a_4 a_6 a_8 a_{10}) \leq 5$, and we are done too. In case of $7 \mid a_1$ one among $P(a_0 a_2 a_4) \leq 2$, $P(a_2 a_3 a_4) \leq 2$, $P(a_0 a_3 a_6) \leq 2$ holds. This completes the case $k = 11$.

The case $k = 14$.

Note that without loss of generality we may assume that $13 \mid a_i$ with $3 \leq i \leq 10$, otherwise the statement follows by induction from the case $k = 11$. Then, in particular we have $13 \nmid d$.

The tests described in the previous section suffice to dispose of the case $\gcd(3 \cdot 7 \cdot 13, d) = 1$. Assume now that $\gcd(3 \cdot 7 \cdot 13, d) > 1$ (but recall that $13 \nmid d$).

Suppose first that $7 \mid d$. Among the odd coefficients $a_1, a_3, \ldots, a_{13}$ there are at most three multiples of 3, two multiples of 5 and one multiple of 11. As $13 \overset{c}{\equiv} 1 \pmod 7$, this shows that at least for one of these a_i-s we have $a_i \overset{c}{\equiv} 1 \pmod 7$. Hence $a_i \overset{c}{\equiv} 1 \pmod 7$ for every $i = 1, 3, \ldots, 13$. Further, as none of $3, 5, 11$ is a cube modulo 7, we deduce that if i is odd, then either $\gcd(3 \cdot 5 \cdot 11, a_i) = 1$ or a_i must be divisible by at least two out of $3, 5, 11$. Noting that $13 \nmid d$, by Lemma 6.3.2 at most four numbers among $a_1, a_3, \ldots, a_{13}$ can be equal to ± 1. Moreover, $\gcd(n, d) = 1$ implies that $15 \mid a_i$ can be valid for at most one $i \in \{0, 1, \ldots, k-1\}$. Hence among the coefficients with odd indices there is exactly one multiple of 11, exactly one multiple of 15, and exactly one multiple of 13. Moreover, the multiple of 11 in question is also divisible either by 3 or by 5. In view of the proof of Lemma 6.3.2 a simple calculation yields that the cubic residues of $a_1, a_3, \ldots, a_{13}$ modulo 13 must be given by $1, 1, 4, 0, 4, 1, 1$, in this order. Looking at the spots where 4 occurs in this sequence, we get that either $3 \mid a_5, a_9$ or $5 \mid a_5, a_9$ is valid. However, this contradicts the assumption $\gcd(n, d) = 1$.

Assume now that $3 \mid d$, but $7 \nmid d$. Then among the odd coefficients $a_1, a_3, \ldots, a_{13}$ there are at most two multiples of 5 and one multiple of 7, 11 and 13 each. Lemma 6.3.2 together with $5 \overset{c}{\equiv} 1 \pmod{13}$ yields that there must be exactly four odd i-s with $a_i \overset{c}{\equiv} 1 \pmod{13}$, and further, another odd i such that a_i is divisible by 13. Hence as above, the proof of Lemma 6.3.2 shows that the a_i-s with odd indices are $\overset{c}{\equiv} 1, 1, 4, 0, 4, 1, 1 \pmod{13}$, in this order. As the prime 11 should divide an a_i with odd i and $a_i \overset{c}{\equiv} 4 \pmod{13}$, this yields that $11 \mid a_5 a_9$. However, as above, this immediately yields that $P(a_0 a_2 \ldots a_{12}) \leq 7$ (or $P(a_2 a_4 \ldots a_{14}) \leq 7$), and the case $k = 14$ follows by induction.

The case $k = 18$.

Using the procedures described in the previous section, the case $\gcd(3 \cdot 7 \cdot 13, d) = 1$ can be excluded. So we may assume $\gcd(3 \cdot 7 \cdot 13, d) > 1$.

Suppose first that $7 \mid d$. Among $a_1, a_3, \ldots, a_{17}$ there are at most three multiples of 3, two multiples of 5 and one multiple of 11, 13 and 17 each. Hence at least for one odd i we have $a_i = \pm 1$. Thus all of $a_1, a_3, \ldots, a_{17}$ are $\overset{c}{\equiv} 1 \pmod 7$. Among the primes $3, 5, 11, 13, 17$ only 13 is $\overset{c}{\equiv} 1 \pmod 7$, so the other primes cannot occur alone. Hence we get that $a_i = \pm 1$ for at least five out of $a_1, a_3, \ldots, a_{17}$. However, by Lemma 6.3.2 this is possible only if $13 \mid d$.

In that case $a_i = \pm 1$ holds for at least six coefficients with i odd. Now a simple calculation shows that among them three are in arithmetic progression. This leads to an equation of the shape $X^3 + Y^3 = 2Z^3$, and Lemma 6.3.1 applies.

Assume next that $13 \mid d$, but $7 \nmid d$. Among the odd coefficients $a_1, a_3, \dots a_{17}$ there are at most three multiples of 3, two multiples of 5 and 7 each, and one multiple of 11 and 17 each. Hence, by $5 \overset{c}{\equiv} 1 \pmod{13}$ there are at least two $a_i \overset{c}{\equiv} 1 \pmod{13}$, whence all $a_i \overset{c}{\equiv} 1 \pmod{13}$. As from this list only the prime 5 is a cube modulo 13, we get that at least four out of the above nine odd a_i-s are equal to ± 1. Recall that $7 \nmid d$ and observe that the cubic residues modulo 7 of a seven-term arithmetic progression with common difference not divisible by 7 is a cyclic permutation of one of the sequences

$$0, 1, 2, 4, 4, 2, 1, \quad 0, 2, 4, 1, 1, 4, 2, \quad 0, 4, 1, 2, 2, 1, 4.$$

Hence remembering that for four odd i we have $a_i = \pm 1$, we get that the cubic residues of $a_1, a_3, \dots, a_{17}$ modulo 7 are given by $1, 1, 4, 2, 0, 2, 4, 1, 1$, in this order. In particular, we have exactly one multiple of 7 among them. Further, looking at the spots where $0, 2$ and 4 occur, we deduce that at most two of the a_i-s with odd indices can be multiples of 3. Switching back to modulo 13, this yields that $a_i = \pm 1$ for at least five a_i-s. However, this contradicts Lemma 6.3.2.

Finally, assume that $3 \mid d$. In view of what we have proved already, we may further suppose that $\gcd(7 \cdot 13, d) = 1$. Among the odd coefficients $a_1, a_3, \dots, a_{17}$ there are at most two multiples of 5 and 7 each, and one multiple of 11, 13 and 17 each. Hence as $7 \nmid d$ and $13 \overset{c}{\equiv} 1 \pmod{7}$, we get that the cubic residues modulo 7 of the coefficients a_i with odd i are given by one of the sequences

$$1, 0, 1, 2, 4, 4, 2, 1, 0, \quad 0, 1, 2, 4, 4, 2, 1, 0, 1, \quad 1, 1, 2, 4, 0, 4, 2, 1, 1.$$

In view of the places of the values 2 and 4, we see that it is not possible to distribute the prime divisors $5, 7, 11$ over the a_i-s with odd indices. This finishes the case $k = 18$.

The case $k = 20$.

By the help of the procedures described in the previous section, in case of $\gcd(3 \cdot 7 \cdot 13, d) = 1$ all solutions to equation (6.2) can be determined. Assume now that $\gcd(3 \cdot 7 \cdot 13, d) > 1$.

We start with the case $7 \mid d$. Then among the odd coefficients $a_1, a_3, \dots, a_{19}$ there are at most four multiples of 3, two multiples of 5, and one multiple of 11, 13, 17 and 19 each. As $13 \overset{c}{\equiv} 1 \pmod{7}$, this yields that $a_i \overset{c}{\equiv} 1 \pmod{7}$ for all i. Hence the primes $3, 5, 11, 17, 19$ must occur at least in pairs in the a_i-s

with odd indices, which yields that at least five such coefficients are equal to ± 1. Thus Lemma 6.3.2 gives $13 \mid d$, whence $a_i \overset{c}{\equiv} 1 \pmod{13}$ for all i. Hence we deduce that the prime 5 may be only a third prime divisor of the a_i-s with odd indices, and so at least seven out of $a_1, a_3, \ldots, a_{19}$ equal ± 1. However, then there are three such coefficients which belong to an arithmetic progression. Thus by Lemma 6.3.1 we get all solutions in this case.

Assume next that $13 \mid d$. Without loss of generality we may further suppose that $7 \nmid d$. Then among the odd coefficients $a_1, a_3, \ldots, a_{19}$ there are at most four multiples of 3, two multiples of 5 and 7 each, and one multiple of 11, 17 and 19 each. As $5 \overset{c}{\equiv} 1 \pmod{13}$ this implies $a_i \overset{c}{\equiv} 1 \pmod{13}$ for all i, whence the primes $3, 7, 11, 17, 19$ should occur at least in pairs in the a_i-s with odd i. Hence at least four of these coefficients are equal to ± 1. By a similar argument as in case of $k = 18$, we get that the cubic residues of $a_1, a_3, \ldots, a_{19}$ modulo 7 are given by one of the sequences

$$1, 0, 1, 2, 4, 4, 2, 1, 0, 1, \quad 1, 1, 4, 2, 0, 2, 4, 1, 1, 4, \quad 4, 1, 1, 4, 2, 0, 2, 4, 1, 1.$$

In view of the positions of the $0, 2$ and 4 values, we get that at most two corresponding terms can be divisible by 3 in the first case, which modulo 13 yields that the number of odd i-s with $a_i = \pm 1$ is at least five. This is a contradiction modulo 7. Further, in the last two cases at most three terms can be divisible by 3, and exactly one term is a multiple of 7. This yields modulo 13 that the number of odd i-s with $a_i = \pm 1$ is at least five, which is a contradiction modulo 7 again.

Finally, suppose that $3 \mid d$. We may assume that $\gcd(7 \cdot 13, d) = 1$. Then among the odd coefficients $a_1, a_3, \ldots, a_{19}$ there are at most two multiples of 5 and 7 each, and one multiple of 11, 13, 17 and 19 each. Hence Lemma 6.3.2 yields that exactly four of these coefficients should be $\overset{c}{\equiv} 1 \pmod{13}$, and exactly one of them must be a multiple of 13. Further, exactly two other a_i-s with odd indices are multiples of 7, and these a_i-s are divisible by none of $11, 13, 17, 19$. So in view of the proof of Lemma 6.3.2 a simple calculation gives that the cubic residues of $a_1, a_3, \ldots, a_{19}$ modulo 13 are given by one of the sequences

$$0, 2, 4, 4, 1, 2, 1, 1, 2, 1, \quad 1, 2, 1, 1, 2, 1, 4, 4, 2, 0,$$

$$2, 4, 2, 1, 1, 4, 0, 4, 1, 1, \quad 1, 1, 4, 0, 4, 1, 1, 2, 4, 2.$$

In the upper cases we get that 7 divides two terms with $a_i \overset{c}{\equiv} 2 \pmod{13}$, whence the power of 7 should be 2 in both cases. However, this implies $7^2 \mid 14d$, hence $7 \mid d$, a contradiction. As the lower cases are symmetric, we may assume that the very last possibility occurs. In that case we have $7 \mid a_5$ and $7 \mid a_{19}$. We may

assume that $11 \mid a_{17}$, otherwise $P(a_6 a_8 \dots a_{18}) \leq 7$ and the statement follows by induction. Further, we also have $13 \mid a_7$, and $17 \mid a_9$ and $19 \mid a_{15}$ or vice versa. Hence either $P(a_3 a_8 a_{13}) \leq 2$ or $P(a_4 a_{10} a_{16}) \leq 2$, and induction suffices to complete the case $k = 20$.

The case $k = 24$.

The procedures described in the previous section suffice to completely treat the case $\gcd(3 \cdot 7 \cdot 13, d) = 1$. So we may assume that $\gcd(3 \cdot 7 \cdot 13, d) > 1$ is valid.

Suppose first that $7 \mid d$. Among the odd coefficients $a_1, a_3, \dots, a_{23}$ there are at most four multiples of 3, three multiples of 5, two multiples of 11, and one multiple of 13, 17, 19 and 23 each. We know that all a_i belong to the same cubic class modulo 7. As $3 \overset{c}{\equiv} 4 \pmod 7$, $5 \overset{c}{\equiv} 2 \pmod 7$ and among the coefficients $a_1, a_3, \dots, a_{23}$ there are at most two multiples of 3^2 and at most one multiple of 5^2, we get that these coefficients are all $\overset{c}{\equiv} 1 \pmod 7$. This yields that the primes $3, 5, 11, 17, 19, 23$ may occur only at least in pairs in the coefficients with odd indices. Thus we get that at least five out of $a_1, a_3, \dots, a_{23}$ are $\overset{c}{\equiv} 1 \pmod{13}$. Hence, by Lemma 6.3.2 we get that $13 \mid d$ and consequently $a_i \overset{c}{\equiv} 1 \pmod{13}$ for all i. This also shows that the 5-s can be at most third prime divisors of the a_i-s with odd indices. So we deduce that at least eight out of the odd coefficients $a_1, a_3, \dots, a_{23}$ are equal to ± 1. However, a simple calculation shows that from the eight corresponding terms we can always choose three forming an arithmetic progression. Hence this case follows from Lemma 6.3.1.

Assume next that $13 \mid d$, but $7 \nmid d$. Among the coefficients with odd indices there are at most four multiples of 3, three multiples of 5, two multiples of 7 and 11 each, and one multiple of 17, 19 and 23 each. Hence, by $5 \overset{c}{\equiv} 1 \pmod{13}$ we deduce $a_i \overset{c}{\equiv} 1 \pmod{13}$ for all i. As before, a simple calculation yields that at least for four of these odd coefficients $a_i = \pm 1$ hold. Hence looking at the possible cases modulo 7, one can easily see that we cannot have four multiples of 3 at the places where $0, 2$ and 4 occur as cubic residues modulo 7. Hence in view of Lemma 6.3.2 we need to use two 11-s, which yields that $11 \mid a_1$ and $11 \mid a_{23}$. Thus the only possibility for the cubic residues of $a_1, a_3, \dots, a_{23}$ modulo 7 is given by the sequence

$$2, 1, 0, 1, 2, 4, 4, 2, 1, 0, 1, 2.$$

However, the positions of the 2-s and 4-s allow to have at most two a_i-s with odd indices which are divisible by 3 but not by 7. Hence switching back to modulo 13, we get that there are at least five a_i-s which are ± 1, a contradiction by Lemma 6.3.2.

Finally, assume that $3 \mid d$, and $\gcd(7\cdot 13, d) = 1$. Then among $a_1, a_3, \ldots, a_{23}$ there are at most three multiples of 5, two multiples of 7 and 11 each, and one multiple of 13, 17, 19 and 23 each. Hence by Lemma 6.3.2 we get that exactly four of the coefficients $a_1, a_3, \ldots, a_{23}$ are $\overset{c}{\equiv} 1 \pmod{13}$, and another is a multiple of 13. Further, all the mentioned prime factors (except the 5-s) divide distinct a_i-s with odd indices. Using that at most these coefficients can be divisible by 7^2 and 11^2, in view of the proof of Lemma 6.3.2 we get that the only possibilities for the cubic residues of these coefficients modulo 13 are given by one of the sequences

$$2, 2, 4, 2, 1, 1, 4, 0, 4, 1, 1, 2, \quad 2, 1, 1, 4, 0, 4, 1, 1, 2, 4, 2, 2.$$

By symmetry we may assume the first possibility. Then we have $7 \mid a_3$, $11 \mid a_1$, $13 \mid a_{15}$, and $17, 19, 23$ divide a_5, a_7, a_{13} in some order. Hence $P(a_4a_9a_{14}) \le 2$, or $5 \mid n + 4d$ whence $P(a_{16}a_{18}a_{20}) \le 2$. In both cases we apply induction.

The case $k = 30$.

By the help of the procedures described in the previous section, the case $\gcd(3 \cdot 7 \cdot 13, d) = 1$ can be excluded. Assume now that $\gcd(3 \cdot 7 \cdot 13, d) > 1$.

We start with the case $7 \mid d$. Then among the odd coefficients $a_1, a_3, \ldots, a_{29}$ there are at most five multiples of 3, three multiples of 5, two multiples of 11 and 13 each, and one multiple of 17, 19, 23 and 29 each. As $13 \overset{c}{\equiv} 29 \overset{c}{\equiv} 1 \pmod 7$, this yields that $a_i \overset{c}{\equiv} 1 \pmod 7$ for all i. Hence the other primes must occur at least in pairs in the a_i-s with odd indices, which yields that at least six such coefficients are equal to ± 1. Further, we get that the number of such coefficients $\overset{c}{\equiv} 0, 1 \pmod{13}$ is at least eight. However, by Lemma 6.3.2 this is possible only if $13 \mid d$, whence $a_i \overset{c}{\equiv} 1 \pmod{13}$ for all i. Then 5 and 29 can be at most third prime divisors of the coefficients a_i-s with odd i-s. So a simple calculation gives that at least ten out of the odd coefficients $a_1, a_3, \ldots, a_{29}$ are equal to ± 1. Hence there are three such coefficients in arithmetic progression, and the statement follows from Lemma 6.3.1.

Assume next that $13 \mid d$, but $7 \nmid d$. Then among the odd coefficients $a_1, a_3, \ldots, a_{29}$ there are at most five multiples of 3, three multiples of 5 and 7 each, two multiples of 11, and one multiple of 17, 19, 23 and 29 each. From this we get that $a_i \overset{c}{\equiv} 1 \pmod{13}$ for all i. Hence the primes different from 5 should occur at least in pairs. We get that at least five out of the coefficients $a_1, a_3, \ldots, a_{29}$ are equal to ± 1. Thus modulo 7 we get that it is impossible to have three terms divisible by 7. Then it follows modulo 13 that at least six a_i-s

with odd indices are equal to ± 1. However, this is possible only if $7 \mid d$, which is a contradiction.

Finally, assume that $3 \mid d$, but $\gcd(7 \cdot 13, d) = 1$. Then among the odd coefficients $a_1, a_3, \ldots, a_{29}$ there are at most three multiples of 5 and 7 each, two multiples of 11 and 13 each, and one multiple of 17, 19, 23 and 29 each. Further, modulo 7 we get that all primes $5, 11, 17, 19, 23$ divide distinct a_i-s with odd indices, and the number of odd i-s with $a_i \overset{c}{\equiv} 0, 1 \pmod 7$ is seven. However, checking all possibilities modulo 7, we get a contradiction. This completes the proof of Theorem 6.2.2. □

Proof of Theorem 6.2.1. Obviously, for $k < 32$ the statement is an immediate consequence of Theorem 6.2.2. Further, observe that $b = 1$ implies that for any k with $31 < k < 39$, one can find j with $0 \leq j \leq k - 30$ such that $P(a_j a_{j+1} \ldots a_{j+29}) \leq 29$. Hence the statement follows from Theorem 6.2.2. □

Bibliography

[1] M. A. Bennett, N. Bruin, K. Győry, and L. Hajdu. Powers from products of consecutive terms in arithmetic progression. *Proc. London Math. Soc. (3)*, 92(2):273–306, 2006.

[2] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[3] B. Brindza, L. Hajdu, and I. Z. Ruzsa. On the equation $x(x+d)\cdots(x+(k-1)d) = by^2$. *Glasg. Math. J.*, 42(2):255–261, 2000.

[4] N. R. Bruin. *Chabauty methods and covering techniques applied to generalized Fermat equations*, volume 133 of *CWI Tract*. Stichting Mathematisch Centrum Centrum voor Wiskunde en Informatica, Amsterdam, 2002. Dissertation, University of Leiden, Leiden, 1999.

[5] Nils Bruin. Chabauty methods using elliptic curves. *J. Reine Angew. Math.*, 562:27–49, 2003.

[6] H. Darmon and L. Merel. Winding quotients and some variants of Fermat's last theorem. *J. Reine Angew. Math.*, 490:81–100, 1997.

[7] L.E. Dickson. *History of the theory of numbers. Vol II: Diophantine analysis*. Chelsea Publishing Co., New York, 1966.

[8] P. Erdös. Note on the product of consecutive integers (II). *J. London Math. Soc.*, 14:245–249, 1939.

[9] P. Erdős and J. L. Selfridge. The product of consecutive integers is never a power. *Illinois J. Math.*, 19:292–301, 1975.

[10] P. Filakovszky and L. Hajdu. The resolution of the Diophantine equation $x(x+d)\cdots(x+(k-1)d) = by^2$ for fixed d. *Acta Arith.*, 98(2):151–154, 2001.

[11] K. Győry. On the Diophantine equation $\binom{n}{k} = x^l$. *Acta Arith.*, 80(3):289–295, 1997.

[12] K. Győry. On the Diophantine equation $n(n+1)\cdots(n+k-1) = bx^l$. *Acta Arith.*, 83(1):87–92, 1998.

[13] K. Györy. Power values of products of consecutive integers and binomial coefficients. In *Number theory and its applications (Kyoto, 1997)*, volume 2 of *Dev. Math.*, pages 145–156. Kluwer Acad. Publ., Dordrecht, 1999.

[14] K. Győry. Perfect powers in products with consecutive terms from arithmetic progressions. In *More sets, graphs and numbers*, volume 15 of *Bolyai Soc. Math. Stud.*, pages 143–155. Springer, Berlin, 2006.

[15] K. Győry, L. Hajdu, and N. Saradha. On the Diophantine equation $n(n+d)\cdots(n+(k-1)d) = by^l$. *Canad. Math. Bull.*, 47(3):373–388, 2004.

[16] G. Hanrot, N. Saradha, and T. N. Shorey. Almost perfect powers in consecutive integers. *Acta Arith.*, 99(1):13–25, 2001.

[17] N. Hirata-Kohno, S. Laishram, T. N. Shorey, and R. Tijdeman. An extension of a theorem of Euler. *Acta Arith.*, 129(1):71–102, 2007.

[18] Shanta Laishram. An estimate for the length of an arithmetic progression the product of whose terms is almost square. *Publ. Math. Debrecen*, 68(3-4):451–475, 2006.

[19] Shanta Laishram and T. N. Shorey. The equation $n(n+d)\cdots(n+(k-1)d) = by^2$ with $\omega(d) \leq 6$ or $d \leq 10^{10}$. *Acta Arith.*, 129(3):249–305, 2007.

[20] R. Marszałek. On the product of consecutive elements of an arithmetic progression. *Monatsh. Math.*, 100(3):215–222, 1985.

[21] Richard Obláth. Über das Produkt fünf aufeinander folgender Zahlen in einer arithmetischen Reihe. *Publ. Math. Debrecen*, 1:222–226, 1950.

[22] O. Rigge. über ein diophantisches problem. In *9th Congress Math. Scand.*, pages 155–160. Mercator 1939, Helsingfors 1938.

[23] J. W. Sander. Rational points on a class of superelliptic curves. *J. London Math. Soc. (2)*, 59(2):422–434, 1999.

[24] N. Saradha. On perfect powers in products with terms from arithmetic progressions. *Acta Arith.*, 82(2):147–172, 1997.

[25] N. Saradha. Squares in products with terms in an arithmetic progression. *Acta Arith.*, 86(1):27–43, 1998.

[26] N. Saradha and T. N. Shorey. Almost perfect powers in arithmetic progression. *Acta Arith.*, 99(4):363–388, 2001.

[27] N. Saradha and T. N. Shorey. Almost squares and factorisations in consecutive integers. *Compositio Math.*, 138(1):113–124, 2003.

[28] N. Saradha and T. N. Shorey. Almost squares in arithmetic progression. *Compositio Math.*, 138(1):73–111, 2003.

[29] N. Saradha and T. N. Shorey. Contributions towards a conjecture of Erdős on perfect powers in arithmetic progression. *Compos. Math.*, 141(3):541–560, 2005.

[30] Ernst S. Selmer. The Diophantine equation $ax^3 + by^3 + cz^3 = 0$. *Acta Math.*, 85:203–362 (1 plate), 1951.

[31] T. N. Shorey. Perfect powers in products of arithmetical progressions with fixed initial term. *Indag. Math. (N.S.)*, 7(4):521–525, 1996.

[32] T. N. Shorey. Powers in arithmetic progression. In *A panorama of number theory or the view from Baker's garden (Zürich, 1999)*, pages 325–336. Cambridge Univ. Press, Cambridge, 2002.

[33] T. N. Shorey. Powers in arithmetic progressions. II. *Sūrikaisekikenkyūsho Kōkyūroku*, (1274):202–214, 2002. New aspects of analytic number theory (Japanese) (Kyoto, 2001).

[34] T. N. Shorey. Diophantine approximations, Diophantine equations, transcendence and applications. *Indian J. Pure Appl. Math.*, 37(1):9–39, 2006.

[35] T. N. Shorey and R. Tijdeman. Perfect powers in products of terms in an arithmetical progression. *Compositio Math.*, 75(3):307–344, 1990.

[36] T. N. Shorey and R. Tijdeman. Perfect powers in products of terms in an arithmetical progression. II. *Compositio Math.*, 82(2):119–136, 1992.

[37] T. N. Shorey and R. Tijdeman. Perfect powers in products of terms in an arithmetical progression. III. *Acta Arith.*, 61(4):391–398, 1992.

[38] T. N. Shorey and R. Tijdeman. Some methods of Erdős applied to finite arithmetic progressions. In *The mathematics of Paul Erdős, I*, volume 13 of *Algorithms Combin.*, pages 251–267. Springer, Berlin, 1997.

[39] Sz. Tengely. *Effective Methods for Diophantine Equations*. PhD thesis, Leiden Univ., Leiden, The Netherlands, 2005.

[40] Sz. Tengely. Note on the paper: "An extension of a theorem of Euler" [Acta Arith. 129 (2007), no. 1, 71–102; mr2326488] by N. Hirata-Kohno, S. Laishram, T. N. Shorey and R. Tijdeman. *Acta Arith.*, 134(4):329–335, 2008.

[41] R. Tijdeman. Diophantine equations and Diophantine approximations. In *Number theory and applications (Banff, AB, 1988)*, volume 265 of *NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci.*, pages 215–243. Kluwer Acad. Publ., Dordrecht, 1989.

7

Arithmetic progressions consisting of unlike powers

*B*ruin, N., Győry, K., Hajdu, L. and Tengely, Sz.,
Indag. Math. (N.S.) **17** (2006), 539–555.

Abstract

In this paper we present some new results about unlike powers in arithmetic progression. We prove among other things that for given $k \geq 4$ and $L \geq 3$ there are only finitely many arithmetic progressions of the form $(x_0^{l_0}, x_1^{l_1}, \ldots, x_{k-1}^{l_{k-1}})$ with $x_i \in \mathbb{Z}$, $\gcd(x_0, x_1) = 1$ and $2 \leq l_i \leq L$ for $i = 0, 1, \ldots, k-1$. Furthermore, we show that, for $L = 3$, the progression $(1, 1, \ldots, 1)$ is the only such progression up to sign. Our proofs involve some well-known theorems of Faltings [10], Darmon and Granville [7] as well as Chabauty's method applied to superelliptic curves.

7.1 Introduction

By a classical result of Euler, which apparently was already known to Fermat (see [9] pp. 440 and 635), four distinct squares cannot form an arithmetic progression. Darmon and Merel [8] proved that, apart from trivial cases, there do not exist 3-term arithmetic progressions consisting of l-th powers, provided $l \geq 3$. More generally, perfect powers from products of consecutive terms in arithmetic progression have been extensively studied in a great number of papers; see e.g. [20], [17] and [2] and the references there. In our article we deal with the following problem.

Question. For all $k \geq 3$ characterize the non-constant arithmetic progressions

$$(h_0, h_1, \ldots, h_{k-1})$$

with $\gcd(h_0, h_1) = 1$ such that each $h_i = x_i^{l_i}$ for some $x_i \in \mathbb{Z}$ and $l_i \geq 2$.

Note that we impose the seemingly artificial primitivity condition $\gcd(h_0, h_1) = 1$. In case the h_i are all like powers, the homogeneity of the conditions ensures that up to scaling, we can assume $\gcd(h_0, h_1) = 1$ without loss of generality. If we do not take all l_i equal, however, there are infinite families that are not quite trivial, but are characterized by the fact they have a fairly large common factor in their terms; see the examples below Theorem 3.

By a recent result of Hajdu [13] the ABC conjecture implies that if

$$(x_0^{l_0}, x_1^{l_1}, \ldots, x_{k-1}^{l_{k-1}})$$

is an arithmetic progression with $\gcd(x_0, x_1) = 1$ and $l_i \geq 2$ for each i, then k and the l_i are bounded. Furthermore, he shows unconditionally that k can be bounded above in terms of $\max_i\{l_i\}$. In fact Hajdu proves these results for more general arithmetic progressions which satisfy the assumptions (i), (ii) of our Theorem 2 below.

As is known (see e.g. [14],[7],[15],[20],[19] and the references given there), there exist integers $l_0, l_1, l_2 \geq 2$ for which there are infinitely many primitive arithmetic progressions of the form $(x_0^{l_0}, x_1^{l_1}, x_2^{l_2})$. In these progressions the exponents in question always satisfy the condition

$$\frac{1}{l_0} + \frac{1}{l_1} + \frac{1}{l_2} \geq 1.$$

One would, however, expect only very few primitive arithmetic progressions of length at least four and consisting entirely from powers at least two. A definitive answer to the above question seems beyond present techniques. As in [13], we restrict the size of the exponents l_i and prove the following finiteness result:

Theorem 7.1.1. *Let $k \geq 4$ and $L \geq 2$. There are only finitely many k-term integral arithmetic progressions $(h_0, h_1, \ldots, h_{k-1})$ such that $\gcd(h_0, h_1) = 1$ and $h_i = x_i^{l_i}$ with some $x_i \in \mathbb{Z}$ and $2 \leq l_i \leq L$ for $i = 0, 1, \ldots, k-1$.*

The proof of this theorem uses that for each of the finitely many possible exponent vectors $(l_0, \ldots, l_{k-1})$, the primitive arithmetic progressions of the form $(x_0^{l_0}, \ldots, x_{k-1}^{l_{k-1}})$ correspond to the rational points on finitely many algebraic curves. In most cases, these curves are of genus larger than 1 and thus, by Faltings' theorem [10], give rise to only finitely many solutions.

In fact, our Theorem 1 above is a direct consequence of the following more general result and a theorem by Euler on squares in arithmetic progression. For a finite set of primes S, we write $\mathbb{Z}_S^*$ for the set of rational integers not divisible by primes outside S.

Theorem 7.1.2. *Let L, k and D be positive integers with $L \geq 2, k \geq 3$, and let S be a finite set of primes. Then there are at most finitely many arithmetic progressions $(h_0, h_1, \ldots, h_{k-1})$ satisfying the following conditions:*

(i) For $i = 0, \ldots, k-1$, there exist $x_i \in \mathbb{Z}$, $2 \leq l_i \leq L$ and $\eta_i \in \mathbb{Z}_S^*$ such that

$$h_i = \eta_i x_i^{l_i},$$

(ii) $\gcd(h_0, h_1) \leq D$,

(iii) either $k \geq 5$, or $k = 4$ and $l_i \geq 3$ for some i, or $k = 3$ and $\frac{1}{l_0} + \frac{1}{l_1} + \frac{1}{l_2} < 1$.

Remark. In (iii) the assumptions concerning the exponents l_i are necessary. For $k = 3$ this was seen above. In case of $k = 4$ the condition $l_i \geq 3$ for some i cannot be omitted as is shown by e.g. the arithmetic progression $x_0^2, x_1^2, x_2^2, 73x_3^2$ with $S = \{73\}$. We have the homogeneous system of equations

$$x_0^2 + x_2^2 = 2x_1^2$$
$$x_1^2 + 73x_3^2 = 2x_2^2.$$

A non-singular intersection of two quadrics in $\mathbb{P}^3$ is a genus 1 curve. If there is a rational point on it, it is isomorphic to its Jacobian - an elliptic curve. In this example the elliptic curve has infinitely many rational points. Therefore we also have infinitely many rational solutions $(x_0 : x_1 : x_2 : x_3)$. After rescaling, those all give primitive integral solutions as well.

For small l_i we can explicitly find the parametrizing algebraic curves and, using Chabauty's method, the rational points on them. This allows us to prove:

Theorem 7.1.3. *Let $k \geq 4$, and suppose that $(h_0, h_1, \ldots, h_{k-1}) = (x_0^{l_0}, x_1^{l_1}, \ldots, x_{k-1}^{l_{k-1}})$ is a primitive integral arithmetic progression with $x_i \in \mathbb{Z}$ and $2 \leq l_i \leq 3$ for $i = 0, 1, \ldots, k-1$. Then*

$$(h_0, h_1, \ldots, h_{k-1}) = \pm(1, 1, \ldots, 1).$$

The proof is rather computational in nature and uses p-adic methods to derive sharp bounds on the number of rational points on specific curves. The methods are by now well-established. Of particular interest to the connoisseur would be the argument for the curve $\mathcal{C}_4$ in Section 3, where we derive that an elliptic curve has rank 0 and a non-trivial Tate-Shafarevich group by doing a full 2-descent on an isogenous curve and the determination of the solutions to equation (7). The novelty for the latter case lies in the fact that, rather than considering a hyperelliptic curve, we consider a superelliptic curve of the form

$$f(x) = y^3, \text{ with } \deg(f) = 6.$$

We then proceed similarly to [4]. We determine an extension K over which $f(x) = g(x) \cdot h(x)$, with g, h both cubic. We then determine that $\mathbb{Q}$-rational solutions to $f(x) = y^3$ by determining, for finitely many values δ, the K-rational points on the genus 1 curve $g(x) = \delta y_1^3$, with $x \in \mathbb{Q}$.

Remark. The condition $\gcd(h_0, h_1) = 1$ in Theorems 1 and 3 is necessary. This can be illustrated by the following examples with $k = 4$. Note that the progressions below can be "reversed" to get examples for the opposite orders of the exponents l_0, l_1, l_2, l_3.

- In case of $(l_0, l_1, l_2, l_3) = (2, 2, 2, 3)$

$$((u^2 - 2uv - v^2)f(u,v))^2, ((u^2 + v^2)f(u,v))^2, ((u^2 + 2uv - v^2)f(u,v))^2, (f(u,v))^3$$

is an arithmetic progression for any $u, v \in \mathbb{Z}$, where $f(u,v) = u^4 + 8u^3v + 2u^2v^2 - 8uv^3 + v^4$.

- In case of $(l_0, l_1, l_2, l_3) = (2, 2, 3, 2)$

$$((u^2-2uv-2v^2)g(u,v))^2, ((u^2+2v^2)g(u,v))^2, (g(u,v))^3, ((u^2+4uv-2v^2)g(u,v))^2$$

is an arithmetic progression for any $u, v \in \mathbb{Z}$, where $g(u,v) = u^4 + 4u^3v + 8u^2v^2 - 8uv^3 + 4v^4$.

7.2 Auxiliary results

The proof of Theorem 2 depends on the following well-known result by Darmon and Granville [7].

Theorem A. Let A, B, C and r, s, t be non-zero integers with $r, s, t \geq 2$, and let S be a finite set of primes. Then there exists a number field K such that all solutions $x, y, z \in \mathbb{Z}$ with $\gcd(x, y, z) \in \mathbb{Z}_S^*$ to the equation

$$Ax^r + By^s = Cz^t$$

correspond, up to weighted projective equivalence, to K-rational points on some algebraic curve $X_{r,s,t}$ defined over K. Putting $u = -Ax^r/Cz^t$, the curve X is a Galois-cover of the u-line of degree d, unramified outside $u \in \{0, 1, \infty\}$ and with ramification indices $e_0 = r, e_1 = s, e_2 = t$. Writing $\chi(r, s, t) = 1/r + 1/s + 1/t$ and g for the genus of X, we find

- if $\chi(r, s, t) > 1$ then $g = 0$ and $d = 2/\chi(r, s, t)$,
- if $\chi(r, s, t) = 1$ then $g = 1$,

- if $\chi(r,s,t) < 1$ then $g > 1$.

The two results below will be useful for handling special progressions, containing powers with small exponents. The first one deals with the quadratic case.

Theorem B. Four distinct squares cannot form an arithmetic progression.

Proof. The statement is a simple consequence of a classical result of Euler (cf. [14], p. 21), which was already known by Fermat (see [9] pp. 440 and 635). □

We also need a classical result on a cubic equation.

Theorem C. The equation $x^3 + y^3 = 2z^3$ has the only solutions $(x,y,z) = \pm(1,1,1)$ in non-zero integers x,y,z with $\gcd(x,y,z) = 1$.

Proof. See Theorem 3 in [14] on p. 126. □

The next lemma provides the parametrization of the solutions of certain ternary Diophantine equations.

Lemma 7.2.1. *All solutions of the equations*

$$i)\ 2b^2 - a^2 = c^3, \quad ii)\ a^2 + b^2 = 2c^3, \quad iii)\ a^2 + 2b^2 = 3c^3, \quad iv)\ 3b^2 - a^2 = 2c^3,$$

$$v)\ 3b^2 - 2a^2 = c^3, \quad vi)\ a^2 + b^2 = 2c^2, \quad vii)\ 2a^2 + b^2 = 3c^2, \quad viii)\ a^2 + 3b^2 = c^2$$

in integers a, b and c with $\gcd(a,b,c) = 1$ are given by the following parametrizations:

i)	$a = \pm(x^3 + 6xy^2)$	*or*	$a = \pm(x^3 + 6x^2y + 6xy^2 + 4y^3)$
	$b = \pm(3x^2y + 2y^3)$		$b = \pm(x^3 + 3x^2y + 6xy^2 + 2y^3)$
ii)	$a = \pm(x^3 - 3x^2y - 3xy^2 + y^3)$		
	$b = \pm(x^3 + 3x^2y - 3xy^2 - y^3)$		
iii)	$a = \pm(x^3 - 6x^2y - 6xy^2 + 4y^3)$		
	$b = \pm(x^3 + 3x^2y - 6xy^2 - 2y^3)$		
iv)	$a = \pm(x^3 + 9x^2y + 9xy^2 + 9y^3)$	*or*	$a = \pm(5x^3 + 27x^2y + 45xy^2 + 27y^3)$
	$b = \pm(x^3 + 3x^2y + 9xy^2 + 3y^3)$		$b = \pm(3x^3 + 15x^2y + 27xy^2 + 15y^3)$
v)	$a = \pm(x^3 + 9x^2y + 18xy^2 + 18y^3)$	*or*	$a = \pm(11x^3 + 81x^2y + 198xy^2 + 162y^3)$
	$b = \pm(x^3 + 6x^2y + 18xy^2 + 12y^3)$		$b = \pm(9x^3 + 66x^2y + 162xy^2 + 132y^3)$
vi)	$a = \pm(x^2 - 2xy - y^2)$		
	$b = \pm(x^2 + 2xy - y^2)$		
vii)	$a = \pm(x^2 + 2xy - 2y^2)$		
	$b = \pm(x^2 - 4xy - 2y^2)$		
viii)	$a = \pm(x^2 - 3y^2)/2$		
	$b = \pm xy$		

Here x and y are coprime integers and the $\pm$ signs can be chosen independently.

Proof. The statement can be proved via factorizing the expressions in the appropriate number fields. More precisely, we have to work in the rings of integers of the following fields: $\mathbb{Q}(\sqrt{-2}), \mathbb{Q}(i), \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{6})$. Note that the class number is one in all of these fields. As the method of the proof of the separate cases are rather similar, we give it only in two characteristic instances, namely for the cases i) and vii).

i) In $\mathbb{Z}[\sqrt{2}]$ we have

$$(a + \sqrt{2}b)(a - \sqrt{2}b) = (-c)^3.$$

Using $\gcd(a, b) = 1$, a simple calculation gives that

$$\gcd(a + \sqrt{2}b, a - \sqrt{2}b) \mid 2\sqrt{2}$$

in $\mathbb{Z}[\sqrt{2}]$. Moreover, $1 + \sqrt{2}$ is a fundamental unit of $\mathbb{Z}[\sqrt{2}]$, and the only roots of unity are ± 1, which are perfect cubes. Hence we have

$$a + \sqrt{2}b = (1 + \sqrt{2})^{\alpha}(\sqrt{2})^{\beta}(x + \sqrt{2}y)^3, \tag{7.1}$$

where $\alpha \in \{-1, 0, 1\}$, $\beta \in \{0, 1, 2\}$ and x, y are some rational integers. By taking norms, we immediately obtain that $\beta = 0$. If $\alpha = 0$, then expanding the right hand side of (7.1) we get

$$a = x^3 + 6xy^2, \quad b = 3x^2y + 2y^3.$$

Otherwise, when $\alpha = \pm 1$ then (1) yields

$$a = x^3 \pm 6x^2y + 6xy^2 \pm 4y^3, \quad b = \pm x^3 + 3x^2y \pm 6xy^2 + 2y^3.$$

In both cases, substituting $-x$ and $-y$ for x and y, respectively, we obtain the parametrizations given in the statement. Furthermore, observe that the coprimality of a and b implies $\gcd(x, y) = 1$.

vii) By factorizing in $\mathbb{Z}[\sqrt{-2}]$ we obtain

$$(b + \sqrt{-2}a)(b - \sqrt{-2}a) = 3c^2.$$

Again, $\gcd(a, b) = 1$ implies that

$$\gcd(b + \sqrt{-2}a, b - \sqrt{-2}a) \mid 2\sqrt{-2}$$

in $\mathbb{Z}[\sqrt{-2}]$. Note that $\mathbb{Z}[\sqrt{-2}]$ has no other units than ± 1. Since $2 = -(\sqrt{-2})^2$, we can write

$$b + \sqrt{-2}a = (-1)^{\alpha}(1 + \sqrt{-2})^{\beta}(1 - \sqrt{-2})^{\gamma}(\sqrt{-2})^{\delta}(x + \sqrt{-2}y)^2, \tag{2}$$

where $\alpha, \beta, \gamma, \delta \in \{0, 1\}$ and x, y are some rational integers. By taking norms, we immediately get that $\delta = 0$ and $\beta + \gamma = 1$. In these cases, by expanding the right hand side of (2) we obtain (choosing the $\pm$ signs appropriately) that

$$a = \pm(\pm x^2 + 2xy \mp y^2), \quad b = \pm(x^2 \mp 4xy - 2y^2).$$

Substituting $-x$ and $-y$ in places of x and y, respectively, we get the parametrizations indicated in the statement. Again, $\gcd(a, b) = 1$ gives $\gcd(x, y) = 1$. □

7.3 Proofs of the Theorems

Note that Theorem 1 directly follows from Theorem B and Theorem 2. Hence we begin with the proof of the latter statement.

Proof of Theorem 2. Since an arithmetic progression of length $k > 5$ contains an arithmetic progression of length 5, we only have to consider the cases $k = 5, 4$ and 3. The condition that $2 \leq l_i \leq L$ leaves only finitely many possibilities for the exponent vector $\underline{l} = (l_0, \ldots, l_{k-1})$. Therefore, it suffices to prove the finiteness for a given exponent vector $\underline{l}$.

Note that if $h_i = \eta_i x_i^{l_i}$ for some $\eta_i \in \mathbb{Z}_S^*$, then without loss of generality, η_i can be taken to be l_i-th power free. This means that, given $\underline{l}$, we only need to consider finitely many vectors $\underline{\eta} = (\eta_0, \ldots, \eta_{k-1})$. Hence, we only need to prove the theorem for $k = 3, 4, 5$, and $\underline{l}$ and $\underline{\eta}$ fixed. Note that if $\gcd(h_0, h_1) \leq D$, then certainly $\gcd(x_i, x_j) \leq D$. We enlarge S with all primes up to D.

We write $n = h_1 - h_0$ for the increment of the arithmetic progression. With $k, \underline{l}, \underline{\eta}$ fixed, the theorem will be proved if we show that the following system of equations has only finitely many solutions:

(a) $\eta_i x_i^{l_i} - \eta_j x_j^{l_j} = (i - j)n$ for all $0 \leq i < j \leq k - 1$.

(b) $(x_0, \ldots, x_{k-1}) \in \mathbb{Z}^k$ with $\gcd(x_0, x_1) \leq D$.

Hence, we need to solve

$$(j - m)\eta_i x_i^{l_i} + (m - i)\eta_j x_j^{l_j} + (i - j)\eta_m x_m^{l_m} = 0 \text{ for all } 0 \leq m, i, j \leq k - 1.$$

For $m = 0, i = 1$, we obtain that each of our solutions would give rise to a solution to

$$j\eta_1 x_1^{l_1} - \eta_j x_j^{l_j} + (1 - j)\eta_0 x_0^{l_0} = 0. \tag{7.2}$$

By applying Theorem A we see that such solutions give rise to K_j-rational points on some algebraic curve C_j over some number field K_j. Furthermore, putting

$$u = \frac{\eta_1 x_1^{l_1}}{\eta_0 x_0^{l_0}},$$

we obtain that C_j is a Galois-cover of the u-line, with ramification indices l_0, l_1, l_j over $u = \infty, 0, j/(j-1)$ respectively and unramified elsewhere.

If $k = 3$, we recover the approach of Darmon and Granville. Theorem A immediately implies that if $1/l_0 + 1/l_1 + 1/l_2 < 1$ then C_2 has genus larger than 1 and thus (by Faltings) has only finitely many rational points. This establishes the desired finiteness result.

If $k = 4$, we are interested in solutions to (7.2) for $j = 2, 3$ simultaneously. Let M be a number field containing both K_2 and K_3. Then the solutions we are interested in, correspond to M-rational points on C_2 and C_3 that give rise to the same value of u, i.e., we want the rational points on the fibre product $C_2 \times_u C_3$. This fibre product is again Galois and has ramification indices at least l_0, l_1, l_2, l_3 over $u = \infty, 0, 2, \frac{3}{2}$, respectively. Since $C_2 \times_u C_3$ is Galois over the u-line, all its connected components have the same genus and degree, say, d. Writing g for the genus of this component, the Riemann-Hurwitz formula gives us

$$2g - 2 \geq d \left(2 - \frac{1}{l_0} - \frac{1}{l_1} - \frac{1}{l_2} - \frac{1}{l_3}\right).$$

Hence, we see that $g \leq 1$ only if $l_0 = l_1 = l_2 = l_3 = 2$. For other situations, we have $g \geq 2$, so $C_2 \times_u C_3$ has only finitely many M-rational points.

If $k = 5$, we argue similarly, but now we consider $C_2 \times_u C_3 \times_u C_4$, with ramification indices at least l_0, l_1, l_2, l_3, l_4 over $u = 0, \infty, 1, \frac{3}{2}, \frac{4}{3}$, respectively. Hence, we obtain

$$2g - 2 \geq d \left(3 - \frac{1}{l_0} - \frac{1}{l_1} - \frac{1}{l_2} - \frac{1}{l_3} - \frac{1}{l_4}\right),$$

so that $g \geq 2$ in all cases. □

Proof of Theorem 3. The proof involves some explicit computations that are too involved to do either by hand or reproduce here on paper. Since the computations are by now completely standard, we choose not to bore the reader with excessive details and only give a conceptual outline of the proof. For full details, we refer the reader to the electronic resource [1], where a full transcript of a session using the computer algebra system MAGMA [3] can be found. We are greatly indebted to all contributors to this system. Without their work, the computations sketched here would not at all have been trivial to complete.

It suffices to prove the assertion for $k = 4$. We divide the proof into several parts, according to the exponents of the powers in the arithmetic progression. If $(l_0, l_1, l_2, l_3) = (2, 2, 2, 2)$, $(3, 3, 3, 3)$, $(2, 3, 3, 3)$ or $(3, 3, 3, 2)$, then our statement follows from Theorems B and C. We handle the remaining cases by Chabauty's method. We start with those cases where the classical variant works. After that we consider the cases where we have to resort to considering some covers of elliptic curves.

The cases $(l_0, l_1, l_2, l_3) = (2, 2, 2, 3)$ and $(3, 2, 2, 2)$.

From the method of our proof it will be clear that by symmetry we may suppose $(l_0, l_1, l_2, l_3) = (2, 2, 2, 3)$. That is, the progression is of the form $x_0^2, x_1^2, x_2^2, x_3^3$. Applying part i) of our Lemma to the last three terms of the progression, we get that either

$$x_1 = \pm(x^3 + 6xy^2), \quad x_2 = \pm(3x^2y + 2y^3)$$

or

$$x_1 = \pm(x^3 + 6x^2y + 6xy^2 + 4y^3), \quad x_2 = \pm(x^3 + 3x^2y + 6xy^2 + 2y^3)$$

where x, y are some coprime integers in both cases.

In the first case by $x_0^2 = 2x_1^2 - x_2^2$ we get

$$x_0^2 = 2x^6 + 15x^4y^2 + 60x^2y^4 - 4y^6.$$

Observe that $x \neq 0$. By putting $Y = x_0/x^3$ and $X = y^2/x^2$ we obtain the elliptic equation

$$Y^2 = -4X^3 + 60X^2 + 15X + 2.$$

A straightforward calculation with MAGMA gives that the elliptic curve described by this equation has no affine rational points.

In the second case by the same assertion we obtain

$$x_0^2 = x^6 + 18x^5y + 75x^4y^2 + 120x^3y^3 + 120x^2y^4 + 72xy^5 + 28y^6.$$

If $y = 0$, then the coprimality of x and y yields $x = \pm 1$, and we get the trivial progression $1, 1, 1, 1$. So assume that $y \neq 0$ and let $Y = x_0/y^3$, $X = x/y$. By these substitutions we are led to the hyperelliptic (genus two) equation

$$\mathcal{C}_1 : Y^2 = X^6 + 18X^5 + 75X^4 + 120X^3 + 120X^2 + 72X + 28.$$

We show that $\mathcal{C}_1(\mathbb{Q})$ consists only of the two points on $\mathcal{C}_1$ above $X = \infty$, denoted by ∞^+ and ∞^-.

The order of $\mathcal{J}_{\text{tors}}(\mathbb{Q})$ (the torsion subgroup of the Mordell-Weil group $\mathcal{J}(\mathbb{Q})$ of the Jacobian of $\mathcal{C}_1$) is a divisor of $\gcd(\#\mathcal{J}(\mathbb{F}_5), \#\mathcal{J}(\mathbb{F}_7)) = \gcd(21, 52) = 1$. Therefore the torsion subgroup is trivial. Moreover, using the algorithm of M. Stoll [18] implemented in MAGMA we get that the rank of $\mathcal{J}(\mathbb{Q})$ is at most one. As the divisor $D = [\infty^+ - \infty^-]$ has infinite order, the rank is exactly one. Since the rank of $\mathcal{J}(\mathbb{Q})$ is less than the genus of $\mathcal{C}_1$, we can apply Chabauty's method [6] to obtain a bound for the number of rational points on $\mathcal{C}_1$. For applications of the method on related problems, we refer to [5], [11], [12], [16].

As the rank of $\mathcal{J}(\mathbb{Q})$ is one and the torsion is trivial, we have $\mathcal{J}(\mathbb{Q}) = \langle D_0 \rangle$ for some $D_0 \in \mathcal{J}(\mathbb{Q})$ of infinite order. A simple computation $\pmod{13}$ shows that $D \notin 5\mathcal{J}(\mathbb{Q})$, and a similar computation $\pmod{139}$ yields that $D \notin 29\mathcal{J}(\mathbb{Q})$. Hence $D = kD_0$ with $5 \nmid k$, $29 \nmid k$. The reduction of $\mathcal{C}_1$ modulo p is a curve of genus two for any prime $p \neq 2, 3$. We take $p = 29$. Using Chabauty's method as implemented in MAGMA by Stoll, we find that there are at most two rational points on $\mathcal{C}_1$. Therefore we conclude that $\mathcal{C}_1(\mathbb{Q}) = \{\infty^+, \infty^-\}$, which proves the theorem in this case.

The cases $(l_0, l_1, l_2, l_3) = (2, 2, 3, 2)$ and $(2, 3, 2, 2)$.

Again, by symmetry we may suppose that $(l_0, l_1, l_2, l_3) = (2, 2, 3, 2)$. Then the progression is given by $x_0^2, x_1^2, x_2^3, x_3^2$. Now from part iii) of our Lemma, applied to the terms with indices $0, 2, 3$ of the progression, we get

$$x_0 = \pm(x^3 - 6x^2y - 6xy^2 + 4y^3), \quad x_3 = \pm(x^3 + 3x^2y - 6xy^2 - 2y^3)$$

where x, y are some coprime integers. Using $x_1^2 = (2x_0^2 + x_3^2)/3$ we obtain

$$x_1^2 = x^6 - 6x^5y + 15x^4y^2 + 40x^3y^3 - 24xy^5 + 12y^6.$$

If $y = 0$, then in the same way as before we deduce that the only possibility is given by the progression $1, 1, 1, 1$. Otherwise, if $y \neq 0$, then write $Y = x_1/y^3$, $X = x/y$ to get the hyperelliptic (genus two) curve

$$\mathcal{C}_2 : Y^2 = X^6 - 6X^5 + 15X^4 + 40X^3 - 24X + 12.$$

By a calculation similar to that applied in the previous case (but now with $p = 11$ in place of $p = 29$) we get that $\mathcal{C}_2(\mathbb{Q})$ consists only of the points ∞^+ and ∞^-. Hence the statement is proved also in this case.

The cases $(l_0, l_1, l_2, l_3) = (3, 2, 3, 2)$ and $(2, 3, 2, 3)$.

As before, without loss of generality we may assume $(l_0, l_1, l_2, l_3) = (3, 2, 3, 2)$. Then the progression is given by $x_0^3, x_1^2, x_2^3, x_3^2$. We have

$$x_1^2 = \frac{x_0^3 + x_2^3}{2}, \quad x_3^2 = \frac{-x_0^3 + 3x_2^3}{2}. \tag{7.3}$$

We note that $x_2 = 0$ implies $x_1^2 = -x_3^2$, hence $x_1 = x_3 = 0$. So we may assume that $x_2 \neq 0$, whence we obtain from (7.3) that

$$\left(\frac{2x_1x_3}{x_2^3}\right)^2 = -\left(\frac{x_0}{x_2}\right)^6 + 2\left(\frac{x_0}{x_2}\right)^3 + 3.$$

Thus putting $Y = 2x_1x_3/x_2^3$ and $X = x_0/x_2$, it is sufficient to find all rational points on the hyperelliptic curve

$$\mathcal{C}_3 : Y^2 = -X^6 + 2X^3 + 3.$$

We show that $\mathcal{C}_3(\mathbb{Q}) = \{(-1, 0), (1, \pm 2)\}$.

Using MAGMA we obtain that the rank of the Jacobian $\mathcal{J}(\mathbb{Q})$ of $\mathcal{C}_3(\mathbb{Q})$ is at most one, and the torsion subgroup $\mathcal{J}_{\text{tors}}(\mathbb{Q})$ of $\mathcal{J}(\mathbb{Q})$ consists of the elements $\mathcal{O}$ and $[(\frac{1-\sqrt{3}i}{2}, 0) + (\frac{1+\sqrt{3}i}{2}, 0) - \infty^+ - \infty^-]$. As the divisor $D = [(-1, 0) + (1, -2) - \infty^+ - \infty^-]$ has infinite order, the rank of $\mathcal{J}(\mathbb{Q})$ is exactly one. The only Weierstrass point on $\mathcal{C}_3$ is $(-1, 0)$. We proceed as before, using the primes 7 and 11 in this case. We conclude that $(1, \pm 2)$ are the only non-Weierstrass points on $\mathcal{C}_3$. It is easy to check that these points give rise only to the trivial arithmetic progression, so our theorem is proved also in this case.

The case $(l_0, l_1, l_2, l_3) = (3, 2, 2, 3)$.

Now the arithmetic progression is given by $x_0^3, x_1^2, x_2^2, x_3^3$. A possible approach would be to follow a similar argument as in the previous case. That is, multiplying the formulas

$$x_1^2 = \frac{2x_0^3 + x_3^3}{3}, \quad x_2^2 = \frac{x_0^3 + 2x_3^3}{3}$$

we get

$$(3x_1x_2)^2 = 2x_0^6 + 5x_0^3x_3^3 + 2x_3^6.$$

If $x_3 = 0$ then $\gcd(x_2, x_3) = 1$ yields $x_1^2 = \pm 2$, a contradiction. So we may suppose that $x_3 \neq 0$, and we obtain

$$Y^2 = 2X^6 + 5X^3 + 2$$

with $X = x_0/x_3$ and $Y = 3x_1x_2/x_3^3$. However, a calculation with MAGMA gives that the rank of the Jacobian of the above hyperelliptic curve is two, hence we cannot apply the classical Chabauty argument in this case. So we follow a different method, which also makes it possible to exhibit an elliptic curve (over some number field) having non-trivial Tate-Shafarevich group.

For this purpose, observe that we have

$$(-x_0x_3)^3 = 2d^2 - (x_1x_2)^2,$$

where d denotes the increment of the progression. Using part i) of our Lemma we get that there are two possible parametrizations given by

$$x_1x_2 = \pm(x^3+6x^2y+6xy^2+4y^3),\ d = \pm(x^3+3x^2y+6xy^2+2y^3),\ x_0x_3 = -x^2+2y^2$$

or

$$x_1x_2 = \pm(x^3+6xy^2),\ d = \pm(3x^2y+2y^3),\ x_0x_3 = x^2-2y^2.$$

Therefore from $x_1^2+d=x_2^2$ either

$$x_1^4+dx_1^2-(x^3+6x^2y+6xy^2+4y^3)^2=0 \tag{7.4}$$

or

$$x_1^4+dx_1^2-(x^3+6xy^2)^2=0 \tag{7.5}$$

follows, respectively. In the first case, the left hand side of (7.4) can be considered as a polynomial of degree two in x_1^2. Hence its discriminant must be a perfect square in $\mathbb{Z}$, and we get the equation

$$5x^6+54x^5y+213x^4y^2+360x^3y^3+384x^2y^4+216xy^5+68y^6=z^2$$

in integers x, y, z. A simple calculation with MAGMA shows that the Jacobian of the corresponding hyperelliptic curve

$$Y^2 = 5X^6+54X^5+213X^4+360X^3+384X^2+216X+68$$

is of rank zero (anyway it has three torsion points), and there is no rational point on the curve at all. Hence in this case we are done. It is interesting to note, however, that this curve does have points everywhere locally. We really do need this global information on the rank of its Jacobian in order to decide it does not have any rational points.

In case of (7.5) by a similar argument we obtain that $d^2+4(x^3+6xy^2)^2=z^2$, whence

$$4x^6+57x^4y^2+156x^2y^4+4y^6=z^2$$

with certain integers x, y, z. Observe that $y=0$ yields a non-primitive solution. Hence after putting $Y=z/2y^3$ and $X=x/y$, we get that to solve the above equation it is sufficient to find all rational points on the curve

$$\mathcal{C}_4 : Y^2 = f(X) = X^6+(57/4)X^4+39X^2+1.$$

We show that the rational points on $\mathcal{C}_4$ all have $X\in\{0,\infty\}$.

A straightforward computation shows that the rank of the Jacobian $\mathcal{J}(\mathbb{Q})$ of $\mathcal{C}_4$ is two, so we cannot apply Chabauty's method as before (cf. also [5]). We use part of the 2-coverings of $\mathcal{C}_4$ following [4]. For details, see [1]. Let

$$K=\mathbb{Q}(\alpha)=\mathbb{Q}[X]/(X^3+(57/4)X^2+39X+1).$$

Over this field, we have

$$f(X) = Q(X)R(X) =$$
$$(X^2 - \alpha)(X^4 + (\alpha + 57/4)X^2 + \alpha^2 + (57/4)\alpha + 39).$$

One easily gets that $\mathrm{Res}(Q, R)$ is a unit outside

$$S = \{\text{places } \mathfrak{p} \text{ of } K \text{ dividing } 6 \text{ or } \infty\}$$

. Therefore, if $(X, Y) \in \mathcal{C}_4(\mathbb{Q})$ then we have

$$D_\delta : \quad (Y_1)^2 = \delta R(X)$$
$$L_\delta : \quad (Y_2)^2 = \delta Q(X)$$

for some $Y_1, Y_2 \in K$ and $\delta \in K^*$ representing some element of the finite group

$$K(S, 2) := \{[d] \in K^*/K^{*2} : 2 \mid \mathrm{ord}_{\mathfrak{p}}(d) \text{ for all places } \mathfrak{p} \notin S\}.$$

Furthermore, since $N_{K[X]/\mathbb{Q}[X]}(Q) = f$, we see that $N_{K/\mathbb{Q}}(\delta) \in \mathbb{Q}^{*2}$. Running through these finitely many candidates, we see that the only class for which D_δ has points locally at the places of K above 2 and ∞ is represented by $\delta = 1$. Over K, the curve D_1 is isomorphic to

$$E : v^2 = u^3 - \frac{4\alpha + 57}{2}u^2 - \frac{48\alpha^2 + 456\alpha - 753}{16}u,$$

where $X = v/(2u)$. This curve has full 2-torsion over K and a full 2-descent or any 2-isogeny descent gives a rank bound of two for $E(K)$. However, one of the isogenous curves,

$$E' : Y^2 = X^3 + (4\alpha + 57)X^2 + (16\alpha^2 + 228\alpha + 624)X$$

has $S^{(2)}(E'/K) \simeq \mathbb{Z}/2\mathbb{Z}$, which shows that $E'(K)$ is of rank zero, since E' has 4-torsion over K. This shows that E has non-trivial 2-torsion in its Tate-Shafarevich group and that $E(K)$ consists entirely of torsion. In fact,

$$E(K) = \{\infty, (0, 0), ((12\alpha^2 + 195\alpha + 858)/32, 0), ((-12\alpha^2 - 131\alpha + 54)/32, 0)\}.$$

It follows that

$$X(\mathcal{C}_4(\mathbb{Q})) \subset X(D_1(K)) = \{0, \infty\},$$

where $X(.)$ denotes the set of the X-coordinates of the appropriate points on the corresponding curve. This proves that for all the rational points on $\mathcal{C}_4$ we have $X \in \{0, \infty\}$, which implies the theorem also in this case.

The cases $(l_0, l_1, l_2, l_3) = (2, 2, 3, 3)$ and $(3, 3, 2, 2)$.

Again by symmetry, we may assume that $(l_0, l_1, l_2, l_3) = (2, 2, 3, 3)$. Then the progression is $x_0^2, x_1^2, x_2^3, x_3^3$, whence

$$x_1^2 = 2x_2^3 - x_3^3 \quad \text{and} \quad x_0^2 = 3x_2^3 - 2x_3^3.$$

If $x_3 = 0$ then the coprimality of x_2 and x_3 gives $x_1^2 = \pm 2$, which is a contradiction. Hence we may assume that $x_3 \neq 0$, and we get the equation

$$y^2 = F(x) = 6x^6 - 7x^3 + 2$$

with $x = x_2/x_3$, $y = x_0x_1/x_3^3$. Put $K = \mathbb{Q}(\alpha)$ with $\alpha = \sqrt[3]{2}$ and observe that we have the factorization $F(x) = G(x)H(x)$ over K where

$$G(x) = 3\alpha x^4 - 3x^3 - 2\alpha x + 2 \quad \text{and} \quad H(x) = \alpha^2 x^2 + \alpha x + 1.$$

A simple calculation by MAGMA gives that $\mathrm{Res}(G, H)$ is a unit outside the set $S = \{\text{places } \mathfrak{p} \text{ of } K \text{ dividing } 6 \text{ or } \infty\}$. Hence we can write

$$3\alpha x^4 - 3x^3 - 2\alpha x + 2 = \delta z^2$$

with some z from K and δ from the integers of K dividing 6. Moreover, observe that the norm of δ is a square in $\mathbb{Z}$. Using that $\alpha - 1$ is a fundamental unit of K, $2 = \alpha^3$ and $3 = (\alpha - 1)(\alpha + 1)^3$, local considerations show that we can only have solutions with $x \in \mathbb{Q}$ with both $G(x)$ and $H(x) \in K^{*2}$ if, up to squares, $\delta = \alpha - 1$. We consider

$$3\alpha x^4 - 3x^3 - 2\alpha x + 2 = (\alpha - 1)z^2$$

with $x \in \mathbb{Q}$ and $z \in K$. Now by the help of the point $(1, 1)$, we can transform this curve to Weierstrass form

$$E : X^3 + (-72\alpha^2 - 90\alpha - 108)X + (504\alpha^2 + 630\alpha + 798) = Y^2.$$

We have $E(K) \simeq \mathbb{Z}$ as an Abelian group and the point $(X, Y) = (-\alpha^2 - 1, 12\alpha^2 + 15\alpha + 19)$ is a non-trivial point on this curve. Again applying elliptic Chabauty with $p = 5$, we get that the only solutions of our original equation is $(x, z) = (1, 1)$. Hence the theorem follows also in this case.

The case $(l_0, l_1, l_2, l_3) = (2, 3, 3, 2)$.

Now we have a progression $x_0^2, x_1^3, x_2^3, x_3^2$, and we can write

$$x_0^2 = 2x_1^3 - x_2^3 \quad \text{and} \quad x_3^2 = -x_1^3 + 2x_2^3.$$

If $x_2 = 0$ then the coprimality of x_1 and x_2 gives $x_0^2 = \pm 2$, which is a contradiction. Hence we may assume that $x_2 \neq 0$, and we are led to the equation

$$y^2 = F(x) = -2x^6 + 5x^3 - 2$$

with $x = x_1/x_2$, $y = x_0x_3/x_2^3$. Now we have the factorization $F(x) = G(x)H(x)$ over $K = \mathbb{Q}(\alpha)$ with $\alpha = \sqrt[3]{2}$, where

$$G(x) = \alpha^2x^4 + (\alpha+2)x^3 + (\alpha^2+2\alpha+1)x^2 + (\alpha+2)x + \alpha^2$$

and

$$H(x) = -\alpha x^2 + (\alpha^2+1)x - \alpha.$$

One can easily verify that $\mathrm{Res}(G,H) = 1$. Thus we obtain

$$\alpha^2x^4 + (\alpha+2)x^3 + (\alpha^2+2\alpha+1)x^2 + (\alpha+2)x + \alpha^2 = \delta z^2$$

where $z \in K$ and δ is a unit of K. Moreover, as the norm of δ is a square in $\mathbb{Z}$, we get that, up to squares, $\delta = 1$ or $\alpha - 1$. The case when $\delta = 1$ yields the equation

$$\alpha^2x^4 + (\alpha+2)x^3 + (\alpha^2+2\alpha+1)x^2 + (\alpha+2)x + \alpha^2 = z^2$$

in $x \in \mathbb{Q}$ and $z \in K$. We can transform this equation to an elliptic one by the help of its point $(1, \alpha^2+\alpha+1)$. Then applying elliptic Chabauty, the procedure "Chabauty" of MAGMA with $p = 5$ in this case gives that this equation has four solutions with $x \in \mathbb{Q}$, namely $(x,z) = (0,1),(1,0),(\pm 1,1)$. Lifting these solutions to the original problem, our theorem follows also in this case.

When $\delta = \alpha - 1$, using $x = x_1/x_2$ we get the equation

$$\alpha^2x_1^4 + (\alpha+2)x_1^3x_2 + (\alpha^2+2\alpha+1)x_1^2x_2^2 + (\alpha+2)x_1x_2^3 + \alpha^2x_2^4 = (\alpha-1)\gamma^2$$

with some integer γ of K. Writing now γ in the form $\gamma = u + \alpha v + \alpha^2 w$ with some $u, v, w \in \mathbb{Z}$ and comparing the coefficients of 1 and α in the above equation, a simple calculation shows that $x_1^3x_2 + x_1^2x_2^2 + x_1x_2^3$ must be even. However, then $2 \mid x_1x_2$, and considering the progression $x_0^2, x_1^3, x_2^3, x_3^2$ modulo 4 we get a contradiction. Hence the theorem follows also in this case.

The case $(l_0,l_1,l_2,l_3) = (3,3,2,3)$ and $(3,2,3,3)$.

As previously, without loss of generality we may assume that $(l_0,l_1,l_2,l_3) = (3,3,2,3)$. Then the progression is of the form $x_0^3, x_1^3, x_2^2, x_3^3$. We note that using the cubes one would find $3x_1^3 = x_3^3 + 2x_0^3$ which leads to an elliptic curve. However, this elliptic curve has positive rank, hence this approach does not work.

So we use some other argument. We have $x_1^3 + x_3^3 = 2x_2^2$, whence

$$x_1 + x_3 = 2su^2, \quad x_1^2 - x_1x_3 + x_3^2 = sv^2,$$

where $u, v, s \in \mathbb{Z}$ with $s \mid 3$. By considerations modulo 3 we obtain that only $s = 1$ is possible. Hence $(2x_1 - x_3)^2 + 3x_3^2 = (2v)^2$ and from part viii) of our Lemma we get that

$$f(x, y) := 3x^6 + 18x^5y + 9x^4y^2 - 148x^3y^3 - 27x^2y^4 + 162xy^5 - 81y^6 = 2(\pm 4x_0)^3 \tag{7.6}$$

in coprime integers x, y.

Note that the equation $f(x, y) = 2z^3$ is invariant under the transformation $(x, y, z) \mapsto (-3y, x, -3z)$. The two obvious solutions $(x, y, z) = (1, -1, -4)$ and $(x, y, z) = (3, 1, 12)$ are interchanged by this involution.

We have the factorization $f(x, y) = g(x, y)h(x, y)$ with

$$g(x, y) = (\alpha^2 + 2\alpha + 1)x^3 + (-2\alpha^3 - \alpha^2 + 2\alpha + 1)x^2y +$$

$$(3\alpha^2 - 26\alpha - 13)xy^2 + (-6\alpha^3 - 3\alpha^2 + 6\alpha + 3)y^3$$

and

$$h(x, y) = (2\alpha^3 + 3\alpha^2 - 2\alpha + 9)x^3 + (12\alpha^3 + 17\alpha^2 - 10\alpha + 53)x^2y +$$

$$(6\alpha^3 + 9\alpha^2 - 6\alpha + 27)xy^2 + (-92\alpha^3 - 141\alpha^2 + 66\alpha - 401)y^3$$

over the number field $\mathbb{Q}(\alpha)$ defined by a root α of the polynomial $X^4 + 2X^3 + 4X + 2$.

Using the same reasoning as before, we have that a rational solution to $f(x, y) = 2z^3$ with x, y, z not all 0, yields a solution to the system of equations

$$g(x, y) = \delta(u_0 + u_1\alpha + u_2\alpha^2 + u_3\alpha^3)^3$$
$$h(x, y) = 2/\delta(v_0 + v_1\alpha + v_2\alpha^2 + v_3\alpha^3)^3$$

with $x, y, u_0, \ldots, v_3 \in \mathbb{Q}$ and where δ is a representative of an element of the finite group $K(S, 3)$, with $S = \{\text{places } \mathfrak{p} \text{ of } K \text{ dividing } 6 \text{ or } \infty\}$. For each δ, the equations above can be expressed as eight homogeneous equations of degree 3, describing some non-singular curve in $\mathbb{P}^8$ over $\mathbb{Q}$. The only values of δ for which this curve is locally solvable at 3 are

$$\delta_1 = (\alpha^3 + 2\alpha^2 - 2\alpha - 2)/2 \text{ and } \delta_2 = (\alpha^3 + 4\alpha^2 + 6\alpha + 2)/2.$$

These values correspond to the obvious solutions with $(x, y) = (1, -1)$ and $(x, y) = (3, 1)$ respectively.

We now determine the K-rational points on the curve

$$g(x, y) = \delta_1 z_1^3$$

with $x/y \in \mathbb{Q}$. Using the K-rational point $(x : y : z) = (1 : -1 : -2\alpha)$, we can see that this curve is isomorphic to the elliptic curve

$$E : Y^2 = X^3 - 48\alpha^3 + 33\alpha^2 + 480\alpha + 210.$$

Using a 2-descent we can verify that $E(K)$ has rank at most 3 and some further computations show that $E(K) \simeq \mathbb{Z}^3$, where the points with X-coordinates

$$\begin{aligned}&(-2\alpha^3 + 13\alpha^2 - 28\alpha + 44)/9,\\ &(16\alpha^3 + 52\alpha^2 + 14\alpha - 1)/9,\\ &(2\alpha^3 + 3\alpha^2 - 14\alpha - 6)/3\end{aligned}$$

generate a finite index subgroup with index prime to 6. The function x/y on the curve $g(x, y) = \delta_1 z_1^3$ yields a degree 3 function on E as well.

Using the Chabauty-method described in [4] and implemented in MAGMA 2.11 as Chabauty, using $p = 101$, we determine that the given point is in fact the only one with $x/y \in \mathbb{Q}$. For details, see [1].

For δ_2 we simply observe that using the involution $(x, y) \mapsto (-3y, x)$, we can reduce this case to the computations we have already done for δ_1.

We conclude that $(x, y) = (1, -1)$ and $(x, y) = (3, 1)$ give the only solutions to $f(x, y) = 2z^3$. These solutions correspond to the arithmetic progressions $(0, 1, 2, 3)$ (which up to powers of 2, 3 indeed consists of second and third powers), $(1, 1, 1, 1)$ and their $\mathbb{Z}^*_{\{2,3\}}$-equivalent counterparts.

□

7.4 Acknowledgement

The authors are grateful to the referee for his useful and helpful remarks.

Bibliography

[1] Transcript of computations. http://www.cecm.sfu.ca/∼nbruin/unlikepowers.

[2] M. A. Bennett, N. Bruin, K. Győry, and L. Hajdu. Powers from products of consecutive terms in arithmetic progression. *Proc. London Math. Soc. (3)*, 92(2):273–306, 2006.

[3] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[4] N. R. Bruin. *Chabauty methods and covering techniques applied to generalized Fermat equations*, volume 133 of *CWI Tract*. Stichting Mathematisch Centrum Centrum voor Wiskunde en Informatica, Amsterdam, 2002. Dissertation, University of Leiden, Leiden, 1999.

[5] J. W. S. Cassels and E. V. Flynn. *Prolegomena to a middlebrow arithmetic of curves of genus* 2, volume 230 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1996.

[6] C. Chabauty. Sur les points rationnels des courbes algébriques de genre supérieur à l'unité. *C. R. Acad. Sci. Paris*, 212:882–885, 1941.

[7] H. Darmon and A. Granville. On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$. *Bull. London Math. Soc.*, 27(6):513–543, 1995.

[8] H. Darmon and L. Merel. Winding quotients and some variants of Fermat's last theorem. *J. Reine Angew. Math.*, 490:81–100, 1997.

[9] L.E. Dickson. *History of the theory of numbers. Vol II: Diophantine analysis*. Chelsea Publishing Co., New York, 1966.

[10] G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.*, 73(3):349–366, 1983.

[11] E. V. Flynn. A flexible method for applying Chabauty's theorem. *Compositio Math.*, 105(1):79–94, 1997.

[12] E. V. Flynn, B. Poonen, and E. F. Schaefer. Cycles of quadratic polynomials and rational points on a genus-2 curve. *Duke Math. J.*, 90(3):435–463, 1997.

[13] L. Hajdu. Perfect powers in arithmetic progression. A note on the inhomogeneous case. *Acta Arith.*, 113(4):343–349, 2004. Dedicated to Robert Tijdeman on the occasion of his 60th birthday.

[14] L. J. Mordell. *Diophantine equations*. Pure and Applied Mathematics, Vol. 30. Academic Press, London, 1969.

[15] I. Pink and Sz. Tengely. Full powers in arithmetic progressions. *Publ. Math. Debrecen*, 57(3-4):535–545, 2000.

[16] B. Poonen. The classification of rational preperiodic points of quadratic polynomials over Q: a refined conjecture. *Math. Z.*, 228(1):11–29, 1998.

[17] T. N. Shorey. Powers in arithmetic progression. In *A panorama of number theory or the view from Baker's garden (Zürich, 1999)*, pages 325–336. Cambridge Univ. Press, Cambridge, 2002.

[18] Michael Stoll. Implementing 2-descent for Jacobians of hyperelliptic curves. *Acta Arith.*, 98(3):245–277, 2001.

[19] Sz. Tengely. *Effective Methods for Diophantine Equations*. PhD thesis, Leiden Univ., Leiden, The Netherlands, 2005.

[20] R. Tijdeman. Diophantine equations and Diophantine approximations. In *Number theory and applications (Banff, AB, 1988)*, volume 265 of *NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci.*, pages 215–243. Kluwer Acad. Publ., Dordrecht, 1989.

8

Arithmetic progressions of squares, cubes and n-th powers

*H*ajdu, L. and Tengely, Sz.,
Funct. Approx. Comment. Math. **41** (2009), 129–138.

Abstract

In this paper we continue the investigations about unlike powers in arithmetic progression. We provide sharp upper bounds for the length of primitive non-constant arithmetic progressions consisting of squares/cubes and n-th powers.

8.1 Introduction

It was claimed by Fermat and proved by Euler (see [10] pp. 440 and 635) that four distinct squares cannot form an arithmetic progression. It was shown by Darmon and Merel [9] that, apart from trivial cases, there do not exist three-term arithmetic progressions consisting of n-th powers, provided $n \geq 3$. An arithmetic progression $a_1, a_2, \ldots, a_t$ of integers is called primitive if $\gcd(a_1, a_2) = 1$. A recent result of Hajdu [11] implies that if

$$x_1^{l_1}, \ldots, x_t^{l_t} \tag{8.1}$$

is a primitive arithmetic progression in $\mathbb{Z}$ with $2 \leq l_i \leq L$ $(i = 1, \ldots, t)$, then t is bounded by some constant $c(L)$ depending only on L. Note that $c(L)$ is effective, but it is not explicitly given in [11], and it is a very rapidly growing function of L.

An the other hand, it is known (see e.g. [12], [8], [14] and the references given there) that there exist exponents $l_1, l_2, l_3 \geq 2$ for which there are infinitely many

primitive arithmetic progressions of the form (8.1). In this case the exponents in question satisfy the condition

$$\frac{1}{l_1} + \frac{1}{l_2} + \frac{1}{l_3} \geq 1.$$

In [5] Bruin, Győry, Hajdu and Tengely among other things proved that for any $t \geq 4$ and $L \geq 3$ there are only finitely many primitive arithmetic progressions of the form (8.1) with $2 \leq l_i \leq L$ $(i = 1, \ldots, t)$. Furthermore, they showed that in case of $L = 3$ we have $x_i = \pm 1$ for all $i = 1, \ldots, t$.

The purpose of the present paper is to give a good, explicit upper bound for the length t of the progression (8.1) under certain restrictions. More precisely, we consider the cases when the set of exponents is given by $\{2, n\}$, $\{2, 5\}$ and $\{3, n\}$, and (excluding the trivial cases) we show that the length of the progression is at most six, four and four, respectively.

8.2 Results

Theorem 8.2.1. *Let n be a prime and $x_1^{l_1}, \ldots, x_t^{l_t}$ be a primitive non-constant arithmetic progression in $\mathbb{Z}$ with $l_i \in \{2, n\}$ $(i = 1, \ldots, t)$. Then we have $t \leq 6$. Further, if $t = 6$ then*

$$(l_1, l_2, l_3, l_4, l_5, l_6) = (2, n, n, 2, 2, 2), (2, 2, 2, n, n, 2).$$

In the special case $n = 5$ we are able to prove a sharper result.

Theorem 8.2.2. *Let $x_1^{l_1}, \ldots, x_t^{l_t}$ be a primitive non-constant arithmetic progression in $\mathbb{Z}$ with $l_i \in \{2, 5\}$ $(i = 1, \ldots, t)$. Then we have $t \leq 4$. Further, if $t = 4$ then*

$$(l_1, l_2, l_3, l_4) = (2, 2, 2, 5), (5, 2, 2, 2).$$

Theorem 8.2.3. *Let n be a prime and $x_1^{l_1}, \ldots, x_t^{l_t}$ be a primitive non-constant arithmetic progression in $\mathbb{Z}$ with $l_i \in \{3, n\}$ $(i = 1, \ldots, t)$. Then we have $t \leq 4$. Further, if $t = 4$ then*

$$(l_1, l_2, l_3, l_4) = (3, 3, n, n), (n, n, 3, 3), (3, n, n, 3), (n, 3, 3, n).$$

Note that Theorems 8.2.2 and 8.2.3 are almost best possible. This is demonstrated by the primitive non-constant progression $-1, 0, 1$. (In fact one can easily give infinitely many examples of arithmetic progressions of length three, consisting of squares and fifth powers.)

We also remark that by a previously mentioned result from [5], the number of progressions of length at least four is finite in each case occurring in the above theorems.

8.3 Proofs of Theorems 8.2.1 and 8.2.3

In the proof of these theorems we need several results about ternary equations of signatures $(n, n, 2)$ and $(n, n, 3)$, respectively. We start this section with summarizing these statements. The first three lemmas are known from the literature, while the fourth one is new.

Lemma 8.3.1. *Let n be a prime. Then the Diophantine equations*

$$X^n + Y^n = 2Z^2 \quad (n \geq 5),$$
$$X^n + Y^n = 3Z^2 \quad (n \geq 5),$$
$$X^n + 4Y^n = 3Z^2 \quad (n \geq 7)$$

have no solutions in nonzero pairwise coprime integers (X, Y, Z) with $XY \neq \pm 1$.

Proof. The statement follows from results of Bennett and Skinner [1], and Bruin [4]. □

Lemma 8.3.2. *Let $n \geq 5$ be a prime. Then the Diophantine equation*

$$X^n + Y^n = 2Z^3$$

has no solutions in coprime nonzero integers X, Y, Z with $XYZ \neq \pm 1$.

Proof. The result is due to Bennett, Vatsal and Yazdani [2]. □

Lemma 8.3.3. *Let $n \geq 3$ be a prime. Then the Diophantine equation*

$$X^n + Y^n = 2Z^n$$

has no solutions in coprime nonzero integers X, Y, Z with $XYZ \neq \pm 1$.

Proof. The result is due to Darmon and Merel [9]. □

Lemma 8.3.4. *Let $n \geq 3$ be a prime. Then the Diophantine equation*

$$X^3 + Y^3 = 2Z^n$$

has no solutions in coprime nonzero integers X, Y, Z with $XYZ \neq \pm 1$ and $3 \nmid Z$.

Proof. First note that in case of $n = 3$ the statement follows from Lemma 8.3.3. Let $n \geq 5$, and assume to the contrary that (X, Y, Z) is a solution to the equation with $\gcd(X, Y, Z) = 1$, $XYZ \neq \pm 1$ and $3 \nmid Z$. Note that the coprimality of X, Y, Z shows that XY is odd. We have

$$(X + Y)(X^2 - XY + Y^2) = 2Z^n.$$

Our assumptions imply that $\gcd(X+Y, X^2-XY+Y^2) \mid 3$, whence $2 \nmid XY$ and $3 \nmid Z$ yield that

$$X+Y = 2U^n \text{ and } X^2-XY+Y^2 = V^n$$

hold, where $U, V \in \mathbb{Z}$ with $\gcd(U,V) = 1$. Combining these equations we get

$$f(X) := 3X^2 - 6U^nX + 4U^{2n} - V^n = 0.$$

Clearly, the discriminant of f has to be a square in $\mathbb{Z}$, which leads to an equality of the form

$$V^n - U^{2n} = 3W^2$$

with some $W \in \mathbb{Z}$. However, this is impossible by Lemma 8.3.1. □

Now we are ready to prove our Theorems 8.2.1 and 8.2.3.

Proof of Theorem 8.2.1. Suppose that we have an arithmetic progression (8.1) of the desired form, with $t = 6$. In view of a result from [5] about the case $n = 3$ and Theorem 8.2.2, without loss of generality we may assume that $n \geq 7$.

First note that the already mentioned classical result of Fermat and Euler implies that we cannot have four consecutive squares in our progression. Further, observe that Lemmas 8.3.1 and 8.3.3 imply that we cannot have three consecutive terms with exponents $(n,2,n)$ and (n,n,n), respectively, and further that $(l_1,l_3,l_5) = (n,2,n)$, (n,n,n) are also impossible.

If $(l_1,l_2,l_3,l_4,l_5) = (n,2,2,n,2)$ or $(2,n,2,2,n)$, then we have

$$4x_4^n - x_1^n = 3x_5^2 \quad \text{or} \quad 4x_2^n - x_5^n = 3x_1^2,$$

respectively, both equations yielding a contradiction by Lemma 8.3.1.

To handle the remaining cases, let d denote the common difference of the progression. Let $(l_1,l_2,l_3,l_4,l_5) = (2,2,n,2,2)$. Then (as clearly $x_1 \neq 0$) we have

$$(1+X)(1+3X)(1+4X) = Y^2$$

where $X = d/x_1$ and $Y = x_2x_4x_5/x_1$. However, a simple calculation with Magma [3] shows that the rank of this elliptic curve is zero, and it has exactly eight torsion points. However, none of these torsion points gives rise to any appropriate arithmetic progression.

When $(l_1,l_2,l_3,l_4,l_5,l_6) = (2,2,n,n,2,2)$, then in a similar manner we get

$$(1+X)(1+4X)(1+5X) = Y^2$$

with $X = d/x_1$ and $Y = x_2x_5x_6/x_1$, and just as above, we get a contradiction.

In view of the above considerations, a simple case-by-case analysis yields that the only remaining possibilities are the ones listed in the theorem. Hence to complete the proof we need only to show that the possible six-term progressions cannot be extended to seven-term ones. Using symmetry it is sufficient to deal with the case given by

$$(l_1, l_2, l_3, l_4, l_5, l_6) = (2, n, n, 2, 2, 2).$$

However, one can easily verify that all the possible extensions lead to a case treated before, and the theorem follows. □

Proof of Theorem 8.2.3. In view of Lemma 8.3.3 and the previously mentioned result from [5] we may suppose that $n \geq 5$. Assume that we have an arithmetic progression of the indicated form, with $t = 4$. By the help of Lemmas 8.3.2 and 8.3.3 we get that there cannot be three consecutive terms with exponents $(n, 3, n)$, and $(3, 3, 3)$ or (n, n, n), respectively. Hence a simple calculation yields that the only possibilities (except for the ones listed in the theorem) are given by

$$(l_1, l_2, l_3, l_4) = (3, n, 3, 3), (3, 3, n, 3).$$

Then Lemma 8.3.4 yields that $3 \mid x_2$ and $3 \mid x_3$, respectively. However, looking at the progressions modulo 9 and using that $x^3 \equiv 0, \pm 1 \pmod 9$ for all $x \in \mathbb{Z}$ we get a contradiction with the primitivity condition in both cases.

Finally, one can easily check that the extensions of the four-term sequences corresponding to the exponents listed in the statement to five-term ones, yield cases which have been treated already. Hence the proof of the theorem is complete. □

8.4 Proof of Theorem 8.2.2

To prove this theorem we need some lemmas, obtained by the help of elliptic Chabauty's method. To prove the lemmas we used the program package Magma [3]. The transcripts of computer calculations can be downloaded from the URL-s www.math.klte.hu/∼tengely/Lemma4.1 and www.math.klte.hu/∼tengely/Lemma4.2, respectively.

Lemma 8.4.1. *Let $\alpha = \sqrt[5]{2}$ and put $K = \mathbb{Q}(\alpha)$. Then the equations*

$$C_1 : \quad \alpha^4 X^4 + \alpha^3 X^3 + \alpha^2 X^2 + \alpha X + 1 = (\alpha - 1) Y^2 \tag{8.2}$$

and

$$C_2 : \quad \alpha^4 X^4 - \alpha^3 X^3 + \alpha^2 X^2 - \alpha X + 1 = (\alpha^4 - \alpha^3 + \alpha^2 - \alpha + 1) Y^2 \tag{8.3}$$

in $X \in \mathbb{Q}$, $Y \in K$ have the only solutions

$$(X, Y) = (1, \pm(\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1)), \ \left(-\frac{1}{3}, \pm\frac{3\alpha^4 + 5\alpha^3 - \alpha^2 + 3\alpha + 5}{9}\right)$$

and $(X, Y) = (1, \pm 1)$, respectively.

Proof. Using the so-called elliptic Chabauty's method (see [6], [7]) we determine all points on the above curves for which X is rational. The algorithm is implemented by N. Bruin in Magma, so here we indicate the main steps only, the actual computations can be carried out by Magma. We can transform C_1 to Weierstrass form

$$E_1 : \quad x^3 - (\alpha^2 + 1)x^2 - (\alpha^4 + 4\alpha^3 - 4\alpha - 5)x + (2\alpha^4 - \alpha^3 - 4\alpha^2 - \alpha + 4) = y^2.$$

The torsion subgroup of E_1 consists of two elements. Moreover, the rank of E_1 is two, which is less than the degree of the number field K. Applying elliptic Chabauty (the procedure "Chabauty" of Magma) with $p = 3$, we obtain that $X \in \{1, -1/3\}$.

In case of C_2 a similar procedure works. Now the corresponding elliptic curve E_2 is of rank two. Applying elliptic Chabauty this time with $p = 7$, we get that $X = 1$, and the lemma follows. □

Lemma 8.4.2. *Let $\beta = (1 + \sqrt{5})/2$ and put $L = \mathbb{Q}(\beta)$. Then the only solutions to the equation*

$$C_3 : \quad X^4 + (8\beta - 12)X^3 + (16\beta - 30)X^2 + (8\beta - 12)X + 1 = Y^2 \qquad (8.4)$$

in $X \in \mathbb{Q}$, $Y \in L$ are $(X, Y) = (0, \pm 1)$.

Proof. The proof is similar to that of Lemma 8.4.1. We can transform C_3 to Weierstrass form

$$E_3 : \quad x^3 - (\beta - 1)x^2 - (\beta + 2)x + 2\beta = y^2.$$

The torsion group of E_3 consists of four points and $(x, y) = (\beta - 1, 1)$ is a point of infinite order. Applying elliptic Chabauty with $p = 13$, we obtain that $(X, Y) = (0, \pm 1)$ are the only affine points on C_3 with rational first coordinates. □

Now we can give the

Proof of Theorem 8.2.2. Suppose that we have a four-term progression of the desired form. Then by Lemmas 8.3.1, 8.3.3 and the result of Fermat and Euler

we obtain that all the possibilities (except for the ones given in the statement) are

$$(l_1, l_2, l_3, l_4) = (2,2,5,5), (5,5,2,2), (2,5,5,2),$$
$$(5,2,2,5), (2,2,5,2), (2,5,2,2).$$

We show that these possibilities cannot occur. Observe that by symmetry we may assume that we have

$$(l_1, l_2, l_3, l_4) = (2,2,5,5), (2,5,5,2), (5,2,2,5), (2,2,5,2).$$

In the first two cases the progression has a sub-progression of the shape a^2, b^5, c^5. Note that here $\gcd(b,c) = 1$ and bc is odd. Indeed, if c would be even then we would get $4 \mid a^2, c^5$, whence it would follow that b is even - a contradiction. Taking into consideration the fourth term of the original progression, a similar argument shows that b is also odd. Using this subprogression we obtain the equality $2b^5 - c^5 = a^2$. Putting $\alpha = \sqrt[5]{2}$ we get the factorization

$$(\alpha b - c)(\alpha^4 b^4 + \alpha^3 b^3 c + \alpha^2 b^2 c^2 + \alpha b c^3 + c^4) = a^2 \tag{8.5}$$

in $K = \mathbb{Q}(\alpha)$. Note that the class number of K is one, $\alpha^4, \alpha^3, \alpha^2, \alpha, 1$ is an integral basis of K, $\varepsilon_1 = \alpha - 1$, $\varepsilon_2 = \alpha^3 + \alpha + 1$ provides a system of fundamental units of K with $N_{K/\mathbb{Q}}(\varepsilon_1) = N_{K/\mathbb{Q}}(\varepsilon_2) = 1$, and the only roots of unity in K are given by ± 1. A simple calculation shows that

$$D := \gcd(\alpha b - c, \alpha^4 b^4 + \alpha^3 b^3 c + \alpha^2 b^2 c^2 + \alpha b c^3 + c^4) \mid \gcd(\alpha b - c, 5\alpha b c^3)$$

in the ring of integers O_K of K. Using $\gcd(b,c) = 1$ and $2 \nmid c$ in $\mathbb{Z}$, we get $D \mid 5$ in O_K. Using e.g. Magma, one can easily check that $5 = (3\alpha^4 + 4\alpha^3 - \alpha^2 - 6\alpha - 3)(\alpha^2 + 1)^5$, where $3\alpha^4 + 4\alpha^3 - \alpha^2 - 6\alpha - 3$ is a unit in K, and $\alpha^2 + 1$ is a prime in O_K with $N_{K/\mathbb{Q}}(\alpha^2 + 1) = 5$. By the help of these information, we obtain that

$$\alpha b - c = (-1)^{k_0} (\alpha - 1)^{k_1} (\alpha^3 + \alpha + 1)^{k_2} (\alpha^2 + 1)^{k_3} z^2$$

with $k_0, k_1, k_2, k_3 \in \{0, 1\}$ and $z \in O_K$. Taking the norms of both sides of the above equation, we get that $k_0 = k_3 = 0$. Further, if $(k_1, k_2) = (0,0), (1,1), (0,1)$ then putting $z = z_4\alpha^4 + z_3\alpha^3 + z_2\alpha^2 + z_1\alpha + z_0$ with $z_i \in \mathbb{Z}$ $(i = 0, \ldots, 4)$ and expanding the right hand side of the above equation, we get $2 \mid b$, which is a contradiction. (Note that to check this assertion, in case of $(k_1, k_2) = (0,1)$ one can also use that the coefficients of α^2 and α^3 on the left hand side are zero.) Hence we may conclude that $(k_1, k_2) = (1,0)$. Thus using (8.5) we get that

$$\alpha^4 b^4 + \alpha^3 b^3 c + \alpha^2 b^2 c^2 + \alpha b c^3 + c^4 = (\alpha - 1) y^2$$

with some $y \in O_K$. Hence after dividing this equation by c^4 (which cannot be zero), we get (8.2), and then a contradiction by Lemma 8.4.1. Hence the first two possibilities for (l_1, l_2, l_3, l_4) are excluded.

Assume next that $(l_1, l_2, l_3, l_4) = (5, 2, 2, 5)$. Then we have $2x_1^5 + x_4^5 = 3x_2^2$. Using the notation of the previous paragraph, we can factorize this equation over K to obtain

$$(\alpha x_1 + x_4)(\alpha^4 x_1^4 - \alpha^3 x_1^3 x_4 + \alpha^2 x_1^2 x_4^2 - \alpha x_1 x_4^3 + x_4^4) = 3x_2^2. \tag{8.6}$$

Observe that the primitivity condition implies that $\gcd(x_1, x_4) = 1$, and $2 \nmid x_1 x_4$. Hence in the same manner as before we obtain that the greatest common divisor of the terms on the left hand side of (8.6) divides 5 in O_K. Further, a simple calculation e.g. with Magma yields that $3 = (\alpha + 1)(\alpha^4 - \alpha^3 + \alpha^2 - \alpha + 1)$, where $\alpha + 1$ and $\alpha^4 - \alpha^3 + \alpha^2 - \alpha + 1$ are primes in O_K with $N_{K/\mathbb{Q}}(\alpha + 1) = 3$ and $N_{K/\mathbb{Q}}(\alpha^4 - \alpha^3 + \alpha^2 - \alpha + 1) = 81$, respectively. Using these information we can write

$$\alpha x_1 + x_4 = (-1)^{k_0}(\alpha - 1)^{k_1}(\alpha^3 + \alpha + 1)^{k_2}(\alpha + 1)^{k_3}(\alpha^4 - \alpha^3 + \alpha^2 - \alpha + 1)^{k_4} z^2$$

with $k_0, k_1, k_2, k_3, k_4 \in \{0, 1\}$ and $z \in O_K$. Taking the norms of both sides of the above equation, we get that $k_0 = 0$ and $k_3 = 1$. Observe that $k_4 = 1$ would imply $3 \mid x_1, x_4$. This is a contradiction, whence we conclude $k_4 = 0$. Expanding the above equation as previously, we get that if $(k_1, k_2) = (0, 1), (1, 0), (1, 1)$ then x_1 is even, which is a contradiction again. (To deduce this assertion, when $(k_1, k_2) = (1, 1)$ we make use of the fact that the coefficients of α^3 and α^2 vanish on the left hand side.) So we have $(k_1, k_2) = (0, 0)$, which by the help of (8.6) implies

$$\alpha^4 x_1^4 - \alpha^3 x_1^3 x_4 + \alpha^2 x_1^2 x_4^2 - \alpha x_1 x_4^3 + x_4^4 = (\alpha^4 - \alpha^3 + \alpha^2 - \alpha + 1) y^2$$

with some $y \in O_K$. However, after dividing this equation by x_1^4 (which is certainly non-zero), we get (8.3), and then a contradiction by Lemma 8.4.1.

Finally, suppose that $(l_1, l_2, l_3, l_4) = (2, 2, 5, 2)$. Using the identity $x_2^2 + x_4^2 = 2x_3^5$, e.g. by the help of a result of Pink and Tengely [13] we obtain

$$x_2 = u^5 - 5u^4 v - 10u^3 v^2 + 10u^2 v^3 + 5uv^4 - v^5$$

and

$$x_4 = u^5 + 5u^4 v - 10u^3 v^2 - 10u^2 v^3 + 5uv^4 + v^5$$

with some coprime integers u, v. Then the identity $3x_2^2 - x_4^2 = 2x_1^2$ implies

$$(u^2 - 4uv + v^2) f(u, v) = x_1^2 \tag{8.7}$$

where

$$f(u,v) = u^8 - 16u^7v - 60u^6v^2 + 16u^5v^3 + 134u^4v^4 + \\ +16u^3v^5 - 60u^2v^6 - 16uv^7 + v^8.$$

A simple calculation shows that the common prime divisors of the terms at the left hand side belong to the set $\{2,5\}$. However, $2 \mid x_1$ would imply $4 \mid x_1^2, x_3^5$, which would violate the primitivity condition. Further, if $5 \mid x_1$ then looking at the progression modulo 5 and using that by the primitivity condition $x_2^2 \equiv x_4^2 \equiv \pm 1 \pmod 5$ should be valid, we get a contradiction. Hence the above two terms are coprime, which yields that

$$f(u,v) = w^2$$

holds with some $w \in \mathbb{Z}$. (Note that a simple consideration modulo 4 shows that $f(u,v) = -w^2$ is impossible.) Let $\beta = (1+\sqrt{5})/2$, and put $L = \mathbb{Q}(\beta)$. As is well-known, the class number of L is one, $\beta, 1$ is an integral basis of L, β is a fundamental unit of L with $N_{L/\mathbb{Q}}(\beta) = 1$, and the only roots of unity in L are given by ± 1. A simple calculation shows that

$$f(u,v) = g(u,v)h(u,v)$$

with

$$g(u,v) = u^4 + (8\beta - 12)u^3v + (16\beta - 30)u^2v^2 + (8\beta - 12)uv^3 + v^4$$

and

$$h(u,v) = u^4 + (-8\beta - 4)u^3v + (-16\beta - 14)u^2v^2 + (-8\beta - 4)uv^3 + v^4.$$

Further, $\gcd(6, x_1) = 1$ by the primitivity of the progression, and one can easily check modulo 5 that $5 \mid x_1$ is also impossible. Hence we conclude that $g(u,v)$ and $h(u,v)$ are coprime in the ring O_L of integers of L. Thus we have

$$g(u,v) = (-1)^{k_0}\beta^{k_1}z^2$$

with some $k_0, k_1 \in \{0,1\}$ and $z \in O_L$. Note that as $2 \nmid x_1$, equation (8.7) implies that exactly one of u, v is even. Hence a simple calculation modulo 4 shows that the only possibility for the exponents in the previous equation is $k_0 = k_1 = 0$. However, then after dividing the equation with v^4 (which cannot be zero), we get (8.4), and then a contradiction by Lemma 8.4.2.

There remains to show that a four-term progression with exponents $(l_1, l_2, l_3, l_4) = (2,2,2,5)$ or $(5,2,2,2)$ cannot be extended to a five-term one. By symmetry it is sufficient to deal with the first case. If we insert a square or

a fifth power after the progression, then the last four terms yield a progression which has been already excluded. Writing a fifth power, say x_0^5 in front of the progression would give rise to the identity $x_0^5 + x_4^5 = 2x_2^2$, which leads to a contradiction by Lemma 8.3.1. Finally, putting a square in front of the progression is impossible by the already mentioned result of Fermat and Euler. □

8.5 Acknowledgement

The research of the first author was supported in part by the National Office for Research and Technology. The authors are grateful to the referee for his helpful remarks.

Bibliography

[1] M.A. Bennett and C.M. Skinner. Ternary Diophantine equations via Galois representations and modular forms. *Canad. J. Math.*, 56(1):23–54, 2004.

[2] M.A. Bennett, V. Vatsal, and S. Yazdani. Ternary Diophantine equations of signature $(p, p, 3)$. *Compos. Math.*, 140(6):1399–1416, 2004.

[3] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[4] N. Bruin. Some ternary Diophantine equations of signature $(n, n, 2)$. In *Discovering mathematics with Magma*, volume 19 of *Algorithms Comput. Math.*, pages 63–91. Springer, Berlin, 2006.

[5] N. Bruin, K. Győry, L. Hajdu, and Sz. Tengely. Arithmetic progressions consisting of unlike powers. *Indag. Math. (N.S.)*, 17:539–555, 2006.

[6] N. R. Bruin. *Chabauty methods and covering techniques applied to generalized Fermat equations*, volume 133 of *CWI Tract*. Stichting Mathematisch Centrum Centrum voor Wiskunde en Informatica, Amsterdam, 2002. Dissertation, University of Leiden, Leiden, 1999.

[7] Nils Bruin. Chabauty methods using elliptic curves. *J. Reine Angew. Math.*, 562:27–49, 2003.

[8] H. Darmon and A. Granville. On the equations $z^m = f(x, y)$ and $Ax^p + By^q = Cz^r$. *Bull. London Math. Soc.*, 27:513–543, 1995.

[9] H. Darmon and L. Merel. Winding quotients and some variants of Fermat's last theorem. *J. Reine Angew. Math.*, 490:81–100, 1997.

[10] L.E. Dickson. *History of the theory of numbers. Vol II: Diophantine analysis*. Chelsea Publishing Co., New York, 1966.

[11] L. Hajdu. Perfect powers in arithmetic progression. A note on the inhomogeneous case. *Acta Arith.*, 113(4):343–349, 2004. Dedicated to Robert Tijdeman on the occasion of his 60th birthday.

[12] L. J. Mordell. *Diophantine equations*. Pure and Applied Mathematics, Vol. 30. Academic Press, London, 1969.

[13] I. Pink and Sz. Tengely. Full powers in arithmetic progressions. *Publ. Math. Debrecen*, 57(3-4):535–545, 2000.

[14] Sz. Tengely. On the Diophantine equation $x^2 + a^2 = 2y^p$. *Indag. Math. (N.S.)*, 15(2):291–304, 2004.

9

Triangles with two integral sides

*T*engely, Sz.,
Annales Mathematicae et Informaticae **34** (2007), 89–95.

Abstract

We study some Diophantine problems related to triangles with two given integral sides. We solve two problems posed by Zoltán Bertalan and we also provide some generalization.

9.1 Introduction

There are many Diophantine problems arising from studying certain properties of triangles. Most people know the theorem on the lengths of sides of right angled triangles named after Pythagoras. That is $a^2 + b^2 = c^2$.

An integer $n \geq 1$ is called congruent if it is the area of a right triangle with rational sides. Using tools from modern arithmetic theory of elliptic curves and modular forms Tunnell [10] found necessary condition for n to be a congruent number. Suppose that n is a square-free positive integer which is a congruent number.

(a) If n is odd, then the number of integer triples (x, y, z) satisfying the equation $n = 2x^2 + y^2 + 8z^2$ is just twice the number of integer triples (x, y, z) satisfying $n = 2x^2 + y^2 + 32z^2$.

(b) If n is even, then the number of integer triples (x, y, z) satisfying the equation $\frac{n}{2} = 4x^2 + y^2 + 8z^2$ is just twice the number of integer triples (x, y, z) satisfying $\frac{n}{2} = 4x^2 + y^2 + 32z^2$.

A Heronian triangle is a triangle having the property that the lengths of its sides and its area are positive integers. There are several open problems concerning the existence of Heronian triangles with certain properties. It is

not known whether there exist Heronian triangles having the property that the lengths of all their medians are positive integers [6], and it is not known whether there exist Heronian triangles having the property that the lengths of all their sides are Fibonacci numbers [7]. Gaál, Járási and Luca [5] proved that there are only finitely many Heronian triangles whose sides $a, b, c \in S$ and are reduced, that is $\gcd(a, b, c) = 1$, where S denotes the set of integers divisible only by some fixed primes.

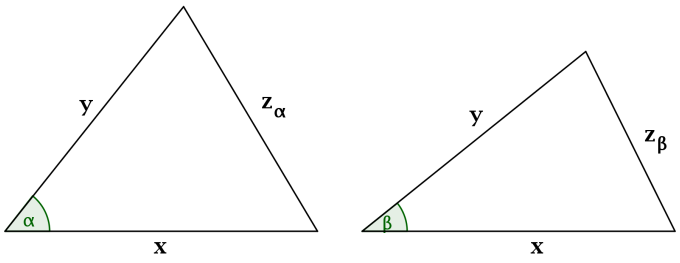
Petulante and Kaja [9] gave arguments for parametrizing all integer-sided triangles that contain a specified angle with rational cosine. It is equivalent to determining a rational parametrization of the conic $u^2 - 2\alpha uv + v^2 = 1$, where α is the rational cosine.

The present paper is motivated by the following two problems due to Zoltán Bertalan.

(i) How to choose x and y such that the distances of the clock hands at 2 o'clock and 3 o'clock are integers?

(ii) How to choose x and y such that the distances of the clock hands at 2 o'clock and 4 o'clock are integers?

We generalize and reformulate the above questions as follows. For given $0 < \alpha, \beta < \pi$ we are looking for pairs of triangles in which the length of the sides (z_α, z_β) opposite the angles α, β are from some given number field $\mathbb{Q}(\theta)$ and the length of the other two sides (x, y) are rational integers. Let $\varphi_1 = \cos(\alpha)$ and $\varphi_2 = \cos(\beta)$.



By means of the law of cosine we obtain the following systems of equations

$$x^2 - 2\varphi_1 xy + y^2 = z_\alpha^2,$$
$$x^2 - 2\varphi_2 xy + y^2 = z_\beta^2,$$

After multiplying these equations and dividing by y^4 we get

$$\mathcal{C}_{\alpha,\beta} : X^4 - 2(\varphi_1 + \varphi_2)X^3 + (4\varphi_1\varphi_2 + 2)X^2 - 2(\varphi_1 + \varphi_2)X + 1 = Y^2,$$

where $X = x/y$ and $Y = z_\alpha z_\beta / y^2$. Suppose $\varphi_1, \varphi_2 \in \mathbb{Q}(\theta)$ for some algebraic number θ. Clearly, the hyperelliptic curve $\mathcal{C}_{\alpha,\beta}$ has a rational point $(X, Y) = (0, 1)$, so it is isomorphic to an elliptic curve $\mathcal{E}_{\alpha,\beta}$. The rational points of an elliptic curve form a finitely generated group. We are looking for points on $\mathcal{E}_{\alpha,\beta}$ for which the first coordinate of its preimage is rational. If $\mathcal{E}_{\alpha,\beta}$ is defined over $\mathbb{Q}$ and the rank is 0, then there are only finitely many solutions, if the rank is greater than 0, then there are infinitely many solutions. If the elliptic curve $\mathcal{E}_{\alpha,\beta}$ is defined over some number field of degree at least two, then one can apply the so-called elliptic Chabauty method (see [2, 3] and the references given there) to determine all solutions with the required property.

9.2 Curves defined over $\mathbb{Q}$

9.2.1 $(\alpha, \beta) = (\pi/3, \pi/2)$

The system of equations in this case is

$$x^2 - xy + y^2 = z_{\pi/3}^2,$$
$$x^2 + y^2 = z_{\pi/2}^2.$$

The related hyperelliptic curve is $\mathcal{C}_{\pi/3,\pi/2}$.

Theorem 9.2.1. *There are infinitely many rational points on $\mathcal{C}_{\pi/3,\pi/2}$.*

Proof. In this case the free rank is 1, as it is given in Cremona's table of elliptic curves [4] (curve 192A1). Therefore there are infinitely many rational points on $\mathcal{C}_{\pi/3,\pi/2}$. □

Corollary. *Problem (i) has infinitely many solutions.*

Few solutions are given in the following table.

x	y	$z_{\pi/3}$	$z_{\pi/2}$
8	15	13	17
1768	2415	2993	3637
10130640	8109409	9286489	12976609
498993199440	136318711969	517278459169	579309170089

9.2.2 $(\alpha, \beta) = (\pi/2, 2\pi/3)$

The system of equations in this case is

$$x^2 + y^2 = z_{\pi/2}^2,$$
$$x^2 + xy + y^2 = z_{2\pi/3}^2.$$

The hyperelliptic curve $\mathcal{C}_{\pi/2,2\pi/3}$ is isomorphic to $\mathcal{C}_{\pi/3,\pi/2}$, therefore there are infinitely many rational points on $\mathcal{C}_{\pi/2,2\pi/3}$.

9.2.3 $(\alpha, \beta) = (\pi/3, 2\pi/3)$

We have

$$x^2 - xy + y^2 = z_{\pi/3}^2,$$
$$x^2 + xy + y^2 = z_{2\pi/3}^2.$$

After multiplying these equations we get

$$x^4 + x^2y^2 + y^4 = (z_{\pi/3}z_{2\pi/3})^2. \tag{9.1}$$

Theorem 9.2.2. *If* (x, y) *is a solution of* (9.1) *such that* $\gcd(x, y) = 1$, *then* $xy = 0$.

Proof. See [8] at page 19. □

Corollary. *Problem (ii) has no solution.*

MAGMA code clock.m:

```
clock:=function(a,b,p)

P1:=ProjectiveSpace(Rationals(),1);
K1:=Parent(a);
K2:=Parent(b);

if IsIntegral(a) then K1:=RationalField(); end if;
if IsIntegral(b) then K2:=RationalField(); end if;

    if Degree(K1)*Degree(K2) eq 1 then K:=RationalField();
    else
        if Degree(K1) gt 1 and Degree(K2) gt 1 then
        K:=CompositeFields(K1,K2)[1];
```

```
        else
            if Degree(K1) eq 1 then K:=K2; else K:=K1;
            end if;
        end if;
    end if;

P<X>:=PolynomialRing(K);
print K;
ka:=K!a;
kb:=K!b;
C:=HyperellipticCurve(X^4-2*(ka+kb)*X^3+
(4*ka*kb+2)*X^2-2*(ka+kb)*X+1);
umap:=map<C->P1|[C.1,C.3]>;
pt:=C![0,1];
E,CtoE:=EllipticCurve(C,pt);
Em,EtoEm:=MinimalModel(E);
U:=Expand(Inverse(CtoE*EtoEm)*umap);
RB:=RankBound(Em);
print Em,RB;

if RB ne 0 then
    success,G,mwmap:=PseudoMordellWeilGroup(Em);
    NC,VC,RC,CC:=Chabauty(mwmap,U,p);
    print success,NC,#VC,RC;
    if NC eq #VC then print
       {EvaluateByPowerSeries(U,mwmap(gp)): gp in VC};
       forall{pr: pr in PrimeDivisors(RC)|
              IsPSaturated(mwmap,pr)};
    end if;
else
success,G,mwmap:=PseudoMordellWeilGroup(Em);
print #G;
print #TorsionSubgroup(Em);
print {EvaluateByPowerSeries(U,mwmap(gp)): gp in G};
end if;
return K,C;
end function;
```

In the following sections we use the so-called elliptic Chabauty's method

(see [2], [3]) to determine all points on the curves $\mathcal{C}_{\alpha,\beta}$ for which X is rational. The algorithm is implemented by N. Bruin in MAGMA [1], so here we indicate the main steps only, the actual computations can be carried out by MAGMA. The MAGMA code clock.m which were used is given below. It requires three inputs, a, b as members of some number fields and p a prime number.

9.3 Curves defined over $\mathbb{Q}(\sqrt{2})$

9.3.1 $(\alpha, \beta) = (\pi/4, \pi/2)$

The hyperelliptic curve $\mathcal{C}_{\pi/4,\pi/2}$ is isomorphic to

$$\mathcal{E}_{\pi/4,\pi/2}: \quad v^2 = u^3 - u^2 - 3u - 1.$$

The rank of $\mathcal{E}_{\pi/4,\pi/2}$ over $\mathbb{Q}(\sqrt{2})$ is 1, which is less than the degree of $\mathbb{Q}(\sqrt{2})$. Applying elliptic Chabauty (the procedure "Chabauty" of MAGMA) with $p = 7$, we obtain that $(X, Y) = (0, \pm 1)$ are the only affine points on $\mathcal{C}_{\pi/4,\pi/2}$ with rational first coordinates. Since $X = x/y$ we get that there does not exist appropriate triangles in this case.

9.3.2 $(\alpha, \beta) = (\pi/4, \pi/3)$

The hyperelliptic curve $\mathcal{C}_{\pi/4,\pi/3}$ is isomorphic to

$$\mathcal{E}_{\pi/4,\pi/3}: \quad v^2 = u^3 + (\sqrt{2} - 1)u^2 - 2u - \sqrt{2}.$$

The rank of $\mathcal{E}_{\pi/4,\pi/2}$ over $\mathbb{Q}(\sqrt{2})$ is 1 and applying elliptic Chabauty's method again with $p = 7$, we obtain that $(X, Y) = (0, \pm 1)$ are the only affine points on $\mathcal{C}_{\pi/4,\pi/3}$ with rational first coordinates. As in the previous case we obtain that there does not exist triangles satisfying the appropriate conditions.

9.4 Curves defined over $\mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{5})$

In the following tables we summarize some details of the computations, that is the pair (α, β), the equations of the elliptic curves $\mathcal{E}_{\alpha,\beta}$, the rank of the Mordell-Weil group of these curves over the appropriate number field ($\mathbb{Q}(\sqrt{3})$ or $\mathbb{Q}(\sqrt{5})$), the rational first coordinates of the affine points and the primes we used.

(α, β)	$\mathcal{E}_{\alpha,\beta}$	Rank	X	p
$(\pi/6, \pi/2)$	$v^2 = u^3 - u^2 - 2u$	1	$\{0, \pm 1\}$	5
$(\pi/6, \pi/3)$	$v^2 = u^3 + (\sqrt{3} - 1)u^2 - u + (-\sqrt{3} + 1)$	1	$\{0\}$	7
$(\pi/5, \pi/2)$	$v^2 = u^3 - u^2 + 1/2(\sqrt{5} - 7)u + 1/2(\sqrt{5} - 3)$	1	$\{0\}$	13
$(\pi/5, \pi/3)$	$v^2 = u^3 + 1/2(\sqrt{5} - 1)u^2 + 1/2(\sqrt{5} - 5)u - 1$	1	$\{0, 1\}$	13
$(\pi/5, 2\pi/5)$	$v^2 = u^3 - 2u - 1$	1	$\{0\}$	7
$(\pi/5, 4\pi/5)$	$v^2 = u^3 + 1/2(-\sqrt{5} + 1)u^2 - 4u + (2\sqrt{5} - 2)$	0	$\{0\}$	-

In case of $(\alpha, \beta) = (\pi/5, \pi/3)$ we get the following family of triangles given by the length of the sides

$$(x, y, z_\alpha) = \left(t, t, \frac{-1+\sqrt{5}}{2} t \right) \text{ and } (x, y, z_\beta) = (t, t, t),$$

where $t \in \mathbb{N}$.

Bibliography

[1] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[2] N. R. Bruin. *Chabauty methods and covering techniques applied to generalized Fermat equations*, volume 133 of *CWI Tract*. Stichting Mathematisch Centrum Centrum voor Wiskunde en Informatica, Amsterdam, 2002. Dissertation, University of Leiden, Leiden, 1999.

[3] Nils Bruin. Chabauty methods using elliptic curves. *J. Reine Angew. Math.*, 562:27–49, 2003.

[4] J. E. Cremona. *Algorithms for modular elliptic curves*. Cambridge University Press, New York, NY, USA, 1992.

[5] I. Gaál, I. Járási, and F. Luca. A remark on prime divisors of lengths of sides of Heron triangles. *Experiment. Math.*, 12(3):303–310, 2003.

[6] Richard K. Guy. *Unsolved problems in number theory*. Problem Books in Mathematics. Springer-Verlag, New York, second edition, 1994. Unsolved Problems in Intuitive Mathematics, I.

[7] H. Harborth, A. Kemnitz, and N. Robbins. Non-existence of Fibonacci triangles. *Congr. Numer.*, 114:29–31, 1996. Twenty-fifth Manitoba Conference on Combinatorial Mathematics and Computing (Winnipeg, MB, 1995).

[8] L. J. Mordell. *Diophantine equations*. Pure and Applied Mathematics, Vol. 30. Academic Press, London, 1969.

[9] N. Petulante and I. Kaja. How to generate all integral triangles containing a given angle. *Int. J. Math. Math. Sci.*, 24(8):569–572, 2000.

[10] J. B. Tunnell. A classical Diophantine problem and modular forms of weight 3/2. *Invent. Math.*, 72(2):323–334, 1983.

10

Integral Points on Hyperelliptic Curves

*B*ugeaud, Y., Mignotte, M., Siksek, S., Stoll, M. and Tengely, Sz.,
Algebra & Number Theory **2** (2008), 859–885.

Abstract

Let $C : Y^2 = a_n X^n + \cdots + a_0$ be a hyperelliptic curve with the a_i rational integers, $n \geq 5$, and the polynomial on the right irreducible. Let J be its Jacobian. We give a completely explicit upper bound for the integral points on the model C, provided we know at least one rational point on C and a Mordell–Weil basis for $J(\mathbb{Q})$. We also explain a powerful refinement of the Mordell–Weil sieve which, combined with the upper bound, is capable of determining all the integral points. Our method is illustrated by determining the integral points on the genus 2 hyperelliptic models $Y^2 - Y = X^5 - X$ and $\binom{Y}{2} = \binom{X}{5}$.

10.1 Introduction

Consider the hyperelliptic curve with affine model

$$C : Y^2 = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0, \tag{10.1}$$

with $a_0, \ldots, a_n$ rational integers, $a_n \neq 0$, $n \geq 5$, and the polynomial on the right irreducible. Let $H = \max\{|a_0|, \ldots, |a_n|\}$. In one of the earliest applications of his theory of lower bounds for linear forms in logarithms, Baker [2] showed that any integral point (X, Y) on this affine model satisfies

$$\max(|X|, |Y|) \leq \exp\exp\exp\{(n^{10n} H)^{n^2}\}.$$

Such bounds have been improved considerably by many authors, including Sprindžuk [44], Brindza [6], Schmidt [40], Poulakis [38], Bilu [3], Bugeaud [14]

and Voutier [52]. Despite the improvements, the bounds remain astronomical and often involve inexplicit constants.

In this paper we explain a new method for explicitly computing the integral points on affine models of hyperelliptic curves (10.1). The method falls into two distinct steps:

(i) We give a completely explicit upper bound for the size of integral solutions of (10.1). This upper bound combines the many refinements found in the papers of Voutier, Bugeaud, etc., together with Matveev's bounds for linear forms in logarithms [31], and a method for bounding the regulators based on a theorem of Landau [29].

(ii) The bounds obtained in (i), whilst substantially better than bounds given by earlier authors, are still astronomical. We explain a powerful variant of the Mordell–Weil sieve which, combined with the bound obtained in (i), is capable of showing that the known solutions to (10.1) are the only ones.

Step (i) requires two assumptions:

(a) We assume that we know at least one rational point P_0 on C.

(b) Let J be the Jacobian of C. We assume that a Mordell–Weil basis for $J(\mathbb{Q})$ is known.

For step (ii) we need assumptions (a), (b) and also:

(c) We assume that the canonical height $\hat{h} : J(\mathbb{Q}) \to \mathbb{R}$ is explicitly computable and that we have explicit bounds for the difference

$$\mu_1 \leq h(D) - \hat{h}(D) \leq \mu_1' \tag{10.2}$$

where h is an appropriately normalized logarithmic height on J that allows us to enumerate points P in $J(\mathbb{Q})$ with $h(P) \leq B$ for a given bound B.

Assumptions (a)–(c) deserve a comment or two. For many families of curves of higher genus, practical descent strategies are available for estimating the rank of the Mordell–Weil group; see for example [17], [37], [39] and [46]. To provably determine the Mordell–Weil group one however needs bounds for the difference between the logarithmic and canonical heights. For Jacobians of curves of genus 2 such bounds have been determined by Stoll [45], [47], building on previous work of Flynn and Smart [25]. At present, no such bounds have been determined for Jacobians of curves of genus ≥ 3, although work on this is in progress. The assumption about the knowledge of a rational point is a common sense

assumption that brings some simplifications to our method, although the method can be modified to cope with the situation where no rational point is known. However, if a search on a curve of genus ≥ 2 reveals no rational points, it is probable that there are none, and the methods of [12], [13], [8] are likely to succeed in proving this.

We illustrate the practicality of our approach by proving the following results.

Theorem 10.1.1. *The only integral solutions to the equation*

$$Y^2 - Y = X^5 - X \tag{10.3}$$

are

$$(X, Y) = (-1, 0),\ (-1, 1),\ (0, 0),\ (0, 1),\ (1, 0),\ (1, 1),\ (2, -5),\\ (2, 6),\ (3, -15),\ (3, 16),\ (30, -4929),\ (30, 4930).$$

Theorem 10.1.2. *The only integral solutions to the equation*

$$\binom{Y}{2} = \binom{X}{5} \tag{10.4}$$

are

$$(X, Y) = (0, 0),\ (0, 1),\ (1, 0),\ (1, 1),\ (2, 0),\ (2, 1),\ (3, 0),\ (3, 1),\ (4, 0),\ (4, 1),\\ (5, -1),\ (5, 2),\ (6, -3),\ (6, 4),\ (7, -6),\ (7, 7),\ (15, -77),\\ (15, 78),\ (19, -152),\ (19, 153).$$

Equations (10.3) and (10.4) are of historical interest and Section 10.2 gives a brief outline of their history. For now we merely mention that these two equations are the first two problems on a list of 22 unsolved Diophantine problems [20], compiled by Evertse and Tijdeman following a recent workshop on Diophantine equations at Leiden.

To appreciate why the innocent-looking equations (10.3) and (10.4) have resisted previous attempts, let us briefly survey the available methods which apply to hyperelliptic curves and then briefly explain why they fail in these cases. To determine the integral points on the affine model C given by an equation (10.1) there are four available methods:

(I) The first is Chabauty's elegant method which in fact determines all rational points on C in many cases, provided the rank of the Mordell–Weil group of its Jacobian is strictly less than the genus g; see for example [23], [53]. Chabauty's method fails if the rank of the Mordell–Weil group exceeds the genus.

(II) A second method is to use coverings, often combined with a version of Chabauty called 'Elliptic Curve Chabauty'. See [9], [10], [26], [27]. This approach often requires computations of Mordell–Weil groups over number fields (and does fail if the rank of the Mordell–Weil groups is too large).

(III) A third method is to combine Baker's approach through S-units with the LLL algorithm to obtain all the solutions provided that certain relevant unit groups and class groups can be computed; for a modern treatment, see [4] or [43, Section XIV.4]. This strategy often fails in practice as the number fields involved have very high degree.

(IV) A fourth approach is to apply Skolem's method to the S-unit equations (see [43, Section III.2]). This needs the same expensive information as the third method.

The Jacobians of the curves given by (10.3) and (10.4) respectively have ranks 3 and 6 and so Chabauty's method fails. To employ Elliptic Curve Chabauty would require the computation of Mordell–Weil groups of elliptic curves without rational 2-torsion over number fields of degree 5 (which does not seem practical at present). To apply the S-unit approach (with either LLL or Skolem) requires the computations of the unit groups and class groups of several number fields of degree 40; a computation that seems completely impractical at present.

Our paper is arranged as follows. Section 10.2 gives a brief history of equations (10.3) and (10.4). In Section 10.3 we show, after appropriate scaling, that an integral point (x, y) satisfies $x-\alpha = \kappa\xi^2$ where α is some fixed algebraic integer, $\xi \in \mathbb{Q}(\alpha)$, and κ is an algebraic integer belonging to a finite computable set. In Section 10.9 we give bounds for the size of solutions $x \in \mathbb{Z}$ to an equation of the form $x-\alpha = \kappa\xi^2$ where α and κ are fixed algebraic integers. Thus, in effect, we obtain bounds for the size of solutions integral points on our affine model for (10.1). Sections 10.4–10.8 are preparation for Section 10.9: in particular Section 10.4 is concerned with heights; Section 10.5 explains how a theorem of Landau can be used to bound the regulators of number fields; Section 10.6 collects and refines various results on appropriate choices of systems of fundamental units; Section 10.7 is devoted to Matveev's bounds for linear forms in logarithms; in Section 10.8 we use Matveev's bounds and the results of previous sections to prove a bound on the size of solutions of unit equations; in Section 10.9 we deduce the bounds for x alluded to above from the bounds for solutions of unit equations. Despite our best efforts, the bounds obtained for x are still so large that no naive search up to those bounds is conceivable. Over the next three sections 10.10, 10.11, 10.12 we explain how to sieve effectively up

to these bounds using the Mordell–Weil group of the Jacobian. In particular, Section 10.11 gives a powerful refinement of the Mordell–Weil sieve ([12], [8]) which we expect to have applications elsewhere. Finally, in Section 10.13 we apply the method of this paper to prove Theorems 10.1.1 and 10.1.2.

We are grateful to the referee and editors for many useful comments, and to Mr. Homero Gallegos–Ruiz for spotting many misprints.

10.2 History of Equations (10.3) and (10.4)

The equation (10.3) is a special case of the family of Diophantine equations

$$Y^p - Y = X^q - X, \qquad 2 \le p < q. \tag{10.5}$$

This family has previously been studied by Fielder and Alford [21] and by Mignotte and Pethő [32]. The (genus 1) case $p = 2$, $q = 3$ was solved by Mordell [33] who showed that the only solutions in this case are

$$(X, Y) = (0,0), (0,1), (\pm 1, 0), (\pm 1, 1), (2,3), (2,-2), (6,15), (6,-14).$$

Fielder and Alford presented the following list of solutions with $X, Y > 1$:

$$(p, q, X, Y) = (2,3,2,3), (2,3,6,15), (2,5,2,6), (2,5,3,16),$$
$$(2,5,30,4930), (2,7,5,280), (2,13,2,91), (3,7,3,13).$$

Mignotte and Pethő proved that for given p and q with $2 \le p < q$, the Diophantine equation (10.5) has only a finite number of integral solutions. Assuming the abc-conjecture, they showed that equation (10.5) has only finitely many solutions with $X, Y > 1$.

If $p = 2$, $q > 2$ and y is a prime power, then Mignotte and Pethő found all solutions of the equation and these are all in Fielder and Alford's list.

Equation (10.4) is a special case of the Diophantine equation

$$\binom{n}{k} = \binom{m}{l}, \tag{10.6}$$

in unknowns k, l, m, n. This is usually considered with the restrictions $2 \le k \le n/2$, and $2 \le l \le m/2$. The only known solutions (with these restrictions) are the following

$$\binom{16}{2} = \binom{10}{3}, \quad \binom{56}{2} = \binom{22}{3}, \quad \binom{120}{2} = \binom{36}{3},$$
$$\binom{21}{2} = \binom{10}{4}, \quad \binom{153}{2} = \binom{19}{5}, \quad \binom{78}{2} = \binom{15}{5} = \binom{14}{6},$$
$$\binom{221}{2} = \binom{17}{8}, \quad \binom{F_{2i+2}F_{2i+3}}{F_{2i}F_{2i+3}} = \binom{F_{2i+2}F_{2i+3}-1}{F_{2i}F_{2i+3}+1} \text{ for } i = 1, 2, \ldots,$$

where F_n is the nth Fibonacci number. It is known that there are no other non-trivial solutions with $\binom{n}{k} \leq 10^{30}$ or $n \leq 1000$; see [19]. The infinite family of solutions was found by Lind [30] and Singmaster [42].

Equation (10.6) has been completely solved for pairs

$$(k,l) = (2,3),\ (2,4),\ (2,6),\ (2,8),\ (3,4),\ (3,6),\ (4,6),\ (4,8).$$

These are the cases when one can easily reduce the equation to the determination of solutions of a number of Thue equations or elliptic Diophantine equations. In 1966, Avanesov [1] found all solutions of equation (10.6) with $(k,l) = (2,3)$. De Weger [18] and independently Pintér [35] solved the equation with $(k,l) = (2,4)$. The case $(k,l) = (3,4)$ reduces to the equation $Y(Y+1) = X(X+1)(X+2)$ which was solved by Mordell [33]. The remaining pairs $(2,6), (2,8), (3,6), (4,6), (4,8)$ were treated by Stroeker and de Weger [50], using linear forms in elliptic logarithms.

There are also some general finiteness results related to equation (10.6). In 1988, Kiss [28] proved that if $k = 2$ and l is a given odd prime, then the equation has only finitely many positive integral solutions. Using Baker's method, Brindza [7] showed that equation (10.6) with $k = 2$ and $l \geq 3$ has only finitely many positive integral solutions.

10.3 Descent

Consider the integral points on the affine model of the hyperelliptic curve (10.1). If the polynomial on the right-hand side is reducible then the obvious factorisation argument reduces the problem of determining the integral points on (10.1) to determining those on simpler hyperelliptic curves, or on genus 1 curves. The integral points on a genus 1 curve can be determined by highly successful algorithms (e.g. [43], [49]) based on LLL and David's bound for linear forms in elliptic logarithms.

We therefore suppose henceforth that the polynomial on the right-hand side of (10.1) is irreducible; this is certainly the most difficult case. By appropriate scaling, one transforms the problem of integral points on (10.1) to integral points on a model of the form

$$ay^2 = x^n + b_{n-1}x^{n-1} + \cdots + b_0, \tag{10.7}$$

where a and the b_i are integers, with $a \neq 0$. We shall work henceforth with this model of the hyperelliptic curve. Denote the polynomial on the right-hand side by f and let α be a root of f. Then a standard argument shows that

$$x - \alpha = \kappa\xi^2$$

where κ, $\xi \in K = \mathbb{Q}(\alpha)$ and κ is an algebraic integer that comes from a finite computable set. In this section we suppose that the Mordell–Weil group $J(\mathbb{Q})$ of the curve C is known, and we show how to compute such a set of κ using our knowledge of the Mordell–Weil group $J(\mathbb{Q})$. The method for doing this depends on whether the degree n is odd or even.

10.3.1 The Odd Degree Case

Each coset of $J(\mathbb{Q})/2J(\mathbb{Q})$ has a coset representative of the form $\sum_{i=1}^{m}(P_i - \infty)$ where the set $\{P_1, \ldots, P_m\}$ is stable under the action of Galois, and where all $y(P_i)$ are non-zero. Now write $x(P_i) = \gamma_i/d_i^2$ where γ_i is an algebraic integer and $d_i \in \mathbb{Z}_{\geq 1}$; moreover if P_i, P_j are conjugate then we may suppose that $d_i = d_j$ and so γ_i, γ_j are conjugate. To such a coset representative of $J(\mathbb{Q})/2J(\mathbb{Q})$ we associate

$$\kappa = a^{(m \bmod 2)} \prod_{i=1}^{m} \left(\gamma_i - \alpha d_i^2 \right).$$

Lemma 10.3.1. *Let $\mathcal{K}$ be a set of κ associated as above to a complete set of coset representatives of $J(\mathbb{Q})/2J(\mathbb{Q})$. Then $\mathcal{K}$ is a finite subset of $\mathbb{O}_K$ and if (x, y) is an integral point on the model* (10.7) *then $x - \alpha = \kappa\xi^2$ for some $\kappa \in \mathcal{K}$ and $\xi \in K$.*

Proof. This follows trivially from the standard homomorphism

$$\theta : J(\mathbb{Q})/2J(\mathbb{Q}) \to K^*/K^{*2}$$

that is given by

$$\theta\left(\sum_{i=1}^{m}(P_i - \infty) \right) = a^m \prod_{i=1}^{m}(x(P_i) - \alpha) \pmod{K^{*2}}$$

for coset representatives $\sum(P_i - \infty)$ with $y(P_i) \neq 0$; see Section 4 of [46]. □

10.3.2 The Even Degree Case

As mentioned in the introduction, we shall assume the existence of at least one rational point P_0. If P_0 is one of the two points at infinity, let $\epsilon_0 = 1$. Otherwise, as f is irreducible, $y(P_0) \neq 0$; write $x(P_0) = \gamma_0/d_0^2$ with $\gamma_0 \in \mathbb{Z}$ and $d_0 \in \mathbb{Z}_{\geq 1}$ and let $\epsilon_0 = \gamma_0 - \alpha d_0^2$.

Each coset of $J(\mathbb{Q})/2J(\mathbb{Q})$ has a coset representative of the form $\sum_{i=1}^{m}(P_i - P_0)$ where the set $\{P_1, \ldots, P_m\}$ is stable under the action of Galois, and where all $y(P_i)$ are non-zero for $i = 1, \ldots, m$. Write $x(P_i) = \gamma_i/d_i^2$ where γ_i is an algebraic

integer and $d_i \in \mathbb{Z}_{\geq 1}$; moreover if P_i, P_j are conjugate then we may suppose that $d_i = d_j$ and so γ_i, γ_j are conjugate. To such a coset representative of $J(\mathbb{Q})/2J(\mathbb{Q})$ we associate

$$\epsilon = \epsilon_0^{(m \bmod 2)} \prod_{i=1}^{m} \left(\gamma_i - \alpha d_i^2 \right).$$

Lemma 10.3.2. *Let $\mathcal{E}$ be a set of ϵ associated as above to a complete set of coset representatives of $J(\mathbb{Q})/2J(\mathbb{Q})$. Let Δ be the discriminant of the polynomial f. For each $\epsilon \in \mathcal{E}$, let $\mathcal{B}_\epsilon$ be the set of square-free rational integers supported only by primes dividing $a\Delta \operatorname{Norm}_{K/\mathbb{Q}}(\epsilon)$. Let $\mathcal{K} = \{\epsilon b : \epsilon \in \mathcal{E},\ b \in \mathcal{B}_\epsilon\}$. Then $\mathcal{K}$ is a finite subset of $\mathbb{O}_K$ and if (x, y) is an integral point on the model* (10.7) *then $x - \alpha = \kappa\xi^2$ for some $\kappa \in \mathcal{K}$ and $\xi \in K$.*

Proof. In our even degree case, the homomorphism θ takes values in $K^*/\mathbb{Q}^*K^{*2}$. Thus if (x, y) is an integral point on the model (10.7), we have that $(x-\alpha) = \epsilon b \xi^2$ for some $\epsilon \in \mathcal{E}$ and b a square-free rational integer. A standard argument shows that $2 \mid \operatorname{ord}_\wp(x-\alpha)$ for all prime ideals $\wp \nmid a\Delta$. Hence, $2 \mid \operatorname{ord}_\wp(b)$ for all $\wp \nmid a\Delta\epsilon$. Let $\wp \mid p$ where p is a rational prime not dividing $a\Delta \operatorname{Norm}_{K/\mathbb{Q}}(\epsilon)$. Then p is unramified in $K/\mathbb{Q}$ and so $\operatorname{ord}_p(b) = \operatorname{ord}_\wp(b) \equiv 0 \pmod 2$. This shows that $b \in \mathcal{B}_\epsilon$ and proves the lemma. □

10.3.3 Remarks

The following remarks are applicable both to the odd and the even degree cases.

- We point out that even if we do not know coset representatives for $J(\mathbb{Q})/2J(\mathbb{Q})$, we can still obtain a suitable (though larger) set of κ that satisfies the conclusions of Lemmas 10.3.1 and 10.3.2 provided we are able to compute the class group and unit group of the number field K; for this see for example [9, Section 2.2].

- We can use local information at small and bad primes to restrict the set $\mathcal{K}$ further, compare [12] and [13], where this is applied to rational points. In our case, we can restrict the local computations to $x \in \mathbb{Z}_p$ instead of $\mathbb{Q}_p$.

10.4 Heights

We fix once and for all the following notation.

K	a number field,
$\mathbb{O}_K$	the ring of integers of K,
M_K	the set of all places of K,
M_K^0	the set of non-Archimedean places of K,
M_K^∞	the set of Archimedean places of K,
υ	a place of K,
K_υ	the completion of K at υ,
d_υ	the local degree $[K_\upsilon : \mathbb{Q}_\upsilon]$.

For $\upsilon \in M_K$, we let $|\cdot|_\upsilon$ be the usual normalized valuation corresponding to υ; in particular if υ is non-Archimedean and p is the rational prime below υ then $|p|_\upsilon = p^{-1}$. Thus if L/K is a field extension, and ω a place of L above υ then $|\alpha|_\omega = |\alpha|_\upsilon$, for all $\alpha \in K$.

Define

$$\alpha_\upsilon = |\alpha|_\upsilon^{d_\upsilon}.$$

Hence for $\alpha \in K^*$, the product formula states that

$$\prod_{\upsilon \in M_K} \alpha_\upsilon = 1.$$

In particular, if υ is Archimedean, corresponding to a real or complex embedding σ of K then

$$|\alpha|_\upsilon = |\sigma(\alpha)| \qquad \text{and} \qquad \alpha_\upsilon = \begin{cases} |\sigma(\alpha)| & \text{if } \sigma \text{ is real} \\ |\sigma(\alpha)|^2 & \text{if } \sigma \text{ is complex.} \end{cases}$$

For $\alpha \in K$, the (absolute) logarithmic height $\mathrm{h}(\alpha)$ is given by

$$\mathrm{h}(\alpha) = \frac{1}{[K:\mathbb{Q}]} \sum_{\upsilon \in M_K} d_\upsilon \log \max\{1, |\alpha|_\upsilon\} = \frac{1}{[K:\mathbb{Q}]} \sum_{\upsilon \in M_K} \log \max\{1, \alpha_\upsilon\}. \tag{10.8}$$

The absolute logarithmic height of α is independent of the field K containing α.

We shall need the following elementary properties of heights.

Lemma 10.4.1. *For any non-zero algebraic number α, we have $\mathrm{h}(\alpha^{-1}) = \mathrm{h}(\alpha)$. For algebraic numbers $\alpha_1, \ldots, \alpha_n$, we have*

$$\mathrm{h}(\alpha_1 \alpha_2 \cdots \alpha_n) \le \mathrm{h}(\alpha_1) + \cdots + \mathrm{h}(\alpha_n), \qquad \mathrm{h}(\alpha_1 + \cdots + \alpha_n) \le \log n + \mathrm{h}(\alpha_1) + \cdots + \mathrm{h}(\alpha_n).$$

Proof. The lemma is Exercise 8.8 in [41]. We do not know of a reference for the proof and so we will indicate briefly the proof of the second

(more difficult) inequality. For $\upsilon \in M_K$, choose i_υ in $\{1, \dots, n\}$ to satisfy $\max\{|\alpha_1|_\upsilon, \dots, |\alpha_n|_\upsilon\} = |\alpha_{i_\upsilon}|_\upsilon$. Note that

$$|\alpha_1 + \cdots + \alpha_n|_\upsilon \le \epsilon_\upsilon |\alpha_{i_\upsilon}|_\upsilon, \qquad \text{where} \qquad \epsilon_\upsilon = \begin{cases} n & \text{if } \upsilon \text{ is Archimedean,} \\ 1 & \text{otherwise.} \end{cases}$$

Thus

$$\log \max\{1, |\alpha_1 + \cdots + \alpha_n|_\upsilon\} \le \log \epsilon_\upsilon + \log \max\{1, |\alpha_{i_\upsilon}|_\upsilon\} \le \log \epsilon_\upsilon + \sum_{i=1}^{n} \log \max\{1, |\alpha_i|_\upsilon\}.$$

Observe that

$$\frac{1}{[K:\mathbb{Q}]} \sum_{\upsilon \in M_K} d_\upsilon \log \epsilon_\upsilon = \frac{\log n}{[K:\mathbb{Q}]} \sum_{\upsilon \in M_K^\infty} d_\upsilon = \log n;$$

the desired inequality follows from the definition of logarithmic height (10.8). □

10.4.1 Height Lower Bound

We need the following result of Voutier [51] concerning Lehmer's problem.

Lemma 10.4.2. *Let K be a number field of degree d. Let*

$$\partial_K = \begin{cases} \frac{\log 2}{d} & \text{if } d = 1, 2, \\ \frac{1}{4} \left(\frac{\log \log d}{\log d} \right)^3 & \text{if } d \ge 3. \end{cases}$$

Then, for every non-zero algebraic number α in K, which is not a root of unity,

$$\deg(\alpha)\, \mathrm{h}(\alpha) \ge \partial_K.$$

Throughout, by the logarithm of a complex number, we mean the principal determination of the logarithm. In other words, if $x \in \mathbb{C}^*$ we express $x = re^{i\theta}$ where $r > 0$ and $-\pi < \theta \le \pi$; we then let $\log x = \log r + i\theta$.

Lemma 10.4.3. *Let K be a number field and let*

$$\partial'_K = \left(1 + \frac{\pi^2}{\partial_K^2}\right)^{1/2}.$$

For any non-zero $\alpha \in K$ and any place $\upsilon \in M_K$

$$\log |\alpha|_\upsilon \le \deg(\alpha)\, \mathrm{h}(\alpha), \qquad \log \alpha_\upsilon \le [K:\mathbb{Q}]\, \mathrm{h}(\alpha).$$

Moreover, if α is not a root of unity and σ is a real or complex embedding of K then

$$|\log \sigma(\alpha)| \le \partial'_K \deg(\alpha)\, \mathrm{h}(\alpha).$$

Proof. The first two inequalities are an immediate consequence of the definition of absolute logarithmic height. For the last, write $\sigma(\alpha) = e^{a+ib}$, with $a = \log|\sigma(\alpha)|$ and $|b| \leq \pi$, and let $d = \deg(\alpha)$. Then we have

$$|\log \sigma(\alpha)| = (a^2 + b^2)^{1/2} \leq (\log^2|\sigma(\alpha)| + \pi^2)^{1/2} \leq ((d\,\mathrm{h}(\alpha))^2 + \pi^2)^{1/2}.$$

By Lemma 10.4.2 we have $d\,\mathrm{h}(\alpha) \geq \partial_K$, so

$$|\log \sigma(\alpha)| \leq d\ \mathrm{h}(\alpha)\ \left(1 + \frac{\pi^2}{\partial_K^2}\right)^{1/2},$$

as required. □

10.5 Bounds for Regulators

Later on we need to give upper bounds for the regulators of complicated number fields of high degree. The following lemma, based on bounds of Landau [29], is an easy way to obtain reasonable bounds.

Lemma 10.5.1. *Let K be a number field with degree $d = u + 2v$ where u and v are respectively the numbers of real and complex embeddings. Denote the absolute discriminant by D_K and the regulator by R_K, and the number of roots of unity in K by w. Suppose, moreover, that L is a real number such that $D_K \leq L$. Let*

$$a = 2^{-v}\,\pi^{-d/2}\,\sqrt{L}.$$

Define the function $f_K(L, s)$ by

$$f_K(L, s) = 2^{-u}\,w\,a^s\,\big(\Gamma(s/2)\big)^u\,\big(\Gamma(s)\big)^v\,s^{d+1}\,(s-1)^{1-d},$$

and let $B_K(L) = \min\{f_K(L, 2 - t/1000)\ : t = 0, 1, \ldots, 999\}$. Then $R_K < B_K(L)$.

Proof. Landau [29, proof of Hilfssatz 1] established the inequality $R_K < f_K(D_K, s)$ for all $s > 1$. It is thus clear that $R_K < B_K(L)$. □

Perhaps a comment is in order. For a complicated number field of high degree it is difficult to calculate the discriminant D_K exactly, though it is easy to give an upper bound L for its size. It is also difficult to minimise the function $f_K(L, s)$ analytically, but we have found that the above gives an accurate enough result, which is easy to calculate on a computer.

10.6 Fundamental Units

For the number fields we are concerned with, we shall need to work with a certain system of fundamental units, given by the following lemma due to Bugeaud and Győry, which is Lemma 1 of [15].

Lemma 10.6.1. *Let K be a number field of degree d and let $r = r_K$ be its unit rank and R_K its regulator. Define the constants*

$$c_1 = c_1(K) = \frac{(r\,!)^2}{2^{r-1}d^r}\,, \qquad c_2 = c_2(K) = c_1\left(\frac{d}{\partial_K}\right)^{r-1}, \qquad c_3 = c_3(K) = c_1\frac{d^r}{\partial_K}\,.$$

Then K admits a system $\{\varepsilon_1, \ldots, \varepsilon_r\}$ of fundamental units such that:

(i) $$\prod_{i=1}^{r} \mathrm{h}(\varepsilon_i) \le c_1 R_K,$$

(ii) $$\mathrm{h}(\varepsilon_i) \le c_2 R_K, \quad 1 \le i \le r,$$

(iii) Write $\mathcal{M}$ for the $r \times r$-matrix $(\log\varepsilon_{i\upsilon})$ where υ runs over r of the Archimedean places of K and $1 \le i \le r$. Then the absolute values of the entries of $\mathcal{M}^{-1}$ are bounded above by c_3.

Lemma 10.6.2. *Let K be a number field of degree d, and let $\{\varepsilon_1, \ldots, \varepsilon_r\}$ be a system of fundamental units as in Lemma 10.6.1. Define the constant $c_4 = c_4(K) = rdc_3$. Suppose $\varepsilon = \zeta\varepsilon_1^{b_1}\ldots\varepsilon_r^{b_r}$, where ζ is a root of unity in K. Then*

$$\max\{|b_1|, \ldots, |b_r|\} \le c_4\,\mathrm{h}(\varepsilon).$$

Proof. Note that for any Archimedean place v of K,

$$\log\varepsilon_v = \sum b_i \log\varepsilon_{iv}.$$

The lemma now follows from part (iii) of Lemma 10.6.1, plus the fact that $\log\varepsilon_v \le d\,\mathrm{h}(\varepsilon)$ for all v given by Lemma 10.4.3. □

The following result is a special case of Lemma 2 of [15].

Lemma 10.6.3. *Let K be a number field of unit rank r and regulator K. Let α be a non-zero algebraic integer belonging to K. Then there exists a unit ε of K such that*

$$\mathrm{h}(\alpha\varepsilon) \le c_5 R_K + \frac{\log|\mathrm{Norm}_{K/\mathbb{Q}}(\alpha)|}{[K:\mathbb{Q}]}$$

where

$$c_5 = c_5(K) = \frac{r^{r+1}}{2\partial_K^{r-1}}.$$

Lemma 10.6.4. *Let K be a number field, $\beta, \varepsilon \in K^*$ with ε being a unit. Let σ be the real or complex embedding that makes $|\sigma(\beta\varepsilon)|$ minimal. Then*

$$\mathrm{h}(\beta\varepsilon) \leq \mathrm{h}(\beta) - \log|\sigma(\beta\varepsilon)|.$$

Proof. As usual, write $d = [K : \mathbb{Q}]$ and $d_\upsilon = [K_\upsilon : \mathbb{Q}_\upsilon]$. Note

$$\begin{aligned}
\mathrm{h}(\beta\varepsilon) &= \mathrm{h}(1/\beta\varepsilon) \\
&= \frac{1}{d}\sum_{\upsilon\in M_K^\infty} d_\upsilon \max\{0, \log(|\beta\varepsilon|_\upsilon^{-1})\} + \frac{1}{d}\sum_{\upsilon\in M_K^0} d_\upsilon \max\{0, \log(|\beta\varepsilon|_\upsilon^{-1})\} \\
&\leq \log(|\sigma(\beta\varepsilon)|^{-1}) + \frac{1}{d}\sum_{\upsilon\in M_K^0} d_\upsilon \max\{0, \log(|\beta|_\upsilon^{-1})\} \\
&\leq -\log|\sigma(\beta\varepsilon)| + \frac{1}{d}\sum_{\upsilon\in M_K} d_\upsilon \max\{0, \log(|\beta|_\upsilon^{-1})\} \\
&\leq -\log|\sigma(\beta\varepsilon)| + \mathrm{h}(\beta),
\end{aligned}$$

as required. □

10.7 Matveev's Lower Bound for Linear Forms in Logarithms

Let L be a number field and let σ be a real or complex embedding. For $\alpha \in L^*$ we define the *modified logarithmic height of α with respect to σ* to be

$$\mathrm{h}_{L,\sigma}(\alpha) := \max\{[L : \mathbb{Q}]\mathrm{h}(\alpha)\ ,\ |\log\sigma(\alpha)|\ ,\ 0.16\}.$$

The modified height is clearly dependent on the number field; we shall need the following Lemma which gives a relation between the modified and absolute height.

Lemma 10.7.1. *Let $K \subseteq L$ be number fields and write*

$$\partial_{L/K} = \max\left\{[L : \mathbb{Q}]\ ,\ [K : \mathbb{Q}]\partial'_K\ ,\ \frac{0.16[K : \mathbb{Q}]}{\partial_K}\right\}.$$

Then for any $\alpha \in K$ which is neither zero nor a root of unity, and any real or complex embedding σ of L,

$$\mathrm{h}_{L,\sigma}(\alpha) \leq \partial_{L/K}\,\mathrm{h}(\alpha).$$

Proof. By Lemma 10.4.3 we have

$$[K : \mathbb{Q}]\partial'_K \, \mathrm{h}(\alpha) \geq \partial'_K \deg(\alpha) \, \mathrm{h}(\alpha) \geq |\log \sigma(\alpha)|.$$

Moreover, by Lemma 10.4.2,

$$\frac{0.16[K : \mathbb{Q}] \, \mathrm{h}(\alpha)}{\partial_K} \geq \frac{0.16 \deg(\alpha) \, \mathrm{h}(\alpha)}{\partial_K} \geq 0.16.$$

The lemma follows. □

We shall apply lower bounds on linear forms, more precisely a version of Matveev's estimates [31]. We recall that log denotes the principal determination of the logarithm.

Lemma 10.7.2. *Let L be a number field of degree d, with $\alpha_1, \ldots, \alpha_n \in L^*$. Define a constant*

$$C(L, n) := 3 \cdot 30^{n+4} \cdot (n + 1)^{5.5} \, d^2 \, (1 + \log d).$$

Consider the "linear form"

$$\Lambda := \alpha_1^{b_1} \cdots \alpha_n^{b_n} - 1,$$

where $b_1, \ldots, b_n$ are rational integers and let $B := \max\{|b_1|, \ldots, |b_n|\}$. If $\Lambda \neq 0$, and σ is any real or complex embedding of L then

$$\log|\sigma(\Lambda)| > -C(L, n)(1 + \log(nB)) \prod_{j=1}^{n} \mathrm{h}_{L,\sigma}(\alpha_j).$$

Proof. This straightforward corollary of Matveev's estimates is Theorem 9.4 of [16]. □

10.8 Bounds for Unit Equations

Now we are ready to prove an explicit version of Lemma 4 of [14]. The proposition below allows us to replace in the final estimate the regulator of the larger field by the product of the regulators of two of its subfields. This often results in a significant improvement of the upper bound for the height. This idea is due to Voutier [52].

Proposition 10.8.1. *Let L be a number field of degree d, which contains K_1 and K_2 as subfields. Let R_{K_i} (respectively r_i) be the regulator (respectively the unit rank) of K_i. Suppose further that ν_1, ν_2 and ν_3 are non-zero elements of L with height $\leq H$ (with $H \geq 1$) and consider the unit equation*

$$\nu_1\varepsilon_1 + \nu_2\varepsilon_2 + \nu_3\varepsilon_3 = 0 \tag{10.9}$$

where ε_1 is a unit of K_1, ε_2 a unit of K_2 and ε_3 a unit of L. Then, for $i = 1$ and 2,

$$\mathrm{h}(\nu_i\varepsilon_i/\nu_3\varepsilon_3) \leq A_2 + A_1 \log\{H + \max\{\mathrm{h}(\nu_1\varepsilon_1), \mathrm{h}(\nu_2\varepsilon_2)\}\},$$

where

$$A_1 = 2H \cdot C(L, r_1 + r_2 + 1) \cdot c_1(K_1)c_1(K_2)\partial_{L/L} \cdot (\partial_{L/K_1})^{r_1} \cdot (\partial_{L/K_2})^{r_2} \cdot R_{K_1}R_{K_2},$$

and

$$A_2 = 2H + A_1 + A_1 \log\{(r_1 + r_2 + 1) \cdot \max\{c_4(K_1), c_4(K_2), 1\}\}.$$

Proof. Let $\{\mu_1, \ldots, \mu_{r_1}\}$ and $\{\rho_1, \ldots, \rho_{r_2}\}$ be respectively systems of fundamental units for K_1 and K_2 as in Lemma 10.6.1; in particular we know that

$$\prod_{j=1}^{r_1} \mathrm{h}(\mu_j) \leq c_1(K_1)R_{K_1}, \qquad \prod_{j=1}^{r_2} \mathrm{h}(\rho_j) \leq c_1(K_2)R_{K_2}. \tag{10.10}$$

We can write

$$\varepsilon_1 = \zeta_1\mu_1^{b_1} \cdots \mu_{r_1}^{b_{r_1}}, \quad \varepsilon_2 = \zeta_2\rho_1^{f_1} \cdots \rho_{r_2}^{f_{r_2}},$$

where ζ_1 and ζ_2 are roots of unity and $b_1, \ldots, b_{r_1}$, and $f_1, \ldots, f_{r_2}$ are rational integers. Set

$$B_1 = \max\{|b_1|, \ldots, |b_{r_1}|\}, \quad B_2 = \max\{|f_1|, \ldots, |f_{r_2}|\}, \quad B = \max\{B_1, B_2, 1\}.$$

Set $\alpha_0 = -\zeta_2\nu_2/(\zeta_1\nu_1)$ and $b_0 = 1$. By (10.9),

$$\frac{\nu_3\varepsilon_3}{\nu_1\varepsilon_1} = \alpha_0^{b_0}\mu_1^{-b_1} \cdots \mu_{r_1}^{-b_{r_1}}\rho_1^{f_1} \cdots \rho_{r_2}^{f_{r_2}} - 1.$$

Now choose the real or complex embedding σ of L such that $|\sigma((\nu_3\varepsilon_3)/(\nu_1\varepsilon_1))|$ is minimal. We apply Matveev's estimate (Lemma 10.7.2) to this "linear form", obtaining

$$\log\left|\sigma\left(\frac{\nu_3\varepsilon_3}{\nu_1\varepsilon_1}\right)\right| > -C(L, n)(1 + \log(nB))\,\mathrm{h}_{L,\sigma}(\alpha_0)\prod_{j=1}^{r_1}\mathrm{h}_{L,\sigma}(\mu_j)\prod_{j=1}^{r_2}\mathrm{h}_{L,\sigma}(\rho_j),$$

where $n = r_1 + r_2 + 1$. Using Lemma 10.7.1 and equation (10.10) we obtain

$$\prod_{j=1}^{r_1} \mathrm{h}_{L,\sigma}(\mu_j) \le (\partial_{L/K_1})^{r_1} \prod_{j=1}^{r_1} \mathrm{h}(\mu_j) \le c_1(K_1)(\partial_{L/K_1})^{r_1} R_{K_1},$$

and a similar estimate for $\prod_{j=1}^{r_2} \mathrm{h}_{L,\sigma}(\rho_j)$. Moreover, again by Lemma 10.7.1 and Lemma 10.4.1, $\mathrm{h}_{L,\sigma}(\alpha_0) \le 2H\partial_{L/L}$. Thus

$$\log \left| \sigma \left(\frac{\nu_3 \varepsilon_3}{\nu_1 \varepsilon_1} \right) \right| > -A_1(1 + \log(nB)).$$

Now applying Lemma 10.6.4, we obtain that

$$\mathrm{h}\left(\frac{\nu_3 \varepsilon_3}{\nu_1 \varepsilon_1} \right) \le \mathrm{h}\left(\frac{\nu_3}{\nu_1} \right) + A_1(1 + \log(nB)) \le 2H + A_1(1 + \log(nB)).$$

The proof is complete on observing, from Lemma 10.6.2, that

$$B \le \max\{c_4(K_1), c_4(K_2), 1)\} \max\{\mathrm{h}(\varepsilon_1), \mathrm{h}(\varepsilon_2), 1\},$$

and from Lemma 10.4.1, $\mathrm{h}(\nu_i \varepsilon_i) \le \mathrm{h}(\varepsilon_i) + \mathrm{h}(\nu_i) \le \mathrm{h}(\varepsilon) + H$. □

10.9 Upper Bounds for the Size of Integral Points on Hyperelliptic Curves

We shall need the following standard sort of lemma.

Lemma 10.9.1. *Let a, b, c, y be positive numbers and suppose that*

$$y \le a + b \log(c + y).$$

Then

$$y \le 2b \log b + 2a + c.$$

Proof. Let $z = c + y$, so that $z \le (a + c) + b \log z$. Now we apply case $h = 1$ of Lemma 2.2 of [34]; this gives $z \le 2(b \log b + a + c)$, and the lemma follows. □

Theorem 10.9.1. *Let α be an algebraic integer of degree at least 3, and let κ be a integer belonging to K. Let α_1, α_2, α_3 be distinct conjugates of α and κ_1, κ_2, κ_3 be the corresponding conjugates of κ. Let*

$$K_1 = \mathbb{Q}(\alpha_1, \alpha_2, \sqrt{\kappa_1 \kappa_2}), \quad K_2 = \mathbb{Q}(\alpha_1, \alpha_3, \sqrt{\kappa_1 \kappa_3}), \quad K_3 = \mathbb{Q}(\alpha_2, \alpha_3, \sqrt{\kappa_2 \kappa_3}),$$

and

$$L = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \sqrt{\kappa_1 \kappa_2}, \sqrt{\kappa_1 \kappa_3}).$$

Let R be an upper bound for the regulators of K_1, K_2 and K_3. Let r be the maximum of the unit ranks of K_1, K_2, K_3. Let

$$c_j^* = \max_{1\le i\le 3} c_j(K_i).$$

Let

$$N = \max_{1\le i,j\le 3} \left|\mathrm{Norm}_{\mathbb{Q}(\alpha_i,\alpha_j)/\mathbb{Q}}(\kappa_i(\alpha_i-\alpha_j))\right|^2.$$

Let

$$H^* = c_5^* R + \frac{\log N}{\min_{1\le i\le 3}[K_i:\mathbb{Q}]} + \mathrm{h}(\kappa).$$

Let

$$A_1^* = 2H^*\cdot C(L,2r+1)\cdot (c_1^*)^2 \partial_{L/L}\cdot\left(\max_{1\le i\le 3}\partial_{L/K_i}\right)^{2r}\cdot R^2,$$

and

$$A_2^* = 2H^* + A_1^* + A_1^*\log\{(2r+1)\cdot\max\{c_4^*,1\}\}.$$

If $x\in\mathbb{Z}\backslash\{0\}$ satisfies $x-\alpha=\kappa\xi^2$ for some $\xi\in K$ then

$$\log|x| \le 8A_1^*\log(4A_1^*) + 8A_2^* + H^* + 20\log 2 + 13\,\mathrm{h}(\kappa) + 19\,\mathrm{h}(\alpha).$$

Proof. Conjugating the relation $x-\alpha=\kappa\xi^2$ appropriately and taking differences we obtain

$$\alpha_1-\alpha_2=\kappa_2\xi_2^2-\kappa_1\xi_1^2,\quad \alpha_3-\alpha_1=\kappa_1\xi_1^2-\kappa_3\xi_3^2,\quad \alpha_2-\alpha_3=\kappa_3\xi_3^2-\kappa_2\xi_2^2.$$

Let

$$\tau_1=\kappa_1\xi_1,\qquad \tau_2=\sqrt{\kappa_1\kappa_2}\xi_2,\qquad \tau_3=\sqrt{\kappa_1\kappa_3}\xi_3.$$

Observe that

$$\kappa_1(\alpha_1-\alpha_2)=\tau_2^2-\tau_1^2,\quad \kappa_1(\alpha_3-\alpha_1)=\tau_1^2-\tau_3^2,\quad \kappa_1(\alpha_2-\alpha_3)=\tau_3^2-\tau_2^2,$$

and

$$\tau_2\pm\tau_1\in K_1,\quad \tau_1\pm\tau_3\in K_2,\quad \tau_3\pm\tau_2\in\sqrt{\kappa_1/\kappa_2}K_3.$$

We claim that each $\tau_i\pm\tau_j$ can be written in the form $\nu\varepsilon$ where ε is a unit in one of the K_i and $\nu\in L$ is an integer satisfying $\mathrm{h}(\nu)\le H^*$. Let us show this for $\tau_2-\tau_3$; the other cases are either similar or easier. Note that $\tau_2-\tau_3=\sqrt{\kappa_1/\kappa_2}\nu''$ where ν'' is an integer belonging to K_3. Moreover, ν'' divides

$$\sqrt{\frac{\kappa_2}{\kappa_1}}(\tau_3-\tau_2)\cdot\sqrt{\frac{\kappa_2}{\kappa_1}}(\tau_3+\tau_2)=\kappa_2(\alpha_2-\alpha_3).$$

Hence $|\mathrm{Norm}_{K_3/\mathbb{Q}}(\nu'')| \leq N$. By Lemma 10.6.3, we can write $\nu'' = \nu'\varepsilon$ where $\varepsilon \in K_3$ and

$$\mathrm{h}(\nu') \leq c_5(K_3)R + \frac{\log N}{[K_3 : \mathbb{Q}]}.$$

Now let $\nu = \sqrt{\kappa_1/\kappa_2}\nu'$. Thus $\tau_2 - \tau_3 = \nu\varepsilon$ where $\mathrm{h}(\nu) \leq \mathrm{h}(\nu') + \mathrm{h}(\kappa) \leq H^*$ proving our claim.

We apply Proposition 10.8.1 to the unit equation

$$(\tau_1 - \tau_2) + (\tau_3 - \tau_1) + (\tau_2 - \tau_3) = 0,$$

which is indeed of the form $\nu_1\varepsilon_1 + \nu_2\varepsilon_2 + \nu_3\varepsilon_3 = 0$ where the ν_i and ε_i satisfy the conditions of that proposition with H replaced by H^*. We obtain

$$\mathrm{h}\left(\frac{\tau_1 - \tau_2}{\tau_1 - \tau_3}\right) \leq A_2^* + A_1^* \log\{H^* + \max\{\mathrm{h}(\tau_2 - \tau_3), \mathrm{h}(\tau_1 - \tau_2)\}\}.$$

Observe that

$$\begin{aligned}\mathrm{h}(\tau_i \pm \tau_j) &\leq \log 2 + \mathrm{h}(\tau_i) + \mathrm{h}(\tau_j)\\ &\leq \log 2 + 2\,\mathrm{h}(\kappa) + 2\,\mathrm{h}(\xi)\\ &\leq \log 2 + 3\,\mathrm{h}(\kappa) + \mathrm{h}(x - \alpha)\\ &\leq 2\log 2 + 3\,\mathrm{h}(\kappa) + \mathrm{h}(\alpha) + \log|x|,\end{aligned}$$

where we have made repeated use of Lemma 10.4.1. Thus

$$\mathrm{h}\left(\frac{\tau_1 - \tau_2}{\tau_1 - \tau_3}\right) \leq A_2^* + A_1^* \log(A_3^* + \log|x|),$$

where $A_3^* = H^* + 2\log 2 + 3\,\mathrm{h}(\kappa) + \mathrm{h}(\alpha)$.

We also apply Proposition 10.8.1 to the unit equation

$$(\tau_1 + \tau_2) + (\tau_3 - \tau_1) - (\tau_2 + \tau_3) = 0,$$

to obtain precisely the same bound for $\mathrm{h}\left(\frac{\tau_1+\tau_2}{\tau_1-\tau_3}\right)$. Using the identity

$$\left(\frac{\tau_1 - \tau_2}{\tau_1 - \tau_3}\right) \cdot \left(\frac{\tau_1 + \tau_2}{\tau_1 - \tau_3}\right) = \frac{\kappa_1(\alpha_2 - \alpha_1)}{(\tau_1 - \tau_3)^2},$$

we obtain that

$$\mathrm{h}(\tau_1 - \tau_3) \leq \frac{\log 2 + \mathrm{h}(\kappa)}{2} + \mathrm{h}(\alpha) + A_2^* + A_1^* \log(A_3^* + \log|x|).$$

Now

$$\begin{aligned}
\log|x| &\le \log 2 + \mathrm{h}(\alpha) + \mathrm{h}(x-\alpha_1) \\
&\le \log 2 + \mathrm{h}(\alpha) + \mathrm{h}(\kappa) + 2\,\mathrm{h}(\tau_1) \qquad (\text{using } x-\alpha_1 = \tau_1^2/\kappa_1) \\
&\le 5\log 2 + \mathrm{h}(\alpha) + \mathrm{h}(\kappa) + 2\,\mathrm{h}(\tau_1+\tau_3) + 2\,\mathrm{h}(\tau_1-\tau_3) \\
&\le 5\log 2 + \mathrm{h}(\alpha) + \mathrm{h}(\kappa) + 2\,\mathrm{h}\left(\frac{\kappa_1(\alpha_3-\alpha_1)}{\tau_1-\tau_3}\right) + 2\,\mathrm{h}(\tau_1-\tau_3) \\
&\le 7\log 2 + 5\,\mathrm{h}(\alpha) + 3\,\mathrm{h}(\kappa) + 4\,\mathrm{h}(\tau_1-\tau_3) \\
&\le 9\log 2 + 9\,\mathrm{h}(\alpha) + 5\,\mathrm{h}(\kappa) + 4A_2^* + 4A_1^*\log(A_3^* + \log|x|).
\end{aligned}$$

The theorem follows from Lemma 10.9.1. □

10.10 The Mordell–Weil Sieve I

The Mordell–Weil sieve is a technique that can be used to show the non-existence of rational points on a curve (for example [12], [8]), or to help determine the set of rational points in conjunction with the method of Chabauty (for example [11]); for connections to the Brauer–Manin obstruction see, for example, [24], [36] or [48]. In this section and the next we explain how the Mordell–Weil sieve can be used to show that any rational point on a curve of genus ≥ 2 is either a known rational point or a very large rational point.

In this section we let $C/\mathbb{Q}$ be a smooth projective curve (not necessarily hyperelliptic) of genus $g \ge 2$ and we let J be its Jacobian. As indicated in the introduction, we assume the knowledge of some rational point on C; henceforth let D be a fixed rational point on C (or even a fixed rational divisor of degree 1) and let $\jmath$ be the corresponding Abel–Jacobi map:

$$\jmath : C \to J, \qquad P \mapsto [P-D].$$

Let W be the image in J of the known rational points on C. The Mordell–Weil sieve is a strategy for obtaining a very large and 'smooth' positive integer B such that

$$\jmath(C(\mathbb{Q})) \subseteq W + BJ(\mathbb{Q}).$$

Recall that a positive integer B is called A-smooth if all its prime factors are $\le A$. By saying that B is smooth, we loosely mean that it is A-smooth with A much smaller than B.

Let S be a finite set of primes, which for now we assume to be primes of good reduction for the curve C. The basic idea is to consider the following

commutative diagram.

$$\begin{array}{ccc} C(\mathbb{Q}) & \xrightarrow{J} & J(\mathbb{Q})/BJ(\mathbb{Q}) \\ \downarrow & & \downarrow \alpha \\ \prod_{p\in S} C(\mathbb{F}_p) & \xrightarrow{J} & \prod_{p\in S} J(\mathbb{F}_p)/BJ(\mathbb{F}_p) \end{array}$$

The image of $C(\mathbb{Q})$ in $J(\mathbb{Q})/BJ(\mathbb{Q})$ must then be contained in the subset of $J(\mathbb{Q})/BJ(\mathbb{Q})$ of elements that map under α into the image of the lower horizontal map. If we find that this subset equals the image of W in $J(\mathbb{Q})/BJ(\mathbb{Q})$, then we have shown that

$$J(C(\mathbb{Q})) \subseteq W + BJ(\mathbb{Q})$$

as desired. Note that, at least in principle, the required computation is finite: each set $C(\mathbb{F}_p)$ is finite and can be enumerated, hence $J(C(\mathbb{F}_p))$ can be determined, and we assume that we know explicit generators of $J(\mathbb{Q})$, which allows us to construct the finite set $J(\mathbb{Q})/BJ(\mathbb{Q})$. In practice, and in particular for the application we have in mind here, we will need a very large value of B, so this naive approach is much too inefficient. In [12] and [8], the authors describe how one can perform this computation in a more efficient way.

One obvious improvement is to replace the lower horizontal map in the diagram above by a product of maps

$$C(\mathbb{Q}_p) \xrightarrow{J} G_p/BG_p$$

with suitable finite quotients G_p of $J(\mathbb{Q}_p)$. We have used this to incorporate information modulo higher powers of p for small primes p. This kind of information is often called "deep" information, as opposed to the "flat" information obtained from reduction modulo good primes.

We can always force B to be divisible by any given (not too big) number. In our application we will want B to kill the rational torsion subgroup of J.

10.11 The Mordell–Weil Sieve II

We continue with the notation of Section 10.10. Let W be the image in $J(\mathbb{Q})$ of all the known rational points on C. We assume that the strategy of Section 10.10 is successful in yielding a large 'smooth' integer B such that any point $P \in C(\mathbb{Q})$ satisfies $J(P) - w \in BJ(\mathbb{Q})$ for some $w \in W$, and moreover, that B kills all the torsion of $J(\mathbb{Q})$.

Let

$$\phi : \mathbb{Z}^r \to J(\mathbb{Q}), \qquad \phi(a_1, \ldots, a_r) = \sum a_i D_i,$$

so that the image of ϕ is simply the free part of $J(\mathbb{Q})$. Our assumption is now that

$$\jmath(C(\mathbb{Q})) \subset W + \phi(B\mathbb{Z}^n).$$

Set $L_0 = B\mathbb{Z}^n$. We explain a method of obtaining a (very long) decreasing sequence of lattices in $\mathbb{Z}^n$:

$$B\mathbb{Z}^n = L_0 \supsetneq L_1 \supsetneq L_2 \supsetneq \cdots \supsetneq L_k \tag{10.11}$$

such that

$$\jmath(C(\mathbb{Q})) \subset W + \phi(L_j)$$

for $j = 1, \ldots, k$.

If q is a prime of good reduction for J we denote by

$$\phi_q : \mathbb{Z}^r \to J(\mathbb{F}_q), \qquad \phi_q(a_1, \ldots, a_r) = \sum a_i \tilde{D}_i,$$

and so $\phi_q(\mathbf{l}) = \widetilde{\phi(\mathbf{l})}$.

Lemma 10.11.1. *Let W be a finite subset of $J(\mathbb{Q})$, and let L be a subgroup of $\mathbb{Z}^r$. Suppose that $\jmath(C(\mathbb{Q})) \subset W + \phi(L)$. Let q be a prime of good reduction for C and J. Let L' be the kernel of the restriction $\phi_q|_L$. Let $\mathbf{l}_1, \ldots, \mathbf{l}_m$ be representatives of the non-zero cosets of L/L' and suppose that $\tilde{w} + \phi_q(\mathbf{l}_i) \notin \jmath C(\mathbb{F}_q)$ for all $w \in W$ and $i = 1, \ldots, m$. Then $\jmath(C(\mathbb{Q})) \subset W + \phi(L')$.*

Proof. Suppose $P \in C(\mathbb{Q})$. Since $j(C(\mathbb{Q})) \subset W + \phi(L)$, we may write $\jmath(P) = w + \phi(\mathbf{l})$ for some $\mathbf{l} \in L$. Now let $\mathbf{l}_0 = \mathbf{0}$, so that $\mathbf{l}_0, \ldots, \mathbf{l}_m$ represent all cosets of L/L'. Then $\mathbf{l} = \mathbf{l}_i + \mathbf{l}'$ for some $\mathbf{l}' \in L'$ and $i = 0, \ldots, m$. However, $\phi_q(\mathbf{l}') = 0$, or in other words, $\widetilde{\phi(\mathbf{l}')} = 0$. Hence

$$\jmath(\tilde{P}) = \widetilde{\jmath(P)} = \tilde{w} + \phi_q(\mathbf{l}) = \tilde{w} + \phi_q(\mathbf{l}_i) + \phi_q(\mathbf{l}') = \tilde{w} + \phi_q(\mathbf{l}_i).$$

By hypothesis, $\tilde{w} + \phi_q(\mathbf{l}_i) \notin \jmath C(\mathbb{F}_q)$ for $i = 1, \ldots, m$, so $i = 0$ and so $\mathbf{l}_i = 0$. Hence $\jmath(P) = w + \mathbf{l}' \in W + L'$ as required. □

We obtain a very long strictly decreasing sequence of lattices as in (10.11) by repeated application of Lemma 10.11.1. However, the conditions of Lemma 10.11.1 are unlikely to be satisfied for a prime q chosen at random. Here we give criteria that we have employed in practice to choose the primes q.

(I) $\gcd(B, \#J(\mathbb{F}_q)) > (\#J(\mathbb{F}_q))^{0.6}$,

(II) $L' \neq L$,

(III) $\#W \cdot (\#L/L' - 1) < 2q$,

(IV) $\tilde{w} + \phi_q(\mathbf{l}_i) \notin {}_JC(\mathbb{F}_q)$ for all $w \in W$ and $i = 1, \ldots, m$.

The criteria I–IV are listed in the order in which we check them in practice. Criterion IV is just the criterion of the lemma. Criterion II ensures that L' is strictly smaller than L, otherwise we gain no new information. Although we would like L' to be strictly smaller than L, we do not want the index L/L' to be too large and this is reflected in Criteria I and III. Note that the number of checks required by Criterion IV (or the lemma) is $\#W \cdot (\#L/L' - 1)$. If this number is large then Criterion IV is likely to fail. Let us look at this in probabilistic terms. Assume that the genus of C is 2. Then the probability that a random element of $J(\mathbb{F}_q)$ lies in the image of $C(\mathbb{F}_q)$ is about $1/q$. If $N = \#W \cdot (\#L/L' - 1)$ then the probability that Criterion IV is satisfied is about $(1 - q^{-1})^N$. Since $(1 - q^{-1})^q \sim e^{-1}$, we do not want N to be too large in comparison to q, and this explains the choice of $2q$ in Criterion III.

We still have not justified Criterion I. The computation involved in obtaining L' is a little expensive. Since we need to do this with many primes, we would like a way of picking only primes where this computation is not wasted, and in particular $\#L/L'$ is not too large. Now at every stage of our computations, L will be some element of our decreasing sequence (10.11) and so contained in $B\mathbb{Z}^n$. Criterion I ensures that a 'large chunk' of L will be in the kernel of $\phi_q : \mathbb{Z}^n \to J(\mathbb{F}_q)$ and so that $\#L/L'$ is not too large. The exponent 0.6 in Criterion I is chosen on the basis of computational experience.

10.12 Lower Bounds for the Size of Rational Points

In this section, we suppose that the strategy of Sections 10.10 and 10.11 succeeded in showing that ${}_JC(\mathbb{Q}) \subset W + \phi(L)$ for some lattice L of huge index in $\mathbb{Z}^r$, where W is the image of J of the set of known rational points in C. In this section we provide a lower bound for the size of rational points not belonging to the set of known rational points.

Lemma 10.12.1. *Let W be a finite subset of $J(\mathbb{Q})$, and let L be a sublattice of $\mathbb{Z}^r$. Suppose that ${}_JC(\mathbb{Q}) \subset W + \phi(L)$. Let μ_1 be a lower bound for $h - \hat{h}$ as in* (10.2). *Let*

$$\mu_2 = \max\left\{\sqrt{\hat{h}(w)} \ : \ w \in W\right\}.$$

Let M be the height-pairing matrix for the Mordell–Weil basis $D_1, \ldots, D_r$ and let $\lambda_1, \ldots, \lambda_r$ be its eigenvalues. Let

$$\mu_3 = \min\left\{\sqrt{\lambda_j} \ : \ j = 1, \ldots, r\right\}.$$

Let $m(L)$ be the Euclidean norm of the shortest non-zero vector of L, and suppose that $\mu_3 m(L) \geq \mu_2$. Then, for any $P \in C(\mathbb{Q})$, either $\jmath(P) \in W$ or

$$h(\jmath(P)) \geq (\mu_3 m(L) - \mu_2)^2 + \mu_1.$$

Note that $m(L)$ is called the minimum of L and can be computed using an algorithm of Fincke and Pohst [22].

Proof. Suppose that $\jmath(P) \notin W$. Then $\jmath(P) = w + \phi(\mathbf{l})$ for some non-zero element $\mathbf{l} \in L$. In particular, if $\cdot$ denotes Euclidean norm then $\mathbf{l} \geq m(L)$.

We can write $M = N\Lambda N^t$ where N is orthogonal and Λ is the diagonal matrix with diagonal entries λ_i. Let $\mathbf{x} = \mathbf{l}N$ and write $\mathbf{x} = (x_1, \ldots, x_r)$. Then

$$\hat{h}(\phi(\mathbf{l})) = \mathbf{l}M\mathbf{l}^t = \mathbf{x}\Lambda\mathbf{x}^t \geq \mu_3^2\mathbf{x}^2 = \mu_3^2\mathbf{l}^2 \geq \mu_3^2 m(L)^2.$$

Now recall that $D \mapsto \sqrt{\hat{h}(D)}$ defines a norm on $J(\mathbb{Q}) \otimes \mathbb{R}$ and so by the triangle inequality

$$\sqrt{\hat{h}(\jmath(P))} \geq \sqrt{\hat{h}(\phi(\mathbf{l}))} - \sqrt{\hat{h}(w)} \geq \mu_3 m(L) - \mu_2.$$

The lemma now follows from (10.2). □

Remark. We can replace $\mu_3 m(L)$ with the minimum of L with respect to the height pairing matrix. This is should lead to a very slight improvement. Since in practice our lattice L has very large index, computing the minimum of L with respect to the height pairing matrix may require the computation of the height pairing matrix to very great accuracy, and such a computation is inconvenient. We therefore prefer to work with the Euclidean norm on $\mathbb{Z}^r$.

10.13 Proofs of Theorems 10.1.1 and 10.1.2

The equation $Y^2 - Y = X^5 - X$ is transformed into

$$C \quad : \quad 2y^2 = x^5 - 16x + 8, \tag{10.12}$$

via the change of variables $y = 4Y - 2$ and $x = 2X$ which preserves integrality. We shall work the model (10.12). Let C be the smooth projective genus 2 curve

Table 10.1:

coset of $J(\mathbb{Q})/2J(\mathbb{Q})$	κ	unit rank of K_i	bound R for regulator of K_i	bound for $\log x$
0	1	12	1.8×10^{26}	1.0×10^{263}
D_1	-2α	21	6.2×10^{53}	7.6×10^{492}
D_2	$4 - 2\alpha$	25	1.3×10^{54}	2.3×10^{560}
D_3	$-4 - 2\alpha$	21	3.7×10^{55}	1.6×10^{498}
$D_1 + D_2$	$-2\alpha + \alpha^2$	21	1.0×10^{52}	3.2×10^{487}
$D_1 + D_3$	$2\alpha + \alpha^2$	25	7.9×10^{55}	5.1×10^{565}
$D_2 + D_3$	$-4 + \alpha^2$	21	3.7×10^{55}	1.6×10^{498}
$D_1 + D_2 + D_3$	$8\alpha - 2\alpha^3$	25	7.9×10^{55}	5.1×10^{565}

with affine model given by (10.12), and let J be its Jacobian. Using MAGMA [5] we know that $J(\mathbb{Q})$ is free of rank 3 with Mordell–Weil basis given by

$$D_1 = (0, 2) - \infty, \qquad D_2 = (2, 2) - \infty, \qquad D_3 = (-2, 2) - \infty.$$

The MAGMA programs used for this step are based on Stoll's papers [45], [46], [47].

Let $f = x^5 - 16x + 8$. Let α be a root of f. We shall choose for coset representatives of $J(\mathbb{Q})/2J(\mathbb{Q})$ the linear combinations $\sum_{i=1}^{3} n_i D_i$ with $n_i \in \{0, 1\}$. Then

$$x - \alpha = \kappa \xi^2,$$

where $\kappa \in \mathcal{K}$ and $\mathcal{K}$ is constructed as in Lemma 10.3.1. We tabulate the κ corresponding to the $\sum_{i=1}^{3} n_i D_i$ in Table 10.1.

Next we compute the bounds for $\log x$ given by Theorem 10.9.1 for each value of κ. We implemented our bounds in MAGMA. Here the Galois group of f is S_5 which implies that the fields K_1, K_2, K_3 corresponding to a particular κ are isomorphic. The unit ranks of K_i, the bounds for their regulator as given by Lemma 10.5.1, and the corresponding bounds for $\log x$ are tabulated in Table 10.1.

A quick search reveals 17 rational points on C:

$$\infty,\ (-2, \pm 2),\ (0, \pm 2),\ (2, \pm 2),\ (4, \pm 22),\ (6, \pm 62),$$
$$(1/2, \pm 1/8),\ (-15/8, \pm 697/256),\ (60, \pm 9859).$$

Let W denote the image of this set in $J(\mathbb{Q})$. Applying the implementation of the Mordell–Weil sieve due to Bruin and Stoll which is explained in Section 10.10

we obtain that $\jmath(C(\mathbb{Q})) \subseteq W + BJ(\mathbb{Q})$ where

$$B = 4449329780614748206472972686179940652515754483274306796568214048000$$
$$= 2^8 \cdot 3^4 \cdot 5^3 \cdot 7^3 \cdot 11^2 \cdot 13^2 \cdot 17^2 \cdot 19 \cdot 23 \cdot 29 \cdot 31^2 \cdot \prod_{\substack{37 \le p \le 149 \\ p \neq 107}} p\,.$$

For this computation, we used "deep" information modulo 2^9, 3^6, 5^4, 7^3, 11^3, 13^2, 17^2, 19^2, and "flat" information from all primes $p < 50000$ such that $\#J(\mathbb{F}_p)$ is 500-smooth (but keeping only information coming from the maximal 150-smooth quotient group of $J(\mathbb{F}_p)$). Recall that an integer is called *A-smooth* if all its prime divisors are $\le A$. This computation took about 7 hours on a 2 GHz Intel Core 2 CPU.

We now apply the new extension of the Mordell–Weil sieve explained in Section 10.11. We start with $L_0 = B\mathbb{Z}^3$ where B is as above. We successively apply Lemma 10.11.1 using all primes $q < 10^6$ which are primes of good reduction and satisfy criteria I–IV of Section 10.11. There are 78498 primes less than 10^6. Of these, we discard 2, 139, 449 as they are primes of bad reduction for C. This leaves us with 78495 primes. Of these, Criterion I fails for 77073 of them, Criterion II fails for 220 of the remaining, Criterion III fails for 43 primes that survive Criteria I and II, and Criterion IV fails for 237 primes that survive Criteria I–III. Altogether, only 922 primes $q < 10^6$ satisfy Criteria I–IV and increase the index of L.

The index of the final L in $\mathbb{Z}^3$ is approximately 3.32×10^{3240}. This part of the computation lasted about 37 hours on a 2.8 GHZ Dual-Core AMD Opteron.

Let μ_1, μ_2, μ_3 be as in the notation of Lemma 10.12.1. Using MAGMA we find $\mu_1 = 2.677$, $\mu_2 = 2.612$ and $\mu_3 = 0.378$ (to 3 decimal places). The shortest vector of the final lattice L is of Euclidean length approximately 1.156×10^{1080} (it should be no surprise that this is roughly the cube root of the index of L in $\mathbb{Z}^3$). By Lemma 10.12.1 if $P \in C(\mathbb{Q})$ is not one of the 17 known rational points then

$$h(\jmath(P)) \ge 1.9 \times 10^{2159}.$$

If P is an integral point, then $h(\jmath(P)) = \log 2 + 2 \log x(P)$. Thus

$$\log x(P) \ge 0.95 \times 10^{2159}.$$

This contradicts the bounds for $\log x$ in Table 10.1 and shows that the integral point P must be one of the 17 known rational points. This completes the proof of Theorem 10.1.1. The proof of Theorem 10.1.2 is similar and we omit the details.

The reader can find the MAGMA programs for verifying the above computations at: http://www.warwick.ac.uk/staff/S.Siksek/progs/intpoint/

Bibliography

[1] È. T. Avanesov. Solution of a problem on figurate numbers. *Acta Arith.*, 12:409–420, 1966/1967.

[2] A. Baker. Bounds for the solutions of the hyperelliptic equation. *Proc. Cambridge Philos. Soc.*, 65:439–444, 1969.

[3] Yu. Bilu. Effective analysis of integral points on algebraic curves. *Israel J. Math.*, 90(1-3):235–252, 1995.

[4] Yuri F. Bilu and Guillaume Hanrot. Solving superelliptic Diophantine equations by Baker's method. *Compositio Math.*, 112(3):273–312, 1998.

[5] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[6] B. Brindza. On S-integral solutions of the equation $y^m = f(x)$. *Acta Math. Hungar.*, 44(1-2):133–139, 1984.

[7] B. Brindza. On a special superelliptic equation. *Publ. Math. Debrecen*, 39(1-2):159–162, 1991.

[8] N. Bruin and M. Stoll. The Mordell-Weil sieve: Proving non-existence of rational points on curves. *ArXiv e-prints*, June 2009.

[9] N. R. Bruin. *Chabauty methods and covering techniques applied to generalized Fermat equations*, volume 133 of *CWI Tract*. Stichting Mathematisch Centrum Centrum voor Wiskunde en Informatica, Amsterdam, 2002. Dissertation, University of Leiden, Leiden, 1999.

[10] Nils Bruin. Chabauty methods using elliptic curves. *J. Reine Angew. Math.*, 562:27–49, 2003.

[11] Nils Bruin and Noam D. Elkies. Trinomials $ax^7 + bx + c$ and $ax^8 + bx + c$ with Galois groups of order 168 and $8 \cdot 168$. In *Algorithmic number theory (Sydney, 2002)*, volume 2369 of *Lecture Notes in Comput. Sci.*, pages 172–188. Springer, Berlin, 2002.

[12] Nils Bruin and Michael Stoll. Deciding existence of rational points on curves: an experiment. *Experiment. Math.*, 17(2):181–189, 2008.

[13] Nils Bruin and Michael Stoll. Two-cover descent on hyperelliptic curves. *Math. Comp.*, 78(268):2347–2370, 2009.

[14] Yann Bugeaud. Bounds for the solutions of superelliptic equations. *Compositio Math.*, 107(2):187–219, 1997.

[15] Yann Bugeaud and Kálmán Győry. Bounds for the solutions of unit equations. *Acta Arith.*, 74(1):67–80, 1996.

[16] Yann Bugeaud, Maurice Mignotte, and Samir Siksek. Classical and modular approaches to exponential Diophantine equations. I. Fibonacci and Lucas perfect powers. *Ann. of Math. (2)*, 163(3):969–1018, 2006.

[17] J. W. S. Cassels and E. V. Flynn. *Prolegomena to a middlebrow arithmetic of curves of genus* 2, volume 230 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1996.

[18] B. M. M. de Weger. A binomial Diophantine equation. *Quart. J. Math. Oxford Ser. (2)*, 47(186):221–231, 1996.

[19] Benjamin M. M. de Weger. Equal binomial coefficients: some elementary considerations. *J. Number Theory*, 63(2):373–386, 1997.

[20] J.-H. Evertse and R. Tijdeman. Some open problems about diophantine equations. http://www.math.leidenuniv.nl/ evertse/07-workshop-problems.pdf.

[21] Daniel C. Fielder and Cecil O. Alford. Observations from computer experiments on an integer equation. In *Applications of Fibonacci numbers, Vol. 7 (Graz, 1996)*, pages 93–103. Kluwer Acad. Publ., Dordrecht, 1998.

[22] U. Fincke and M. Pohst. Improved methods for calculating vectors of short length in a lattice, including a complexity analysis. *Math. Comp.*, 44(170):463–471, 1985.

[23] E. V. Flynn. A flexible method for applying Chabauty's theorem. *Compositio Math.*, 105(1):79–94, 1997.

[24] E. V. Flynn. The Hasse principle and the Brauer-Manin obstruction for curves. *Manuscripta Math.*, 115(4):437–466, 2004.

[25] E. V. Flynn and N. P. Smart. Canonical heights on the Jacobians of curves of genus 2 and the infinite descent. *Acta Arith.*, 79(4):333–352, 1997.

[26] E. Victor Flynn and Joseph L. Wetherell. Finding rational points on bielliptic genus 2 curves. *Manuscripta Math.*, 100(4):519–533, 1999.

[27] E. Victor Flynn and Joseph L. Wetherell. Covering collections and a challenge problem of Serre. *Acta Arith.*, 98(2):197–205, 2001.

[28] Péter Kiss. On the number of solutions of the Diophantine equation $\binom{x}{p} = \binom{y}{2}$. *Fibonacci Quart.*, 26(2):127–130, 1988.

[29] E. Landau. Verallgemeinerung eines Pólyaschen satzes auf algebraische zahlkörper. 1918.

[30] D. A. Lind. The quadratic field $Q(\sqrt{5})$ and a certain Diophantine equation. *Fibonacci Quart.*, 6(3):86–93, 1968.

[31] 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.

[32] M. Mignotte and A. Pethő. On the Diophantine equation $x^p - x = y^q - y$. *Publ. Mat.*, 43(1):207–216, 1999.

[33] L. J. Mordell. On the integer solutions of $y(y+1) = x(x+1)(x+2)$. *Pacific J. Math.*, 13:1347–1351, 1963.

[34] A. Pethö and B. M. M. de Weger. Products of prime powers in binary recurrence sequences. I. The hyperbolic case, with an application to the generalized Ramanujan-Nagell equation. *Math. Comp.*, 47(176):713–727, 1986.

[35] Ákos Pintér. A note on the Diophantine equation $\binom{x}{4} = \binom{y}{2}$. *Publ. Math. Debrecen*, 47(3-4):411–415, 1995.

[36] Bjorn Poonen. Heuristics for the Brauer-Manin obstruction for curves. *Experiment. Math.*, 15(4):415–420, 2006.

[37] Bjorn Poonen and Edward F. Schaefer. Explicit descent for Jacobians of cyclic covers of the projective line. *J. Reine Angew. Math.*, 488:141–188, 1997.

[38] Dimitrios Poulakis. Solutions entières de l'équation $Y^m = f(X)$. *Sém. Théor. Nombres Bordeaux (2)*, 3(1):187–199, 1991.

[39] Edward F. Schaefer. 2-descent on the Jacobians of hyperelliptic curves. *J. Number Theory*, 51(2):219–232, 1995.

[40] Wolfgang M. Schmidt. Integer points on curves of genus 1. *Compositio Math.*, 81(1):33–59, 1992.

[41] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1992. Corrected reprint of the 1986 original.

[42] David Singmaster. Repeated binomial coefficients and Fibonacci numbers. *Fibonacci Quart.*, 13(4):295–298, 1975.

[43] Nigel P. Smart. *The algorithmic resolution of Diophantine equations*, volume 41 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1998.

[44] V. G. Sprindžuk. The arithmetic structure of integer polynomials and class numbers. *Trudy Mat. Inst. Steklov.*, 143:152–174, 210, 1977. Analytic number theory, mathematical analysis and their applications (dedicated to I. M. Vinogradov on his 85th birthday).

[45] Michael Stoll. On the height constant for curves of genus two. *Acta Arith.*, 90(2):183–201, 1999.

[46] Michael Stoll. Implementing 2-descent for Jacobians of hyperelliptic curves. *Acta Arith.*, 98(3):245–277, 2001.

[47] Michael Stoll. On the height constant for curves of genus two. II. *Acta Arith.*, 104(2):165–182, 2002.

[48] Michael Stoll. Finite descent obstructions and rational points on curves. *Algebra Number Theory*, 1(4):349–391, 2007.

[49] R. J. Stroeker and N. Tzanakis. Computing all integer solutions of a genus 1 equation. *Math. Comp.*, 72(244):1917–1933 (electronic), 2003.

[50] Roelof J. Stroeker and Benjamin M. M. de Weger. Elliptic binomial Diophantine equations. *Math. Comp.*, 68(227):1257–1281, 1999.

[51] Paul Voutier. An effective lower bound for the height of algebraic numbers. *Acta Arith.*, 74(1):81–95, 1996.

[52] Paul M. Voutier. An upper bound for the size of integral solutions to $Y^m = f(X)$. *J. Number Theory*, 53(2):247–271, 1995.

[53] J. L. Wetherell. *Bounding the Number of Rational Points on Certain Curves of High Rank*. PhD thesis, University of California at Berkeley, 1997.