Számtani sorozatok multiplikatív tulajdonságú halmazokban

MTA doktori értekezés

Hajdu Lajos

Debrecen, 2009

Tartalomjegyzék

Bevezetés

A számelmélet számtalan kérdése az egész számok additív illetve multiplikatív struktúrájával kapcsolatos. Ezek közül több érdekes, nehéz klasszikus probléma olyan összefüggésekre vonatkozik, ahol additív módon definiált objektumok multiplikatív tulajdonságaira vagyunk kíváncsiak, avagy éppen fordítva, multiplikatív eszközökkel meghatározott számok, halmazok bizonyos additív tulajdonságait firtatjuk. Az ilyen jellegű kérdések általában rendkívül nehezek, mivel igen laza a kapcsolat az egészek additív és multiplikatív struktúrája között. Tipikus példaként megemlíthetjük a híres Fermat-egyenletet, vagy akár a mindmáig megoldatlan ikerprím-problémát és a Goldbach-sejtést.

Disszertációnkban olyan eredményeket tárgyalunk, melyek multiplikatív módon definiált számhalmazokban található számtani sorozatokkal kapcsolatosak. Értekezésünk három fejezetből áll. Az első fejezetben n-edik hatványokból álló számtani sorozatokat vizsgálunk, illetve általánosabban számtani sorozatok tagjainak szorzataiban található teljes hatványokkal foglalkozunk. A második fejezetben a kérdéskör általánosításaként teljes (de nem feltétlenül azonos kitevőjű) hatványokból álló számtani sorozatokat vizsgálunk. Végül a harmadik fejezetben úgynevezett S-egységek összeghalmazaiban található számtani sorozatokkal foglalkozunk. Eredményeinknek több, egymástól meglehetősen távol álló, első ránézésre meglepőnek tűnő alkalmazását adjuk. Mindhárom fejezetben először az éppen vizsgált problémát illetve annak hátterét, irodalmát mutatjuk be. Ezek után a disszertációban szereplő legfontosabb eredményeink ismertetése következik. Mivel a tárgyalt témakörök a diofantikus számelmélet homlokterébe tartozó, sokak által vizsgált területek közé tartoznak, az eredmények irodalmi elhelyezésére különös hangsúlyt fektetünk.

A disszertációban szereplő eredményeket a következő kilenc (nyolc már megjelent, valamint egy közlésre elfogadott) publikációban közöltük: [FH01], [GyHP09], [BBGyH06], [HTT09], [H04], [BGyHT06], [H08], [H07], [BHP].

1. Számtani sorozatot alkotó n-edik hatványok

E terület alapkérdése a következő: adott $n \geq 2$ egész szám esetén milyen hosszú lehet egy n-edik hatványokból álló számtani sorozat? A kérdés Fermat és Euler munkásságáig nyúlik vissza (lásd [Di66], 440. és 635. oldal). Amint azt Fermat megfogalmazta majd Euler be is bizonyította, négy különböző négyzetszám nem alkothat számtani sorozatot. Ugyanakkor jól ismert, hogy

az

$$X^2 - 2Y^2 = -1$$

Pell-egyenlet végtelen sok X, Y egész megoldással rendelkezik. Így (mivel a megoldások nyilvánvalóan egy $1, Y^2, X^2$ alakú számtani sorozatot határoznak meg) eredeti kérdésünk négyzetszámok esetére megoldottnak tekinthető. A probléma általános $n \geq 3$ esetén egy X^n, Z^n, Y^n alakú számtani sorozatból kiindulva az

$$X^n + Y^n = 2Z^n \tag{1}$$

diofantikus egyenlet megoldásainak meghatározására vezet. Nyilván elég azzal az esettel foglalkozni, amikor X, Y, Z relatív prímek. Az (1) egyenletet többen vizsgálták. Az $n = 3$ eset már Mordell klasszikus könyvében ([Mo69], 126. oldal) szerepel, míg az $n = 5$ kitevő vizsgálata egészen Dirichlet és Lebesgue bizonyos eredményeiig nyúlik vissza (lásd [Di66], 735. és 738. oldal). Az első általánosabb érvényű eredmény Dénes [De52] nevéhez fűződik, akinek $n \leq 31$ esetén sikerült (1)-et teljesen megoldania. Valamennyi említett esetben az adódott, hogy az egyenlet csupán az $|XYZ| \leq 1$ feltételnek eleget tevő megoldásokkal rendelkezik. Az (1) egyenletet végül a közelmúltban Darmon és Merel [DM97] oldotta meg teljes általánosságban. Azt nyerték, hogy az egyenlet bármely $n \geq 3$ kitevő esetén csak a már említett $|XYZ| \leq 1$ feltételt teljesítő megoldásokkal bír. Darmon és Merel bizonyításának hátterében a Fermat-egyenlet megoldása során a Wiles [W95] és mások által kidolgozott moduláris módszer áll. Megemlítjük, hogy az (1) egyenlet megoldása a Fermat-egyenlet megoldásánál lényegesen nehezebb, a nemtriviális $(X, Y, Z) = (1, 1, 1)$ megoldás létezése miatt ugyanis a moduláris technika alkalmazása komoly nehézségekbe ütközik.

Az alapkérdés általánosításaként, egy önmagában is érdekes és szerteágazó problémakör kiindulópontjaként tekintsük az

$$x(x + d) \dots (x + (k - 1)d) = by^n \tag{2}$$

diofantikus egyenletet, ahol x, d, k, b, y, n ismeretlen pozitív egészek, melyekre $k, n \geq 2$, $\text{lnko}(x, d) = 1$ és $P(b) \leq k$ teljesül. Itt $P(b)$ a b legnagyobb prímosztóját jelöli; $P(1) = 1$. Az egyenlettel rengeteg matematikus foglalkozott, ezen a ponton csupán Fermat, Euler, Erdős, Selfridge, Obláth, Nesterenko, Shorey, Tijdeman, Saradha, Győry, Brindza, Ruzsa, Bennett, Pintér nevét említjük. A későbbiekben majd eredményeket és hivatkozásokat is megfogalmazunk.

Egyszerű, de a későbbiekben rendkívüli jelentőséggel bíró észrevételként megállapíthatjuk, hogy $\text{lnko}(x, d) = 1$ miatt (2)-ből

$$x + id = a_i x_i^n \tag{3}$$

adódik, ahol a_i négyzetmentes és $P(a_i) \leq k$ $(i = 0, 1, \ldots, k-1)$. Ez az észrevétel azért is érdekes, mert úgy is értelmezhető, hogy az egyenlet megoldása során „majdnem" teljes hatványokból álló számtani sorozatokhoz jutunk: a sorozat tagjai egy teljes hatvány és egy korlátos, csupán „kis" prímekkel osztható együttható szorzataként állnak elő. Így (2) valóban a korábban említett probléma általánosításának tekinthető.

A (2) egyenlet kiinduló esete természetes módon a $d = 1$ választás. Ha a $b = 1$ értéket is rögzítjük, akkor egy szép, klasszikus kérdéshez jutunk: lehet-e egymást követő pozitív egészek szorzata teljes hatvány? Az $n = 2$ esetben Erdős [Er39] és Rigge [Rig39] egymástól függetlenül nemleges választ adtak erre a kérdésre. A probléma teljes megoldása Erdős és Selfridge [ES75] nevéhez fűződik, akik belátták, hogy a (2) egyenletnek (a $d = b = 1$ esetben) nincs megoldása. Egy másik természetes kérdés az egyenlet $d = 1$, $b = k!$ esetén történő vizsgálata. Ekkor ugyanis (2)

$$\binom{x+k-1}{k} = y^n \tag{4}$$

alakra hozható, azaz teljes hatványokat keresünk a binomiális együtthatók körében. Itt a binomiális együttható szimmetriája miatt elegendő az $x > k$ esettel foglalkoznunk. Feltesszük továbbá, hogy $n = 2$ esetén $k > 2$ teljesül. Az $n = k = 2$ választásnál ugyanis (4) (régóta ismert módon) egy végtelen sok megoldással rendelkező Pell-egyenletre vezet. A (4) egyenletet Erdős [Er51] $k \geq 4$ esetén teljesen megoldotta. A $k = 2, 3$ esetek azonban Erdős elemi kombinatorikus számelméleti megfontolásokon alapuló, rendkívül szellemes módszerével nem voltak kezelhetők. Tijdeman [Ti89] a Baker-módszer segítségével megmutatta, hogy ezekben az esetekben $\max(x, y, n)$ egy effektív módon meghatározható abszolút konstanssal korlátozható. Végül a problémát Darmon és Merel [DM97] fent említett eredménye segítségével Győry [Gy97] oldotta meg, megmutatva, hogy a (4) egyenlet egyetlen megoldása $(x, k, y, n) = (48, 3, 140, 2)$. Végül a $d = 1$ eset lezárásaként megemlítjük, hogy Saradha [Sa97] $(k \geq 4$ eset) és Győry [Gy98] $(k = 2, 3$ eset) a $P(b) \leq k$ általános feltétel mellett a (2) egyenletet teljesen megoldotta. Egyetlen megoldásként $P(y) > k$ esetén a már említett $(x, k, y, n) = (48, 3, 140, 2)$ adódott. (A $P(y) > k$ feltétel nélkül az egyenlet végtelen sok, könnyen jellemezhető triviális megoldással bír.)

A $d > 1$ eset szintén hatalmas, messzire visszanyúló irodalommal rendelkezik: elég csupán Fermat és Euler már említett eredményére gondolnunk. Valóban, annak igazolásához, hogy négy különböző négyzetszám nem alkothat számtani sorozatot, Euler valójában (a kérdés általánosításaként) az

$$x(x+d)(x+2d)(x+3d) = y^2$$

egyenletet vizsgálta - amely nem más, mint (2) a $k = 4$, $n = 2$, $b = 1$ választások mellett. Euler megmutatta, hogy a fenti diofantikus egyenletnek nincs x, y, d pozitív egészekben megoldása. Már ezen a ponton megemlítjük, hogy a (2) egyenlet $d > 1$ értékeire történő teljes megoldása e pillanatban még nagyon távolinak tűnik. Az általános eset ugyanis lényegesen, minőségileg nehezebb a $d = 1$ speciális esetnél. Ez jól szemléltethető például (3) segítségével. Ha $d = 1$, akkor a szóbanforgó számtani sorozat i-edik és j-edik $(i \neq j)$ tagjainak különbségét képezve egy

$$AX^n - BY^n = C \tag{5}$$

alakú, úgynevezett binom Thue-egyenlethez jutunk, ahol $A = a_i$, $B = a_j$, $X = x_i$, $Y = x_j$, $C = i - j$. Az egyenlet régóta ismert. Baker [Bak68] valamint Schinzel és Tijdeman [ScTi76] a Baker-módszer segítségével nyert eredményeiből következik, hogy $n \geq 3$ és $|Y| > 1$ esetén (5)-ben $\max(|X|, |Y|, n)$ egy csak A, B, C értékétől függő, effektív módon meghatározható konstanssal korlátozható. Megemlítjük, hogy az A, B, C együtthatókra vonatkozó bizonyos feltételek mellett a közelmúltban az (5) egyenlet összes megoldását sikerült meghatározni; lásd például [BGyMP06], [GyP08], [BMS08], [BBGyP].

Ezzel szemben, ha $d > 1$ tetszőleges ismeretlen egész, akkor egy (5)-höz hasonló összefüggés levezetéséhez két tag helyett **három** tagot, mondjuk az i_1, i_2, i_3 indexű tagokat kell használnunk, ahol $0 \leq i_1 < i_2 < i_3 < k$. Mivel egy számtani sorozattal van dolgunk, könnyen ellenőrizhető, hogy (3) alapján ekkor

$$AX^n + BY^n = CZ^n \tag{6}$$

teljesül, ahol $X = x_{i_1}^n$, $Y = x_{i_3}^n$, $Z = x_{i_2}^n$, $A = i_3 - i_2$, $B = i_2 - i_1$, $C = i_3 - i_1$. Azonban (6) egy, az (5) egyenletnél lényegesen nehezebb úgynevezett ternér egyenlet, melynek például a Fermat-egyenlet (lényegében a legegyszerűbb) speciális esete. A (6) egyenlet tetszőleges n-re való kezeléséhez az (éppen a Fermat-egyenlet megoldása során Wiles [W95] és mások által kifejlesztett) úgynevezett moduláris módszer szükséges. Ezen a ponton e módszerről még nem szólunk részletesen, erre a későbbiekben kerül majd sor. Csupán megemlítjük, hogy a (6) típusú egyenletek hátterében álló mély problémák miatt (2) teljes megoldása a jelenlegi ismeretekre támaszkodva egyelőre áthidalhatatlannak tűnő nehézségekbe ütközik.

A (2) egyenlettel kapcsolatos kutatások lényegében két fő irányban folynak: az egyenlet megoldásaira vonatkozó végességi tételek levezetése (bizonyos paraméterekre vonatkozó korlátok igazolása más paraméterek függvényében); illetve (2) teljes megoldása bizonyos paraméterek rögzítése után. A jelen disszertációban az utóbbi irányba tartozó eredményekről szólunk. Az

elsőként említett kutatási irány legfontosabb eredményeit illetve más kapcsolódó eredményeket többek között a [Ti76a], [ShTi97], [Ti98], [Gy99], [Sh02] áttekintő cikkekben találhatunk.

Általánosságban elmondható, hogy a (2) egyenlet bizonyos esetekben való teljes megoldását az algebrai görbeelmélet közelmúltbeli jelentős fejlődése, és az új eredmények hatékony alkalmazási lehetőségeinek kidolgozása tette lehetővé. Ezen belül, a már említett moduláris módszer mellett különösen fontos szerep jut az elliptikus görbék (1 génuszú görbék) illetve a magasabb génuszú görbék, valamint a rájuk vonatkozó eredmények alkalmazásainak. Az ilyen típusú görbék elsősorban kis kitevők (azaz a (2) egyenletben tipikusan $n = 2, 3$ esetén) bizonyulnak rendkívül hasznosnak. Megemlítjük, hogy az elliptikus görbéknek a problémakörben való első alkalmazása az [FH01] cikkünkben történt, míg a 2 génuszú görbék használatára illetve ehhez kapcsolódóan az ún. Chabauty-módszer alkalmazására (lásd [C41], [F97], [Br03] valamint az utóbbi két cikkben szereplő hivatkozásokat) (2) vonatkozásában először a [BBGyH06] dolgozatunkban került sor.

Elsőként bemutatandó konkrét eredményként a (2) egyenlet teljes megoldásának lehetőségeit tárgyaljuk $n = 2$ és tetszőleges, de rögzített d esetén. Megemlítjük, hogy (mint azt több, a későbbiekben bemutatandó hivatkozás is igazolja) az $n = 2$ eset különleges figyelmet érdemel. Ennek oka abban keresendő, hogy ekkor több olyan eszköz is rendelkezésre áll, melyek nagyobb kitevőkre nem használhatók. Mivel ennek a megfordítása is igaz (azaz a nagyobb n kitevőkre használható módszerek $n = 2$-re sokszor csődöt mondanak), így elmondható, hogy ez az eset valóban különös jelentőséggel bír.

1.1. A (2) egyenlet teljes megoldása rögzített d és $n = 2$ esetén

Az $n = 2$ esetben rögzített d mellet lehetőség nyílik (2) teljes megoldására. Ehhez elméleti szempontból a legjobb kiindulópontot Shorey és Tijdeman [ShTi90] egy eredménye jelenti, mely szerint ebben az esetben k értéke már d prímosztói számának segítségével is korlátozható. (A korábbi hasonló eredmények áttekintésért lásd [ShTi90].) Ez azonban önmagában még messze nem elegendő a (2) egyenlet teljes megoldásához. Az első, (2) összes megoldását szolgáltató eredményt Saradha [Sa98] nyerte $d \leq 22$ esetén. Saradha eredménye lényegében Erdős és Selfridge [ES75] a $d = 1$ esetre vonatkozó kombinatorikus eredményének a $d > 1$ esetre történő adaptálásával történt. Ezen kívül elmondható, hogy Saradha kombinatorikus-prímszámelméleti módszere heurisztikus elemeket is tartalmaz, elvileg nincs arra garancia, hogy az eljárás valóban működik tetszőleges d esetén is. Az [FH01] cikkben egy újszerű, mo-

dern eszközökön alapuló, minden esetben hatékonyan működő eljárást adtunk (2) összes megoldásának meghatározására rögzített d és $n = 2$ mellett. A módszer lényege annak észrevételén múlik, hogy (3) alapján a szóban forgó számtani sorozat bármely három, mondjuk az i_1, i_2, i_3 indexű tagjait összeszorozva egy

$$(x + i_1 d)(x + i_2 d)(x + i_3 d) = cz^2 \tag{7}$$

alakú egyenlethez jutunk. Itt $c = a_{i_1} a_{i_2} a_{i_3}$ és $z = x_{i_1} x_{i_2} x_{i_3}$ teljesül. Rögzített d esetén (7) egy elliptikus egyenlet, melynek x, z egész megoldásait keressük. Ehhez egy Lang [L64], [L78] és Zagier [Za87] által megalapozott, Gebel, Pethő, Zimmer [GPZ94] illetve tőlük függetlenül Stroeker és Tzanakis [StTz94] által kidolgozott eljárást érdemes követnünk, mely az egyenlet racionális megoldásai által meghatározott algebrai struktúra, az úgynevezett Mordell-Weil csoport tulajdonságain alapszik. Az eljárás jól algoritmizálható, és a SIMATH [Sm93] majd később a MAGMA [BCP97] programcsomagban implementálásra is került. Így ezen programcsomagok felhasználásával (legalábbis elviekben) egy adott elliptikus egyenlet összes egész megoldása meghatározható.

A fentiek ismeretében a (2) egyenlet $n = 2$ és rögzített d esetén történő teljes megoldására általunk [FH01] adott algoritmus vázlata a következő. Mivel d rögzített, így k értéke korlátozható: az első ilyen jellegű eredmény Marszalek [Mar85] nevéhez fűződik, mi konkrétan Saradha [Sa98] idevágó eredményeit használtuk. Emiatt (3) alapján, mivel a_i négyzetmentes és $P(a_i) \leq k$ $(i = 0, 1, \ldots, k-1)$, valójában csupán véges sok (7) alakú egyenletet kell megoldanunk. Az egyenletek megoldása a fent ismertetett módon történhet. Megemlítendő, hogy ha a k értékére kapott korlát túl nagy, akkor a fellépő elliptikus egyenletek óriási száma gyakorlati szempontból kezelhetetlenné teszi a problémát. Részben éppen ez jelentette [BHR00] motivációját: az itt (bizonyos feltételek mellett) levezetett $k \leq 7$ igen éles korlát az ismertetett eljárás hatékony működésének egyik elméleti sarokpontja. Módszerünk illusztrálásaként [FH01]-ben az egyenletet $23 \leq d \leq 30$ esetén teljesen megoldottuk, és az alábbi eredményt nyertük.

1. Tétel ([FH01]) *A* (2) *egyenlet összes megoldása* $23 \leq d \leq 30$ *és* $n = 2$ *esetén:*

$$(x, d, k, b, y) = (2, 23, 3, 6, 20), (4, 23, 3, 6, 30), (75, 23, 3, 6, 385),$$

$$(98, 23, 3, 2, 924), (338, 23, 3, 3, 3952), (3675, 23, 3, 6, 91805),$$

$$(75, 23, 4, 6, 4620), (1, 24, 3, 1, 35).$$

Itt valójában nem maga a konkrét tétel az érdekes (azt csak a teljesség kedvéért fogalmaztuk meg), sokkal inkább az alkalmazott módszer bír nagy jelentőséggel. Eljárásunkat többek között az [SS03a], [SS03b], [MS04] cikkek is átvették illetve részben továbbfejlesztették, így az a konkrét problémakörben is több alkalmazást nyert. (Például [SS03a]-ban a szerzők módszerünk továbbfejlesztésével az 1. Tételt kiterjesztették a $d \leq 104$ esetre.) Ugyanakkor fontos megemlítenünk, hogy az általunk bevezetett új eszköz, azaz az elliptikus görbék használata az éppen tárgyalt problémán messze túlmutat. Erről a későbbiekben még részletesebben szólunk majd. Most csupán azt említjük meg, hogy (2)-ben az általános n kitevők esetén felhasználható moduláris módszer a „kis" kitevőkre (pontosabban tipikusan $n = 2, 3, 5$ esetén) nem működik. Ezekben az esetekben a probléma megoldásához más eszközök használatára van szükség. Az $n = 2, 3$ esetben az egyik ilyen eszközt éppen az elliptikus egyenletek a fentiekhez hasonló vagy annál általánosabb használata jelenti.

1.2. A (2) egyenlet teljes megoldása rögzített k esetén

A (2)-re vonatkozó egyik legtermészetesebb kérdés a következő: oldjuk meg az egyenletet rögzített k tagszám esetén! Az irodalomban számos ez irányú eredmény található, lásd például Euler már említett, vagy Obláth [Ob50], [Ob51] tételeit. Ezek az eredmények azonban csupán speciális, fix n kitevőkre (nevezetesen $n = 2, 3$ esetére) vonatkoznak. A moduláris módszer megjelenésével lehetővé vált az egyenlet rögzített k esetén történő teljes megoldása, tetszőleges ismeretlen n kitevő mellett. A moduláris módszer alkalmazhatóságát a tekintett problémára a (3) összefüggés teszi lehetővé: ez alapján bármely három különböző tag megfelelő lineáris kombinációját tekintve egy (6) alakú, úgynevezett (n, n, n) szignatúrájú ternér egyenlethez jutunk. Felhasználva Wiles [W95], Darmon és Merel [DM97] valamint Ribet [Rib97] erdményeit, ahol $A = B = 1$ mellett C értéke rendre 1, 2 és 2^α, Győry [Gy99] megmutatta, hogy a (2) egyenletnek $k = 3$ és $P(b) \leq 2$ esetén nincs megoldása. A későbbiekben (általánosabb ternér egyenletekre vonatkozó, az alábbiakban bemutatandó eredmények segítségével) Győryvel és Saradhával [GyHS04] sikerült kiterjesztenünk az eredményt a $k = 4, 5$ esetre is.

A jelen értekezésben tárgyalt ez irányú fő eredményünk a következő.

2. Tétel. ([GyHP09]) *Ha $3 < k < 35$ és $b = 1$, akkor a (2) egyenletnek nincs megoldása.*

Más szavakkal, $3 < k < 35$ esetén egy k-tagú primitív (az $\text{lnko}(x, d) = 1$ feltételnek eleget tevő) számtani sorozat tagjainak szorzata nem lehet teljes hatvány.

Ez az eredmény az alábbi, általánosabb tételek következményeként adódik. Megemlítjük, hogy a felsorolt eredmények, pontosabban a 3-7. Tételek valójában az $x < 0, y < 0$ esetet is lefedik. Ezekben az állításokban (a többi korábbi feltétel változatlanul hagyása mellett) x és y tetszőleges nemnulla egészek lehetnek. Első eredményünk a $k \leq 11$ esetre vonatkozik.

3. Tétel. ([BBGyH06]) *Legyenek k és n olyan egészek, melyekre $3 \leq k \leq 11$, $n \geq 2$ prím és $(k, n) \neq (3, 2)$ teljesül. Tegyük fel továbbá, hogy x olyan egész, valamint d és b olyan pozitív egészek, hogy $\mathrm{lnko}(x, d) = 1$ és $P(b) \leq P_{k,n}$, ahol $P_{k,n}$ értékeit az alábbi táblázat tartalmazza:*

k	$l = 2$	$l = 3$	$l = 5$	$l \geq 7$
3	–	2	2	2
4	2	3	2	2
5	3	3	3	2
6	5	5	5	2
7	5	5	5	3
8	5	5	5	3
9	5	5	5	3
10	5	5	5	3
11	5	5	5	5

Ekkor a (2) egyenlet megoldásaira

$$(x, d, k) \in \{(-9, 2, 9), (-9, 2, 10), (-9, 5, 4), (-7, 2, 8), (-7, 2, 9), (-6, 1, 6), (-6, 5, 4), (-5, 2, 6), (-4, 1, 4), (-4, 3, 3), (-3, 2, 4), (-2, 3, 3), (1, 1, 4), (1, 1, 6)\}$$

teljesül.

Az egyszerűség kedvéért csupán a megoldásokban előforduló x, d, k értékeket adtuk meg; a hozzájuk tartozó b, y, n értékek (2)-ből könnyen kiszámolhatók.

Amint azt korábban is említettük, a 2. Tétel (illetve a kapcsolódó általánosabb eredmények) bizonyítása során érdemes megkülönböztetni az $n \geq 7$, $n = 5$, $n = 3$ és $n = 2$ eseteket. Ennek oka az, hogy az egyes esetek tárgyalása eltérő módszereket igényel. Az $n \geq 7$ eset lényegében egy, a moduláris technikán alapuló megközelítéssel kezelhető. Az $n = 5$ kitevőértékhez tartozó eset klasszikus algebrai számelméleti eredmények segítségével tárgyalható. Az $n = 3$ és $n = 2$ esetben több módszer ötvözése hozza meg a kívánt eredményt: a bizonyítások többek között a Chabauty-módszeren, az elliptikus egyenletek elméletén, illetve lokális vizsgálatokon alapulnak. A későbbiekben a bizonyítások hátterében álló módszerekről részletesebben is szólunk majd.

Az alábbiakban eszerint a felosztás szerint haladunk, a 3. Tétel által nem lefedett $12 < k < 35$ értékekre szorítkozva. A következő tételünk az $n \geq 7$ esetre vonatkozik.

4. Tétel. ([GyHP09]) *Ha $n \geq 7$ prím, $12 \leq k < 35$ és $P(b) \leq P_{k,n}$ teljesül, ahol*

$$P_{k,n} = \begin{cases} 7, & \text{ha } 12 \leq k \leq 22, \\ \frac{k-1}{2}, & \text{ha } 22 < k < 35, \end{cases}$$

akkor a (2) egyenletnek nincs megoldása.

Következő eredményünk az $n = 5$ esetet tárgyalja. Megemlítjük, hogy $8 \leq k \leq 11$ esetén az 5. Tétel a 3. Tétel javítását is szolgáltatja.

5. Tétel. ([GyHP09]) *Legyen $n = 5$, $8 \leq k < 35$ és $P(b) \leq P_{k,5}$, ahol*

$$P_{k,5} = \begin{cases} 7, & \text{ha } 8 \leq k \leq 22, \\ \frac{k-1}{2}, & \text{ha } 22 < k < 35. \end{cases}$$

Ekkor a (2) egyenlet megoldásaira az alábbiak egyike teljesül:

$$(k,d) = (8,1),\ x \in \{-10,-9,-8,1,2,3\}, \quad (k,d) = (8,2),\ x \in \{-9,-7,-5\},$$
$$(k,d) = (9,1),\ x \in \{-10,-9,1,2\}, \quad (k,d) = (9,2),\ x \in \{-9,-7\},$$
$$(k,d) = (10,1),\ x \in \{-10,1\}, \quad (k,d,x) = (10,2,-9).$$

Az alábbi két tételünk az $n = 3$ esetre vonatkozik. Az első, $b = 1$ mellett megfogalmazott állítás valójában a második, általánosabb b értékekre vonatkozó eredmény következménye.

6. Tétel. ([HTT09]) *Legyen (x,d,k,y) a (2) egyenlet egy megoldása $n = 3$, $k < 39$ és $b = 1$ mellett. Ekkor*

$$(x,d,k,y) = (-4,3,3,2), (-2,3,3,-2), (-9,5,4,6), (-6,5,4,6).$$

7. Tétel. ([HTT09]) *Legyen (x,d,k,b,y) a (2) egy olyan megoldása, melyre $n = 3$, $k < 32$, és $P(b) < k$ ha $k = 3$ vagy $k \geq 13$. Ekkor (x,d,k) az alábbiak egyike:*

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

Hirata-Kohno, Laishram, Shorey és Tijdeman [HKLST07] megmutatta, hogy ha $3 < k < 110$ és $b = 1$, akkor a (2) egyenletnek $n = 2$ esetén nincs megoldása. (Valójában [HKLST07] és [Te08] alapján egy ennél lényegesen pontosabb állítás is megfogalmazható, amely a $P(b) \leq k$ esetet is lefedi, bizonyos k értékek mellett.) Amint az könnyen látható, a 2. Tételünk a 3-7. Tételeink és az $n = 2$ esetre vonatkozó említett állítás következménye.

A következőkben bemutatjuk a felsorolt tételek bizonyításának hátterét. Itt is a korábbi, az n kitevő különböző értékeihez tartozó felosztást követjük. Célunk az, hogy röviden ismertessük a legfontosabb felhasznált módszereket illetve azok alkalmazásának elveit. A részletes bizonyítások a megfelelő cikkekben találhatók. Elöljáróban csupán annyit említünk meg, hogy minden vizsgált esetben sikerült olyan korábban még nem használt módszert kifejlesztenünk, mely a probléma kezelése során igen hatékonynak bizonyult.

1.2.1. Az $n \geq 7$ eset

Ebben az esetben az egyenlet megoldását a Wiles [W95], Darmon és Merel [DM97] Kraus [K97], Ribet [Rib97] és mások által kifejlesztett moduláris technika teszi lehetővé. Értekezésünkben nem ismertetjük a módszer elméleti hátterét, sokkal inkább annak problémánkra való (távolról sem automatikus, több szempontból is új megközelítésmódot igénylő) alkalmazására koncentrálunk. A módszer tömör felvázolása, illetve általános diofantikus alkalmazási lehetőségeinek összegzése Bennett [Ben03] ismertető dolgozatában található.

A moduláris módszer alapvetően háromféle szignatúrájú ternér egyenlet kezelését teszi lehetővé, nevezetesen az alábbiakét:

$$(n, n, n) \text{ szignatúra}: \quad AX^n + BY^n = CZ^n,$$

$$(n, n, 3) \text{ szignatúra}: \quad AX^n + BY^n = CZ^3,$$

$$(n, n, 2) \text{ szignatúra}: \quad AX^n + BY^n = CZ^2.$$

Itt valamennyi esetben A, B, C rögzített prímosztókkal rendelkező nemnulla egészek, X, Y, Z pedig ismeretlen relatív prím egészek. Megemlítjük, hogy $A = B = C = 1$ esetén az első egyenlet éppen a Fermat-egyenlet. Már ezen a ponton felhívjuk a figyelmet két, a későbbiekben fontos szerepet játszó összefüggésre. Egyrészt, bár elvileg a fenti típusú egyenletek kezelhetők (és itt nem feltétlenül a megoldásukra, csupán azok számítógép segítségével történő vizsgálatára gondolunk), ám a gyakorlatban csak azok az egyenletek használhatók, melyek viszonylag alacsony szintű moduláris formákhoz tartoznak - azaz tipikusan azok, melyekben ABC csupán „kevés” és „kicsi” különböző prímosztóval rendelkezik. Másrészt, az elmélet alkalmazhatóságát nagyban

megkönnyíti (sőt sokszor csupán az teszi lehetővé), ha egy további információval is rendelkezünk: ismerjük az XY egy konkrét prímosztóját.

A módszer (2) egyenletre való alkalmazásának kiindulópontja a (3) összefüggés. Az alapelv (meglehetősen leegyszerűsítve) a következő: az összes (3) alakú számtani sorozatot megvizsgálva a (2) egyenlet összes megoldását megkapjuk. Ha k értéke „kicsi" (mondjuk $k \leq 11$), akkor egy meglehetősen komplikált, de alapvetően szisztematikus vizsgálat is használható - lényegében ez történt a [BBGyH06] publikációnkban. Amint azt a (6) alakú egyenletek levezetésénél láthattuk, a (2) egyenletből kiindulva (n, n, n) szignatúrájú ternér egyenletek levezetése nem okoz gondot. Az ilyen egyenletek megoldása viszont már lényegesen nagyobb nehézségekbe ütközik: összességében elmondható, hogy az irodalomban csupán néhány (n, n, n) szignatúrájú ternér egyenlet teljes megoldása szerepel; lásd például [W95], [DM97], [K97], [Rib97], [SS01]. A meglévő eredmények problémánkra jól használhatók, de önmagukban messze nem elegendőek. Viszont olyan új, (n, n, n) szignatúrájú egyenletekre vonatkozó eredményt, amely a problémánk megoldása során jól alkalmazható, nehéz levezetni. Ennek fő oka az, hogy nem tudjuk garantálni, hogy a kapott egyenletben $p \mid XY$ teljesülne valamilyen adott p prímszámmal. Az áttörést az $(n, n, 2)$ szignatúrájú egyenletek alkalmazása hozza. Ilyen típusú egyenletek (3)-ból a következő módon nyerhetők. Legyen $0 \leq i_1 < i_2 \leq i_3 < i_4 < k$ úgy, hogy $i_2 + i_3 = i_1 + i_4$ teljesül. Ekkor fennáll a következő azonosság:

$$(n + i_2 d)(n + i_3 d) - (n + i_1 d)(n + i_4 d) = (i_2 i_3 - i_1 i_4) d^2.$$

Így (3) alapján egy

$$a_{i_2} a_{i_3} (x_{i_2} x_{i_3})^n - a_{i_1} a_{i_4} (x_{i_1} x_{i_4})^n = (i_2 i_3 - i_1 i_4) d^2 \tag{8}$$

alakú $(n, n, 2)$ szignatúrájú ternér egyenlethez jutunk. Az (n, n, n) szignatúrához képest a különbség abban rejlik, hogy itt már (az indexek „ügyes" megválasztásával) garantálható egy $p \mid XY$ típusú feltétel, és ezáltal a fellépő ternér egyenlet kezelhetővé válik, annak összes megoldása meghatározható.

A jelenséget egy példán keresztül illusztráljuk. Legyen $k = 4$, és vizsgáljuk a (2) egyenletet a $P(b) \leq 2$ feltétel mellett. Ekkor (3)-ban $P(a_i) \leq 3$ $(i = 0, 1, 2, 3)$ teljesül. Tegyük fel, hogy $3 \mid a_0$. Ekkor persze $3 \mid x$, így $\text{lnko}(x, d) = 1$ miatt $3 \nmid d$, valamint $3 \nmid (x + d)(x + 2d)$ teljesül. Mivel $P(b) \leq 2$, így azt kapjuk, hogy 3 kitevője $x(x + 3d)$-ben szükségképpen osztható n-nel. De akkor a (8) egyenletben, $i_1 = 0, i_2 = 1, i_3 = 2, i_4 = 3$ választás mellett 3 „beolvasztható" az $x_{i_1} x_{i_4}$ alapba, és így a fellépő ternér egyenletben végül is a $3 \mid XY$ feltételhez jutunk.

Az $(n, n, 2)$ szignatúrájú egyenletek első alkalmazására a [GyHS04] cikkünkben került sor. Itt azonban csupán az irodalomban található néhány

egyenletet (lásd például [BS04]) használtuk, melyek csak a $k = 4, 5$ esetek kezelését tették lehetővé. A későbbiek során, a [BBGyH06] dolgozatban számos új, a megoldások vizsgálata során fellépő $(n, n, 2)$ szignatúrájú egyenletet megoldva lehetővé vált az eredmény kiterjesztése a $k \leq 11$ esetre. Megemlítjük, hogy a probléma $k < 35$ esetén történő vizsgálatához a [GyHP09] dolgozatunkban még több $(n, n, 2)$ szignatúrájú egyenlet megoldása vált szükségessé - erről az alábbiakban részletesebben is szólunk majd.

Az eredmény továbbviteléhez lényeges újításra volt szükség. A k értékének növelésével ugyanis meg kell birkózni a kombinatorikus robbanás jelenségével: a (3) alapján (elméletileg) fellépő számtani sorozatok száma rendkívül gyorsan növekszik. Emiatt a korábban alkalmazott szisztematikus jellegű vizsgálat a gyakorlatban már nem használható. A [GyHP09] cikkünkben a nehézségek áthidalására sziták egy egymásra épülő rendszerét dolgoztuk ki. Ennek lényege (meglehetősen leegyszerűsítve) a következő. A számtani sorozatunk tagjainak $p \leq k$ prímosztóira az $\text{lnko}(x, d) = 1$ összefüggés miatt $p \mid (x + id), (x + jd)$ esetén $p \mid j - i$ teljesül. Így ha tudjuk, hogy egy ilyen p prím oszt egy $x + id$ tagot, akkor az összes p-vel osztható tagot fel tudjuk sorolni. (Ugyanakkor a k-nál nagyobb prímszámok nyilván csak egy tagot oszthatnak, n-nel osztható kitevőn szerepelve.) Az esetek vizsgálatánál először csak az 5-nél nagyobb prímszámok „helyeit" (azaz egy velük osztható tag indexét) rögzítsük. A „kimaradó" helyek (azaz azon tagok, melyek nem rendelkeznek 5-nél nagyobb prímosztóval) segítségével megpróbálhatunk olyan (n, n, n), $(n, n, 3)$ vagy $(n, n, 2)$ szignatúrájú ternér egyenlethez jutni, melynek megoldása az irodalomban már szerepel. A fennmaradó esetekben rögzítsük az 5, majd a 3, végül a 2 „helyét" - minden esetben hasonló vizsgálatokat folytatva. Végül a még mindig kimaradó esetekben próbáljunk meg levezetni olyan ternér egyenletet, mely korábban még nem volt megoldva, de kezelhető. Ez a lépés egyfajta iterációval történik: olyan ternér egyenleteket érdemes keresni és megoldani, melyek „sok" potenciális számtani sorozat létezését zárják ki egyszerre. Az ezen egyenletek segítségével sem kizárható sorozatok esetén keressünk további, hasonló jellegű ternér egyenleteket, stb. Végül a (2) egyenlet $k \leq 34$ esetén történő megoldásához összesen 55 darab $(n, n, 2)$ szignatúrájú egyenlet megoldására került sor, mindegyik esetben egy további $p \mid XY$ ($p \in \{11, 13, 17, 19, 23, 29, 31\}$) feltétel mellett. Megemlítjük, hogy ez összesen körülbelül kétszer annyi új egyenlet megoldását jelentette, mint amennyi az általunk felhasznált irodalomban szerepelt. A módszer jellege miatt bizonyos n kitevők egy-egy konkrét ternér egyenlet megoldásánál „kimaradtak": néhány $AX^n + BY^n = CZ^2$ alakú egyenletet sokszor csak egy $n \notin N$ feltétel mellett sikerült megoldanunk, ahol N egy véges, jellemzően „kevés" és „kicsi" elemekből álló halmaz. Az N-beli n kitevőket külön vizsgálatok segítségével (tipikusan lokális számítások alapján) sikerült ke-

zelnünk.

Az eredmény jelentősége nem csupán annyi, hogy sikerült viszonylag nagy k értékekre is megoldani a (2) egyenletet. A bizonyítás során feltárt összefüggések reményeink szerint a későbbiekben egy még általánosabb eredmény levezetésében is fontosak lehetnek. Mivel jelenleg csupán találgatni tudunk, egyetlen konkrét tényre szeretnénk felhívni a figyelmet: a vizsgált számtani sorozatok **mindegyike** esetében sikerült alacsony szintű ternér egyenletet találnunk. E tapasztalati megfigyelés valamilyen elméleti tétel formájába való öntése rendkívül nagy jelentőséggel bírna.

1.2.2. Az $n = 5$ eset

Ebben az esetben mind a [BBGyH06] mind a [GyHP09] cikkeinkben eredményeink az $AX^5 + BY^5 = CZ^5$ alakú egyenletekre vonatkozó tételeken alapulnak. Így többek között felhasználtuk Dirichlet, Lebesgue, Maillet (lásd [Di66]) és Dénes [De52] klasszikus eredményeit az $A = B = 1$ esetben, illetve Saradha és Shorey [SS01] bizonyos tételeit $C = 1$ esetén. Ezeken túl több új eredmény levezetésére is szükségünk volt. Kiterjesztettük például Dirichlet és Dénes említett eredményeit a $P(C) \leq 7$ esetre (a korábbiakban csupán a $P(C) \leq 3$ esetekkel foglalkoztak). Eredményeinket klasszikus algebrai számelméleti eszközök kombinálásával, valamint lokális vizsgálatok segítségével bizonyítottuk. A részletek a [BBGyH06], [GyHP09] cikkeinkben találhatók.

1.2.3. Az $n = 3$ eset

Viszonylag kis k értékek esetén (azaz mondjuk $k \leq 11$ mellett) (3) alapján az esetek szisztematikus vizsgálata is célravezető volt (lásd [BBGyH06]). A szükséges hátteret Selmer [Se51] $AX^3 + BY^3 = CZ^3$ alakú egyenletekre vonatkozó eredményei, valamint a már említett Chabauty-módszer szolgáltatja. Nagyobb k értékekre azonban a fellépő esetek hatalmas száma miatt finomabb meggondolásokra van szükség. Ezért a [HTT09] cikkünkben bevezettünk egy modulo 7 és modulo 9 köbmaradékokon alapuló szitamódszert, amely jelentős mértékben megkönnyíti az esetek vizsgálatát. A fennmaradó lehetséges számtani sorozatokat Selmer [Se51] már említett eredményeivel, illetve a Cahabauty-módszerrel kezeltük. Az előbbi eszköz alkalmazása (3) alapján kézenfekvő, az utóbbi használatát egy példán illusztráljuk. Tegyük fel, hogy $k = 7$ és (3)-ban

$$(a_0, a_1, a_2, a_3, a_4, a_5, a_6) = (4, 5, 6, 7, 1, 9, 10)$$

teljesül. Mivel egy számtani sorozattal van dolgunk, így a

$$8x_6^3 + x_1^3 = 9x_5^3 \quad \text{és} \quad x_6^3 - 3x_1^3 = -2x_0^3$$

összefüggésekhez jutunk. Az első egyenletet faktorizálva könnyen látható, hogy $4x_6^2-2x_1x_6+x_1^2 = 3u^2$ teljesül valamilyen u egésszel. A második egyenlet bal oldalát a $K = \mathbb{Q}(\sqrt[3]{3})$ testben faktorizálva $x_6-\sqrt[3]{3}x_1 = (1-\sqrt[3]{3})v^3$ adódik, valamilyen K-beli v algebrai egésszel. A fenti összefüggésekből az

$$(X - \sqrt[3]{3})(4X^2 - 2X + 1) = (3 - 3\sqrt[3]{3})Y^3$$

egyenlethez jutunk, ahol $X = x_6/x_1$ illetve $Y = uv/x_1$. Mivel ez az egyenlet egy K feletti 1 génuszú görbét határoz meg, így ennek $(X, Y) \in \mathbb{Q} \times K$ megoldásai az elliptikus Chabauty-módszer segítségével meghatározhatók. Visszahelyettesítéssel kapjuk, hogy a megoldások az $x_1 = \pm 1$, $x_6 = \pm 1$ értékekhez tartoznak. A módszer részletesebb leírását lásd a [BBGyH06] és [HTT09] cikkeinkben.

1.2.4. Az $n = 2$ eset

Ebben az esetben a (3) egyenlet vizsgálatának egyik hatékony eszközét az elliptikus egyenletek jelentik. Mivel azonban most d nem rögzített, így a korábban [FH01]-ben alkalmazott technikánk átalakítására van szükség. Ennek a [BBGyH06] cikkünkben bevezetett új eljárásnak a bemutatásához válasszunk négy tagot a szóban forgó számtani sorozatból. Ekkor (3) alapján

$$X(X + j_1d)(X + j_2d)(X + j_3d) = BY^2$$

adódik. Itt (ha az i_1, i_2, i_3, i_4 indexű tagokat választottuk) $j_l = i_{l+1} - i_1$ ($l = 1, 2, 3$) és $X = x + i_1d$, illetve $B = a_1a_2a_3a_4$ valamint $Y = x_1x_2x_3x_4$ teljesül. Innen, felhasználva hogy $X \neq 0$, az $u = d/x$ és $v = Y/X^2$ helyettesítésekkel kapjuk, hogy

$$(1 + j_1u)(1 + j_2u)(1 + j_3u) = Bv^2,$$

ami egy elliptikus egyenlet. A probléma az, hogy itt u, v **racionális** számok lehetnek, így az egyenlet akár végtelen sok megoldással is rendelkezhet. Viszont ha az egyenlet (pontosabban a hozzá tartozó elliptikus görbe) Mordell-Weil csoportjának rangja nulla (amire a terület egy „folklór" sejtése alapján egy véletlenszerűen választott görbe esetében mintegy 40 százalék „esély" van), akkor a megoldások száma véges. Ezek a megoldások a görbe Mordell-Weil csoportjának torziópontjaihoz tartoznak, és standard matematikai programcsomagok (például a MAGMA [BCP97]) segítségével egyszerűen meghatározhatók. Így ebben az esetben a (2) egyenlet megoldásai is könnyen adódnak. A problémát elsősorban a potenciálisan fellépő (3) sorozatok (k értékével rendkívül gyorsan növekvő) nagy száma jelenti. Ez a nehézség azonban a megfelelő szitatechnikákkal, legalábbis $k \leq 11$ esetén, a [BBGyH06] cikkünkben kezelhetőnek bizonyult. Érdekes módon egy konkrét

esetben, nevezetesen $k = 6$ és $b = 5$ mellett valamennyi fellépő elliptikus görbe rangja pozitív. Ekkor az alábbi egyenlethez jutunk:

$$X(X+1)(X+2)(X+3)(X+4)(X+5) = 5Y^2,$$

ahol $X = x/d$ és $Y = y/d^3$. A fenti egyenlet egy 2 génuszú görbét határoz meg, melynek racionális pontjai (és így visszahelyettesítés után x, y, d értéke) a Chabauty-módszer segítségével meghatározható. Ezt az eredményt az iménti eljárással kombinálva a 3. Tétel $n = 2$ esetén történő bizonyításához jutunk.

Végül megemlítjük, hogy az említett [HKLST07]-beli eredmény bizonyítása részben más módszerrel (egy lokális megfontolásokon alapuló eljárással és a Chabauty-módszer segítségével) történt, mely elsősorban az $x > 0$ megoldások meghatározásakor tűnik hatékonynak, lásd a [HKLST07] és [Te08] cikkeket. (Valóban, az $x < 0$ esetet [HKLST07] nem tárgyalja.)

2. Számtani sorozatot alkotó vegyes hatványok

A (2) egyenlettel kapcsolatos eredmények (3) alapján úgy is interpretálhatóak, hogy olyan számtani sorozatokat keresünk, melyek „majdnem" teljes n-edik hatványokból állnak. Ebben a fejezetben egy általunk nyitott, de számos korábbi híres problémához és eredményhez kapcsolódó kutatási irányban nyert eredményeket mutatunk be. Tekintsük az

$$a_0 x_0^{n_0}, a_1 x_1^{n_1}, \ldots, a_{k-1} x_{k-1}^{n_{k-1}} \tag{9}$$

alakú számtani sorozatokat. Itt $a_i, x_i \in \mathbb{Z}$, $P(a_i) \leq P$ $(i = 0, \ldots, k-1)$ ahol P egy rögzített konstans, és az $n_i \geq 2$ hatványkitevők különbözőek is lehetnek. Az alapkérdés a következő: bizonyos természetes feltételek mellett korlátozható-e a (9) sorozat k hossza? Megemlítjük, hogy könnyen látható, hogy feltételek előírása nélkül k értéke nem korlátozható. Ezt az alábbi egyszerű példa segítségével illusztráljuk (mely a disszertációban is bemutatott [H04]-ben található). Két tetszőleges különböző $x_0^{n_0}$, $x_1^{n_1}$ teljes hatvány felfogható kéttagú számtani sorozatként. Induktívan gondolkodva tegyük fel, hogy

$$x_0^{n_0}, x_1^{n_1}, \ldots, x_{t-1}^{n_{t-1}}$$

egy t tagú számtani sorozat, valamilyen $t \geq 2$ mellett. Legyen $y = x_{t-1}^{n_{t-1}} + d$, ahol $d = x_1^{n_1} - x_0^{n_0}$ a sorozat differenciája. Vegyük észre, hogy ekkor az $N = n_0 \ldots n_{t-1}$ és $N_i = N/n_i$ $(i = 0, 1, \ldots, t-1)$ jelöléseket bevezetve

$$(x_0 y^{N_0})^{n_0}, (x_1 y^{N_1})^{n_1}, \ldots, (x_{t-1} y^{N_{t-1}})^{n_{t-1}}, y^{N+1}$$

egy teljes hatványokból álló $t+1$ tagú számtani sorozat. Így k értéke valóban nem korlátozható.

Amint azt a későbbiekben látni fogjuk, az n_i $(i = 0, 1, \ldots, k-1)$ kitevők illetve $\mathrm{lnko}(a_0x_0, a_1x_1)$ korlátozása esetén a helyzet merőben más jelleget ölt. Az eredmények bemutatása előtt azonban még szeretnénk rávilágítani két dologra. Egyrészt, a probléma nyilvánvalóan a homogén hatványok esetének egyfajta általánosításának tekinthető. A vegyes hatványokból álló számtani sorozatok problémaköre ugyanakkor lényegesen nehezebb az azonos hatványok eseténél. Ezt jól illusztrálja, hogy az itt használható egyik mély eszköz a (6)-hoz képest is jelentősen tovább általánosított Fermat-egyenletek, azaz az

$$AX^p + BY^q = CZ^r \tag{10}$$

alakú egyenletek elmélete, ahol A, B, C nemnulla egészek. A (10) alakú egyenletekre vonatkozó jelenlegi legjobb, Darmontól és Granville-től [DG95] származó eredmény azonban csupán rögzített p, q, r esetén (a szokásos $1/p + 1/q + 1/r > 1$ feltétel mellett) biztosít végességet, ráadásul csak ineffektív formában. (Szemben a már korábban említett, például (6)-ra vonatkozó eredményekkel, melyek tetszőleges n-re érvényesek.)

Másrészt, a nevezetes

$$X^p - Y^q = 1$$

Catalan-egyenlet megoldásai lényegében egy kettő hosszúságú, $d = 1$ differenciájú „vegyes" hatványokból álló számtani sorozatot alkotnak, így a felvetett probléma ehhez az egyenlethez is szorosan kapcsolódik. (A teljesség kedvéért megemlítjük, hogy a Catalan-egyenlet Tijdeman [Ti76b] egy tétele alapján csak véges sok, effektíve meghatározható megoldással rendelkezik. Az egyenlet teljes megoldása Mihăilescu [Mi04] nevéhez fűződik. Az egyetlen megoldás: $(X, Y, p, q) = (3, 2, 2, 3)$.)

Ebben a témakörben lényegében két különböző kutatási irány kezd körvonalazódni: a bizonyos feltételek mellett k-ra (illetve esetlegesen a sorozatok **számára**) vonatkozó korlátok levezetése, valamint bizonyos speciális esetekben az összes megfelelő tulajdonságú sorozat meghatározása. Először az első irányba sorolható eredményeinket mutatjuk be.

8. Tétel. ([H04]) *Legyen L egy rögzített egész, $L \geq 2$. Ekkor bármely olyan (9) alakú számtani sorozatra melyben $n_i \leq L$ $(i = 0, 1, \ldots, k-1)$, $k \leq C(P, L)$ teljesül, ahol $C(P, L)$ egy csak P és L értékétől függő konstans.*

Tételünk bizonyítása során többek között van der Waerden [vdW27] egy híres (ilyen típusú probléma vonatkozásában korábban nem alkalmazott), monokromatikus számtani sorozatokra vonatkozó tételét, illetve Euler valamint Darmon és Merel korábban említett eredményeit kombináltuk.

Megemlítjük, hogy [H04]-ben megmutattuk, hogy az *abc*-sejtés teljesülése esetén az $n_i \leq L$ feltételt az $\text{lnko}(a_0x_0, a_1x_1) = 1$ feltétellel helyettesítve, k a P egy függvénye segítségével korlátozható. Ezen a ponton célszerűnek tűnik az *abc*-sejtés pontos ismertetése. A sejtés szerint tetszőleges relatív prím pozitív egész a, b, c számok és ε pozitív valós szám esetén az $a + b = c$ összefüggésből

$$c \leq C(\varepsilon) \left(\prod_{p|abc} p \right)^{1+\varepsilon}$$

következik, ahol $C(\varepsilon)$ egy csupán ε-tól függő konstans. A sejtés egy gyengébb alakja Oesterlétől [Oe88] származik, fenti formájában először Masser [Mas85] fogalmazta meg. Az *abc* sejtésből rengeteg fontos eredmény levezethető, több vezető szaktekintély szerint a modern diofantikus számelmélet egyik legfontosabb sejtéséről van szó. Itt csupán az érdekesség kedvéért azt említjük meg, hogy egy [GyHS04]-beli eredményünk alapján az *abc*-sejtés fennállása esetén $k \geq 3$ és $n \geq 4$ mellett a (2) egyenlet csupán véges sok x, d, k, b, y, n megoldással rendelkezik (azaz itt minden további feltétel nélkül az **összes** paraméter korlátozható).

9. Tétel. ([BGyHT06]) *Legyen L egy rögzített egész, $L \geq 2$. Ekkor csak véges sok olyan* (10) *alakú számtani sorozat létezik, melyre $n_i \leq L$, $a_i = 1$ $(i = 0, 1, \ldots, k-1)$ és $\text{lnko}(x_0, x_1) = 1$ teljesül.*

E tételünk bizonyításában új eszközt jelent Darmon és Granville fent említett, az általánosított Fermat-egyenletre vonatkozó tétele. Megemlítjük, hogy a [BGyHT06] dolgozatban a 9. Tételt bizonyos egyéb feltételek mellett sikerült tetszőleges a_i együtthatók esetére is kiterjesztenünk.

A fentieken túl olyan eredményeket is sikerült nyernünk, melyek szerint egy (9) típusú számtani sorozat hossza a sorozat (lényegében) bármely tagjának ismeretében, illetve a d differencia segítségével is korlátozható.

10. Tétel. ([H08]) *Legyenek x és n olyan egészek, melyekre $|x| \geq 2$ és $n \geq 2$ teljesül. Ekkor létezik egy olyan, csak x és n értékétől függő $C(x, n)$ konstans, hogy bármely nemkonstans, x^n-et tartalmazó teljes hatványokból álló számtani sorozat hossza legfeljebb $C(x, n)$.*

A bizonyítás során a 8. Tételt különböző elemi aritmetikai megfontolásokkal kombináltuk. Megemlítjük, hogy a 10. Tételben az $x \neq 0$ feltétel szükséges, ugyanakkor $x = \pm 1$ esetén a probléma nyitott marad.

11. Tétel. ([H08]) *Tekintsünk egy olyan* (9) *alakú számtani sorozatot, ahol $a_i = 1$ $(i = 0, 1, \ldots, k-1)$. Jelölje d a sorozat differenciáját. Ekkor mindkét alábbi összefüggés fennáll:*

i) $k \leq \max(3.125 \log(d) - 1, 73)$,

ii) $k \leq \max(2(\omega(d)+1)(\log(\omega(d)+1)+\log\log(\omega(d)+1))-1,21)$,
ahol $\omega(d)$ *a* d *különböző prímosztóinak száma.*

Az utóbbi tétel jelentőségét és érdekességét a következő összefüggés mutatja. Mint azt már korábban említettük, a (2) egyenlettel kapcsolatos egyik legfontosabb kutatási irány a következő: rögzített d esetén korlátozzuk a többi ismeretlent! Shorey és Tijdeman [ShTi90] egy eredménye alapján bármely n esetén k egy csupán $\omega(d)$ értékétől függő konstans segítségével korlátozható. Bár (3) alapján itt a számtani sorozat tagjai csupán „majdnem" teljes hatványok, látható, hogy a 11. Tétel ezen eredmény egyfajta kiterjesztését jelenti a „vegyes" hatványok esetére.

A következőkben két olyan eredményünket ismertetjük, melyek bizonyos speciális, de érdekes esetekben az összes (9) alakú számtani sorozatot meghatározzák.

12. Tétel. ([BGyHT06]) *Tegyük fel, hogy egy* (9) *alakú számtani sorozatra* $k \geq 4$, $lnko(x_0, x_1) = 1$, $a_i = 1$ *és* $n_i \in \{2,3\}$ *teljesül minden* $i = 0,1,\ldots,k-1$ *esetén. Ekkor a sorozat a triviális* $1,1,\ldots,1$ *és* $-1,-1,\ldots,-1$ *sorozatok egyike.*

Ez az eredmény az Euler és Fermat valamint Mordell már említett, négyzetszámokból illetve köbszámokból álló számtani sorozatokról szóló tételeinek közös általánosítását jelenti. Az eredmény igazolásának fő eszközét a 2 génuszú görbék elmélete, illetve a Chabauty-módszer valamint ennek elliptikus változata adja. Megemlítjük, hogy a (disszertációban nem szereplő) [HT] dolgozatban bizonyos feltételek mellett az $n_i \in \{2,n\}$, $n_i \in \{3,n\}$, illetve $n_i \in \{2,5\}$ eseteket is kezelni tudtuk.

A fejezet utolsó eredményeként egy speciális sorozattal kapcsolatos tételt mutatunk be. Ehhez szükségünk van egy új fogalom bevezetésére. Egy

$$x_1^1, x_2^2, \ldots, x_i^i, \ldots$$

alakú számtani sorozatot hatványgazdag (első irodalombeli megjelenése alapján angolul kicsit félrevezetően „powerful") számtani sorozatnak nevezünk. Ha $\mathrm{lnko}(x_1,x_2) = 1$, akkor azt mondjuk, hogy a sorozat primitív. Boklan [Bo98] problémafelvetése után Robertson, illetve tőle függetlenül Elkies és mások (lásd [Ro00]) megmutatták, hogy egy hatványgazdag számtani sorozat hossza legfeljebb öt. Az alábbi eredmény ennél lényegesen pontosabb eredményt szolgáltat.

13. Tétel. ([H08]) *Az egyetlen öttagú primitív hatványgazdag számtani sorozat a triviális* $1,1,1,1,1$ *sorozat. Ugyanakkor végtelen sok öttagú nemprimitív hatványgazdag számtani sorozat létezik.*

A fenti tételen túl a [H08] dolgozatban a hatványgazdag számtani sorozatok lehetséges hosszainak teljes karakterizációját is elvégeztük.

3. Számtani sorozatok S-egységek összeghalmazaiban

A számelmélet számos fontos területén rendkívüli jelentőséggel bírnak bizonyos multiplikatív csoport vagy részcsoport elemeire vonatkozó lineáris egyenletek. (Az érdekesség kedvéért itt például megemlíthetjük az ikerprím problémát.) A diofantikus egyenletek területén a legfontosabb egyenletosztályok egyikét az S-egység egyenletek alkotják. Ezek bemutatásához szükségünk van néhány jelölés bevezetésére. Megjegyezzük, hogy az egyszerűbb bemutathatóság kedvéért a szokásoshoz képest itt egy kissé leegyszerűsített jelölés- és fogalomrendszert használunk.

Legyen $\mathbb{K}$ egy algebrai számtest, $O_{\mathbb{K}}$ a $\mathbb{K}$-beli algebrai egészek gyűrűje, S pedig az $O_{\mathbb{K}}$ prímideáljainak egy véges halmaza. Ha $0 \neq \alpha \in \mathbb{K}$ rendelkezik azzal a tulajdonsággal, hogy az $O_{\mathbb{K}}$ bármely S-en kívüli P prímideálja esetén $\mathrm{ord}_P(\alpha) = 0$ teljesül, akkor azt mondjuk, hogy α egy S-egység. (Itt $\mathrm{ord}_P(\alpha)$ a P kietvője az (α) törtideál faktorizációjában.) Jelölje U_S a $\mathbb{K}$-beli S-egységek halmazát, legyenek $a_0, a_1, \ldots, a_n$ $(n \geq 2)$ $\mathbb{K}$-beli nemnulla elemek, és tekintsük az

$$a_1x_1 + \cdots + a_nx_n = a_0 \tag{11}$$

alakú, úgynevezett S-egység egyenletet, ahol $x_1, \ldots, x_n \in U_S$ ismeretlenek. Az egyenlet egy $(x_1, \ldots, x_n)$ megoldását nemelfajulónak nevezzük, ha $a_{i_1}x_{i_1} + \cdots + a_{i_t}x_{i_t}$ az $\{1, \ldots, n\}$ halmaz egyetlen $\{i_1, \ldots, i_t\}$ részhalmaza esetében sem nulla.

A (11) alakú egyenletek a diofantikus egyenletek elméletében igen fontos szerepet játszanak. Ennek oka részben az a kiemelkedően fontos összefüggés, hogy a széteső forma egyenletek (többek között a norma forma egyenletek, a Thue-egyenletek, a diszkrimináns forma egyenletek, az index forma egyenletek) visszavezethetők S-egység egyenletekre; lásd például [Gy80], [EGy85], [EGy88a], [EGy88b], [EGyST88]. Emellett sok más klasszikus, központi diofantikus probléma direkt módon egységegyenletek megoldására vezet; az [EGyST88] és [Gy92] dolgozatokban számos ilyen alkalmazás található. Mivel mi elsősorban nem egy konkrét (11) egyenlet megoldására koncentrálunk, így ehelyütt csupán a tárgyalás szempontjából legfontosabb végességi eredményekről szólunk. Mély diofantikus approximációelméleti eszközök felhasználásával megmutatható, hogy (11) bármely rögzített $(a_0, a_1, \ldots, a_n)$ esetén csupán véges sok nemelfajuló megoldással rendelkezik; az első ilyen jellegű, az $n = 2$ esetre vonatkozó eredmény Siegel [Si21] nevéhez köthető. Ezen túl (a Schmidt-féle altér tétel segítségével) (11) megoldásszáma is korlátozható. Az általunk a későbbiekben használandó, jelenleg ismert legáltalánosabb becslés Evertse, Schlickewei és Schmidt [ESS02] nevéhez fűződik, mely szerint (11)

nemelfajuló megoldásainak száma egy csupán S elemszámától és n-től függő (a konkrét együtthatóktól független!) explicit értékkel korlátozható. (Megjegyezzük, hogy újabban ezt az eredményt Amoroso és Viada [AV] egy közlés alatt álló dolgozatban élesítette.) Mivel a témakör irodalma rendkívül gazdag és szerteágazó, ugyanakkor tárgyalásunkhoz az említett [ESS02]-beli korlát elégséges, így a kapcsolódó eredményekért csak az [ShTi86], [EGyST88], [Gy92], [ESS02], [AV] munkákra, illetve a bennük található megfelelő hivatkozásokra utalunk. Megemlítjük még, hogy $n = 2$ esetén a Baker-módszer segítségével maguk az x_1, x_2 megoldások (pontosabban azok magassága) is korlátozható. Mivel ebbe az irányba nem teszünk lépéseket, így csak a [Gy79], [ShTi86], [EGyST88], [Gy92], [BGy96], [Gy02], [GyY06] publikációkban található eredményekre és hivatkozásokra utalunk.

Az általunk vizsgált problémakör lényegében a (11) jobboldalán lehetséges értékként fellépő (azaz S-egységek n-tagú, adott K-beli együtthatókkal képzett lineáris kombinációiként előálló) a_0 számokból álló halmaz szerkezetére, aritmetikai tulajdonságaira vonatkozik. Már ezen a ponton megemlítjük, hogy alaperedményünk több, egymástól látszólag teljesen független diofantikus probléma esetén is fontos alkalmazást nyert.

Jelölje H a (11) egyenlet jobboldalán lehetséges értékként fellépő a_0 számokból álló halmazt; pontosabban H az U_S elemeinek összes, adott $a_1, \ldots, a_n$ együtthatókkal képzett lineáris kombinációiból áll. A H halmaz szerkezetét, tulajdonságait többen, több szempontból vizsgálták. Győry, Mignotte és Shorey [GyMS90] (több más eredmény mellett) kvantitatív formában igazolta, hogy ha $a_0 \in H$ és $N_S(a_0)$ (a_0 úgynevezett S-normája) „elég nagy", akkor egyrészt $N_S(a_0)$ nem rendelkezhet csupa „kicsi" prímtényezővel, másrészt $N_S(a_0)$ négyzetmentes része sem lehet „kicsi". Ezen túl, Everest [grE89] bizonyos feltételek mellett aszimptotikus formulát is nyert azon H-beli elemek számára, melyek S-normája egy adott korlát alatt marad. Az utóbbi eredményt (a jelen disszertációban nem szereplő) [AHL09] publikációnkban sikerült pontosítanunk. Mivel ezek az eredmények csak érintőlegesen kapcsolódnak az általunk vizsgált irányhoz, így azokat részletesen nem ismertetjük.

Tárgyalásunk fő csapását a H halmazban található számtani sorozatok vizsgálata jelenti. A következőkben megfogalmazzuk ez irányú alaperedményünket. Ehhez szükség van néhány jelölés bevezetésére. Valójában a fenti jelölések felhasználásával már megfogalmazhatnánk tételünk egy leegyszerűsített változatát, ám az irodalommal való minél pontosabb összevetés érdekében érdemesnek tűnik az eredmény precíz ismertetése.

Legyen K egy nullkarakterisztikájú, algebrailag zárt test. Jelölje K^* a K nemnulla elemei alkotta multiplikatív csoportot, és legyen Γ a K^* egy r (véges) rangú multiplikatív részcsoportja. Legyen továbbá t egy pozitív egész, és legyen $\mathcal{A}$ a K^t egy n-elemű (véges) részhalmaza. Vezessük be az

alábbi jelölést:

$$H_t(\Gamma, \mathcal{A}) = \left\{ \sum_{i=1}^{t} a_i x_i : (a_1, \ldots, a_t) \in \mathcal{A},\ (x_1, \ldots, x_t) \in \Gamma^t \right\}.$$

Ezen a területen a bemutatni kívánt „alaperedményünk" a következő.

14. Tétel. ([H07]) *Létezik egy olyan, csak r, t, n értékétől függő $C(r, t, n)$ konstans, hogy bármely $H_t(\Gamma, \mathcal{A})$-beli nemkonstans számtani sorozat hossza legfeljebb $C(r, t, n)$.*

Jól ismert, hogy U_S végesen generált (multiplikatív) csoport. Így a korábbi jelölésekkel, K-t és Γ-t a megfelelő $\mathbb{K}$ algebrai számtestnek illetve U_S S-egység csoportnak választva eredményünk közvetlen következményeként a H halmazban található nemkonstans számtani sorozatok hossza is korlátozható.

Megemlítjük, hogy a $C(r, t, n)$ korlátban mindhárom paraméter jelenléte szükséges, továbbá, hogy a konstanst [AHL09]-ben explicit alakban is megadtuk. Azt is megjegyezzük, hogy a tekintett tulajdonságú sorozatok **száma** nem korlátozható. Eredményünk bizonyítása a korábban említett, (11)-re vonatkozó [ESS02]-beli végességi tételen (végső soron a Schmidt-féle altértételen), valamint van der Waerden [vdW27] már idézett klasszikus eredményén múlik.

Tőlünk függetlenül Jarden és Narkiewicz [JN07] szintén levezettek egy, a 14. Tételhez hasonló eredményt. A mi eredményünk azonban lényegesen általánosabb és pontosabb: Jarden és Narkiewicz eredményében egyrészt Γ egy végesen generált integritási tartomány egységcsoportjának választandó, másrészt (és az alkalmazások szempontjából ez különösen fontos különbégnek tűnik) állításuk csupán az $\mathcal{A} = \{(1, \ldots, 1)\}$ esetre vonatkozik. Amint látni fogjuk, az utóbbi különbség alapján a mi eredményünk valóban általánosabb alkalmazásokhoz vezet.

Az alábbiakban a 14. Tétel három, látszólag teljesen különböző gyökerű problémára vonatkozó alkalmazását mutatjuk be.

M. Pohst [Po06] vetette fel a következő kérdést: igaz-e, hogy minden prímszám előáll egy kettőhatvány és egy háromhatvány összegeként vagy különbségeként? A kérdés nyilvánvalóan rengeteg, a prímszámok halmazára vonatkozó problémával rokon. A kapcsolódó irodalom akárcsak hozzávetőleges feltérképezése is reménytelen vállalkozásnak tűnik, így arra kísérletet sem teszünk. A [H07] dolgozatban Pohst problémáját sikerült lényegesen általánosabb alakban megoldanunk. Ennek bemutatásához legyen most $K = \mathbb{Q}$. Egy racionális prímszámokból álló véges S halmaz esetén jelölje $\mathbb{Z}_S$ azon egészek halmazát, melyek nem oszthatók S-en kívüli prímszámmal. Végül, legyen t egy adott pozitív egész, és legyen A a $\mathbb{Z}^t$ egy véges részhalmaza. Ekkor a következő állítás igaz.

15. Tétel. ([H07]) *Bármely fenti alakú S, t, A esetén végtelen sok olyan prímszám létezik, amely nem áll elő $\sum_{i=1}^{t} a_i x_i$ alakban, ahol $(a_1, \ldots, a_t) \in A$ és $x_1, \ldots, x_t \in \mathbb{Z}_S$.*

A fenti tétel lényegében a 14. Tétel valamint Green és Tao [GT08] azon ünnepelt eredményének következménye, mely szerint a prímszámok körében tetszőleges (véges) hosszúságú számtani sorozat található. Amint az az

$$S = \{2, 3\}, \quad t = 2, \quad A = \{(1, 1), (1, -1)\}$$

választásokkal azonnal látható, a 15. Tétel azonnali negatív választ szolgáltat Pohst fenti kérdésére.

A 14. Tétel egy másik alkalmazásaként végességi eredményt nyertünk norma forma egyenletek megoldáshalmazaiban található számtani sorozatokkal kapcsolatban [BHP]. A különböző típusú diofantikus egyenletek megoldáshalmaza szerkezetének vizsgálata a diofantikus számelmélet klasszikus területei közé tartozik. Számos ilyen irányú eredmény ismert már a szétesőforma egyenletek vonatkozásában is. Eredményünk, valamint a kapcsolódó irodalom bemutatáshoz szükségünk van néhány jelölés bevezetésére.

Legyen $\mathbb{K}$ egy k-ad fokú algebrai számtest, $\alpha_1, \ldots, \alpha_n \in \mathbb{K}$ pedig $\mathbb{Q}$ felett lineárisan független elemek. Jelölje $D \in \mathbb{Z}$ az $\alpha_1, \ldots, \alpha_n$ számok közös nevezőjét, és legyen $\beta_i = D\alpha_i$ $(i = 1, \ldots, n)$. Ekkor persze $\beta_1, \ldots, \beta_n$ $\mathbb{K}$-beli algebrai egészek. Legyen m egy tetszőleges nemnulla egész szám, és tekintsük az alábbi (úgynevezett norma forma) egyenletet

$$N_{K/\mathbb{Q}}(x_1\alpha_1 + \ldots + x_n\alpha_n) = m, \tag{12}$$

ahol $x_1, \ldots, x_n$ ismeretlen egészek. Legyen most H a (12) egyenlet megoldáshalmaza, $|H|$ pedig H elemszáma. Jól ismert klasszikus eredmény (lásd például [Sc72]), hogy ha az $\alpha_1, \ldots, \alpha_n$ elemek által generált $\mathbb{Z}$-modulus tartalmaz olyan részmodulust, mely teljes a $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ számtest egy $\mathbb{Q}$-tól és a képzetes másodfokú számtestektől különböző valamely részteste felett, akkor (12) végtelen sok megoldással is rendelkezhet.

A H halmaz aritmetikai tulajdonságait többen, több szempontból vizsgálták. Az $n = 2$ esetben, bizonyos további feltételek mellett Pethő [Pe82] illetve Shorey és Stewart [ShSt83] egymástól függetlenül megmutatták, hogy (12) megoldásainak koordinátái között csak véges sok teljes hatvány szerepelhet, és ezek effektív módon meghatározhatók. Evertse és Győry [EGy97], illetve Everest és Győry [grEGy05] általános szétesőforma egyenletek esetén (bizonyos egyéb feltételek mellett) egyrészt aszimptotikus formulákat nyertek a korlátos magasságú megoldások számára, illetve kvantitatív formában megmutatták, hogy ha egy megoldás x_i koordinátája „elég nagy”, akkor x_i szükségképpen rendelkezik „nagy” prímosztóval.

Új kutatási irányként Pethő és társszerzői a közelmúltban számos olyan eredményt nyertek, melyek két, a H-beli elemek koordinátáiban található számtani sorozatokra vonatkozó problémával kapcsolatosak. A „vízszintes" probléma a következő módon fogalmazható meg: hány olyan H-beli elem van, melynek koordinátái számtani sorozatot alkotnak? Ebben az irányban több érdekes effektív és numerikus végességi eredmény is született, például Bérczes és Pethő [BP04], [BP06], Bérczes, Pethő és Ziegler [BPZ06] valamint Bazsó [Bazs07] tollából. Mi most az alábbi „függőleges" problémára koncentrálunk: létezik-e a H-beli elemek valamelyik koordinátájában tetszőleges hosszúságú számtani sorozat? E kérdést a kvadratikus esetben (amikoris (12) egy Pell-egyenlet) Pethő és Ziegler [PZ08] megválaszolta: megmutatták, hogy az ilyen típusú sorozatok hossza effektív módon korlátozható (lásd még [DPT08]). Az általuk kifejlesztett módszer azonban a magasabbfokú esetben nem használható. A 14. Tétel alkalmazásával ugyanakkor lehetőség nyílik az alábbi általános végességi eredmény igazolására.

16. Tétel. ([BHP]) *Legyen $(x_1^{(j)}, \dots, x_n^{(j)})$ $(j = 1, \dots, t)$ egy H-beli sorozat, melyre $x_i^{(j)}$ egy nemkonstans számtani sorozat valamilyen $i \in \{1, \dots, n\}$ esetén. Ekkor $t \leq C(k, m, D)$ teljesül, ahol $C(k, m, D)$ egy, csak k, m, D értékétől függő explicit módon meghatározható konstans.*

Megemlítjük, hogy a [BHP] dolgozatban több más eredmény is született; sikerült például a konstans számtani sorozatok esetét is kezelnünk. A 16. Tétel bizonyításának egyik legfontosabb lépését a 14. Tétel alkalmazása jelenti.

A 14. Tétel harmadik bemutatandó alkalmazása az irodalomban a „unit sum number" néven ismert problémával kapcsolatos. Az alapprobléma a következő: adott R egységelemes gyűrű esetén döntsük el, létezik-e egy olyan t egész szám, hogy R valamennyi eleme előáll legfeljebb t számú R-beli egység összegeként. Az első ilyen jellegű kérdést 55 évvel ezelőtt Zelinsky [Ze54] vetette fel, bizonyos endomorfizmus-gyűrűkkel kapcsolatban. Később a kiinduló problémát többen általánosították, míg végül a fent megfogalmazott alakját Goldsmith, Pabst és Scott [GPS98] cikkében érte el. Ashrafi és Vámos [AV05]-ben a másod- és harmadfokú algebrai számtestek egészeinek gyűrűje esetén, valamint bizonyos körosztási testek vonatkozásában a kérdésre negatív választ adott. Végül, a probléma algebrai számtestekben való egyfajta lezárásaként Jarden és Narkiewicz [JN07] az alábbi általános tételt nyerte.

Tétel (Jarden és Narkiewicz, [JN07]) *Legyen R egy végesen generált nullkarakterisztikájú integritási tartomány. Ekkor minden t természetes számhoz található olyan R-beli elem, amely nem áll elő legfeljebb t számú R-beli egység összegeként.*

A fenti tétel a 14. Tételhez hasonló (bár annál speciálisabb) [JN07]-beli

eredmény triviális következménye. Csupán az érdekesség kedvéért megemlítjük, hogy valójában a 14. Tételből az alábbi élesebb (még nem publikált) következmény automatikusan adódik.

A 14. Tétel következménye. *Legyen R egy végesen generált nullkarakterisztikájú integritási tartomány. Ekkor bármely t természetes számhoz és R^t bármely véges A részhalmazához található olyan R-beli elem, mely nem áll elő*

$$\sum_{i=1}^{t} a_i x_i \quad ((a_1, \ldots, a_t) \in A,\ x_1, \ldots, x_t\ R\text{-beli egység}) \tag{13}$$

alakban.

Mivel itt $a_i = 0$ is megengedett, a fenti következmény valóban Jarden és Narkiewicz tételének élesítése. Ugyanakkor az állítás valóban a 14. Tétel egyszerű következménye. Ennek igazolásához csupán azt kell észrevennünk, hogy tetszőleges nemnulla R-beli α elem esetén $\alpha, 2\alpha, \ldots, k\alpha$ számok számtani sorozatot alkotnak. Így ha k „elég nagy", akkor a 14. Tétel miatt ezen elemek mindegyike nem állhat elő (13) alakban.

Hivatkozások

[AHL09] Zs. Ádám, L. Hajdu and F. Luca, *Representing integers as linear combinations of S-units*, Acta Arith. **138** (2009), 101–107.

[AV] F. Amoroso and E. Viada, *Small points on rational subvarieties of tori*, (közlésre benyújtva).

[AV05] N. Ashrafi and P. Vámos, *On the unit sum number of some rings*, The Quarterly Journal of Mathematics **56** (2005), 1–12.

[Bak68] A. Baker, *Contributions to the theory of diophantine equations*, Phil. Trans. R. Soc. London **263** (1968), 173–208.

[Bazs07] A. Bazsó, *Further computational experiences on norm form equations with solutions forming arithmetic progressions*, Publ. Math. Debrecen **71** (2007), 489–497.

[BBGyP] A. Bazsó, A. Bérczes, K. Győry and Á. Pintér, *On the resolution of equations $Ax^n - By^n = C$ in integers x, y and $n \geq 3$ II*, Publ. Math. Debrecen (közlésre elfogadva).

[Ben03] M. A. Bennett, *Recipes for ternary Diophantine equations of signature (p, p, k)*, Proc. RIMS Kokyuroku (Kyoto) **1319** (2003), 51–55.

[BBGyH06] M. Bennett, N. Bruin, K. Győry and L. Hajdu, *Powers from products of consecutive terms in arithmetic progression*, Proc. London Math. Soc. **92** (2006), 273–306.

[BGyMP06] M. A. Bennett, K. Győry, M. Mignotte and Á. Pintér, *Binomial Thue equations and polynomial powers*, Compositio Math. **142** (2006), 1103–1121.

[BS04] M. A Bennett and C. Skinner, *Ternary Diophantine equations via Galois representations and modular forms*, Canad. J. Math. **56** (2004), 23–54.

[BHP] A. Bérczes, L. Hajdu and A. Pethő, *Arithmetic progressions in the solution sets of norm form equations*, Rocky Mountain J. Math. (közlésre elfogadva).

[BP04] A. Bérczes and A. Pethő, *On norm form equations with solutions forming arithmetic progressions*, Publ. Math. Debrecen **65** (2004), 281–290.

[BP06] A. Bérczes and A. Pethő, *Computational experiences on norm form equations with solutions forming arithmetic progressions*, Glasnik Math. **41** (2006), 1–8.

[BPZ06] A. Bérczes, A. Pethő and V. Ziegler, *Parameterized norm form equations with arithmetic progressions*, J. Symbolic Comput. **41** (2006), 790–810.

[Bo98] K. D. Boklan, *Problem 10702*, Amer. Math. Monthly **105** (1998), p. 956.

[BCP97] W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), 235–265.

[BHR00] B. Brindza, L. Hajdu and I. Z. Ruzsa, *On the equation* $x(x+d)\dots(x+(k-1)d) = by^2$, Glasgow Math. J. **42** (2000), 255–261.

[Br03] N. Bruin, *Chabauty methods using elliptic curves*, J. Reine Angew. Math. **562** (2003), 27–49.

[BGyHT06] N. Bruin, K. Győry, L. Hajdu and Sz. Tengely, *Arithmetic progressions consisting of unlike powers*, Indag. Math. **17** (2006), 539–555.

[BGy96] Y. Bugeaud and K. Győry, *Bounds for the solutions of unit equations*, Acta Arith. **74** (1996), 67–80.

[BMS08] Y. Bugeaud, M. Mignotte and S. Siksek, *A multi-Frey approach to some multi-parameter families of Diophantine equations*, Canad. J. Math. **60** (2008), 491–519.

[C41] C. Chabauty, *Sur les points rationnels des variétés algébriques dont l'irrégularité est supérieure á la dimension*, C. R. Acad. Sci. Paris **212** (1941), 1022–1024.

[DG95] 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** (1995), 513–543.

[DM97] H. Darmon and L. Merel, *Winding quotients and some variants of Fermat's Last Theorem*, J. Reine Angew. Math. **490** (1997), 81–100.

[De52] P. Dénes, *Über die diophantische Gleichung* $x^l + y^l = cz^l$, Acta Math. **88** (1952), 241–251.

[Di66] L. E. Dickson, *History of the theory of numbers. Vol. II: Diophantine analysis*, Chelsea Publishing Co., New York, 1966, xxv+803 pp.

[DPT08] A. Dujella, A. Pethő and P. Tadić, *On arithmetic progressions on Pellian equations*, Acta Math. Hungar. **120** (2008), 29–38.

[Er39] P. Erdős, *Note on the product of consecutive integers*, J. London Math. Soc. **14** (1939), 194–198.

[Er51] P. Erdős, *On a diophantine equation*, J. London Math. Soc. **26** (1951), 176–178.

[ES75] P. Erdős and J. L. Selfridge, *The product of consecutive integers is never a power*, Illinois J. Math. **19** (1975), 292–301.

[grE89] G. R. Everest, *Counting the values taken by sums of* S*-units*, J. Number Theory **35** (1990), 269–286.

[grEGy05] G. R. Everest and K. Győry, *On some arithmetical properties of solutions of decomposable form equations*, Math. Proc. Camb. Phil. Soc. **139** (2005), 27–40.

[EGy85] J.-H. Evertse and K. Győry, *On unit equations and decomposable form equations*, J. Reine Angew. Math. **358** (1985), 6–19.

[EGy88a] J.-H. Evertse and K. Győry, *Finiteness criteria for decomposable form equations*, Acta Arith. **50** (1988), 357–379.

[EGy88b] J.-H. Evertse and K. Győry, *Decomposable form equations*, in: New Advances in Transcendence Theory (A. Baker ed.), pp. 175–202, Cambridge University Press, 1988.

[EGy97] J.-H. Evertse and K. Győry, *The number of families of solutions of decomposable form equations*, Acta Arith. **80** (1997), 367–394.

[EGySST88] J.-H. Evertse, K. Győry, C. Stewart and R. Tijdeman, *S-unit equations and their applications*, in: New Advances in Transcendence Theory (A. Baker ed.), pp. 110–174, Cambridge University Press, 1988.

[ESS02] J.-H. Evertse, H. P. Schlickewei and W. M. Schmidt, *Linear equations in variables which lie in a multiplicative group*, Annals Math. **155** (2002), 807–836.

[F83] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983) 349–366.

[FH01] P. Filakovszky and L. Hajdu, The resolution of the equation $x(x+d)\dots(x+(k-1)d) = by^2$ for fixed d, Acta Arith. **98** (2001), 151–154.

[F97] E. V. Flynn, *A flexible method for applying Chabauty's theorem*, Compositio Math. **105** (1997), 79–94.

[GPZ94] J. Gebel, A. Pethő and H. G. Zimmer, *Computing integral points on elliptic curves*, Acta Arith. **68** (1994), 171–192.

[GPS98] B. Goldsmith, S. Pabst and A. Scott, *Unit sum numbers of rings and modules*, Q. J. Math. Oxf. II. Ser. **49** (1998), 331–344.

[GT08] B. Green and T. Tao, *The primes contain arbitrarily long arithmetic progressions*, Annals of Math. **167** (2008), 481–547.

[Gy79] K. Győry, *On the number of solutions of linear equations in units of an algebraic number field*, Comment. Math. Helv. **54** (1979), 583–600.

[Gy80] K. Győry, *Résultats effectifs sur la représentation des entiers par des formes décomposables*, Queen's Papers in Pure and Appl. Math. **56**, Kingston, Canada, 1980.

[Gy92] K. Győry, *Some recent applications of S-unit equations*, in: Journées Arithmétiques de Geneve (1991), (D. F. Coray, Y.-F. S. Pétermann eds.), Astérisque **209**, Soc. Math. France, 1992, pp. 17–38.

[Gy97] K. Győry, *On the diophantine equation $\binom{n}{k} = x^l$*, Acta Arith. **80** (1997), 289–295.

[Gy98] K. Győry, *On the diophantine equation $n(n+1)\dots(n+k-1) = bx^l$*, Acta Arith. **83** (1998), 87–92.

[Gy99] K. Győry, *Power values of products of consecutive integers and binomial coefficients*, Number Theory and Its Applications, Kluwer Acad. Publ. 1999, 145–156.

[Gy02] K. Győry, *Solving Diophantine equations by Baker's theory*, in: A panorama of number theory or the view from Baker's garden (G. Wüstholz, ed.), Cambridge Univ. Press, 2002, pp. 38–72.

[GyHP09] K. Győry, L. Hajdu and Á. Pintér, *Perfect powers from products of consecutive terms in arithmetic progression*, Compositio Math. **145** (2009), 845–864.

[GyHS04] K. Győry, L. Hajdu and N. Saradha, *On the Diophantine equation $n(n+d)\dots(n+(k-1)d) = by^l$*, Canad. Math. Bull. **47** (2004), 373–388.

[GyMS90] K. Győry, M. Mignotte and T. Shorey, *On some arithmetical properties of weighted sums of S-units*, Math. Pann. **1** (1990), 25–43.

[GyP08] K. Győry and Á. Pintér, *Polynomial powers and a common generalization of binomial Thue-Mahler equations and S-unit equations*, in: Diophantine Equations (Mumbai, 2005, N. Saradha ed.), Narosa Publishing House, Mumbai, 2008, 103–121.

[GyY06] K. Győry and Kunrui Yu, *Bounds for the solutions of S-unit equations and decomposable form equations*, Acta Arith. **123** (2006), 9–41.

[H04] L. Hajdu, *Perfect powers in arithmetic progression. A note on the inhomogeneous case*, Acta Arith. **113** (2004), 343–349.

[H07] L. Hajdu, *Arithmetic progressions in linear combinations of S-units*, Period. Math. Hungar. **54** (2007), 175–181.

[H08] L. Hajdu, *Powerful arithmetic progressions*, Indag. Math. **19** (2008), 547–561.

[HT] L. Hajdu and Sz. Tengely, *Arithmetic progressions of squares, cubes and n-th powers*, J. Functiones et Approximatio (közlésre elfogadva).

[HTT09] L. Hajdu, Sz. Tengely and R. Tijdeman, *Cubes in products of terms in arithmetic progression*, Publ. Math. Debrecen **74** (2009), 215–232.

[HKLST07] N. Hirata-Kohno, S. Laishram, T. N. Shorey and R. Tijdeman, *An extension of a theorem of Euler*, Acta Arith. **129** (2007), 71–102.

[JN07] M. Jarden and W. Narkiewicz, *On sums of units*, Monatsh. Mat. **150** (2007), 327–332.

[K97] A. Kraus, *Majorations effectives pour l'équation de Fermat généralisée*, Canad. J. Math. **49** (1997), 1139–1161.

[L64] S. Lang, *Diophantine approximation on toruses*, Amer. J. Math. **86** (1964), 521–533.

[L78] S. Lang, *Elliptic Curves; Diophantine Analysis*, Grundlehren Math. Wiss. **231**, Springer, Berlin, 1978.

[Mar85] R. Marszalek, *On the product of consecutive elements of an arithmetic progression*, Monatsh. für Math. **100** (1985), 215–222.

[Mas85] D. W. Masser, *Open problems*, in: Proc. Symp. Analytic Number Theory (W. W. L. Chen ed.), Imperial Coll. London, 1985.

[Mi04] P. Mihăilescu, *Primary cyclotomic units and a proof of Catalan's conjecture*, J. Reine Angew. Math. **572** (2004), 167–195.

[Mo69] L. J. Mordell, *Diophantine Equations*, Academic Press, London and New York, 1969.

[MS04] A. Mukhopadhyay and T. N. Shorey, *Square free part of products of consecutive integers*, Publ. Math. Debrecen **64** (2004), 79–99.

[Ob50] R. Obláth, *Über das Produkt fünf aufeinander folgender Zahlen in einer arithmetischen Reiche*, Publ. Math. Debrecen **1** (1950), 222–226.

[Ob51] R. Obláth, *Eine Bemerkung über Produkte aufeinander folgender Zahlen*, J. Indian Math. Soc. **15** (1951), 135–139.

[Oe88] J. Oesterlé, *Nouvelles approches du „Théorème" de Fermat*, Astérisque **161** (1988), 165–186.

[Pe82] A. Pethő, *Perfect powers in second order linear recurrences*, J. Number Theory **15** (1982), 5–13.

[PZ08] A. Pethő and V. Ziegler, *Arithmetic progressions on Pell equations*, J. Number Theory **128** (2008), 1389–1409.

[Po06] M. Pohst, Private communication, 2006.

[Rib97] K. Ribet, *On the equation* $a^p + 2^\alpha b^p + c^p = 0$, Acta Arith. **79** (1997), 7–16.

[Rig39] O. Rigge, *Über ein diophantisches Problem*, in: 9th Congress Math. Scand. (Helsingfors 1938.), Mercator, 1939, pp. 155–160.

[Ro00] J. P. Robertson, *The Maximum Length of a Powerful Arithmetic Progression: 10702*, Amer. Math. Monthly **107** (2000), p. 951.

[Sa97] N. Saradha, *On perfect powers in products with terms from arithmetic progressions*, Acta Arith. **82** (1997), 147–172.

[Sa98] N. Saradha, *Squares in products with terms in an arithmetic progression*, Acta Arith. **86** (1998), 27–43.

[SS01] N. Saradha and T.N. Shorey, *Almost perfect powers in arithmetic progression*, Acta Arith. **99** (2001), 363–388.

[SS03a] N. Saradha and T. N. Shorey, *Almost squares in arithmetic progression*, Compositio Math. **138** (2003), 73–111.

[SS03b] N. Saradha and T. N. Shorey, *Almost squares and factorisations in consecutive integers*, Compositio Math. **138** (2003), 113–124.

[ScTi76] A. Schinzel and R. Tijdeman, *On the equation* $y^m = P(x)$, Acta Arith. **31** (1976), 199–204.

[Sc72] W. M. Schmidt, *Norm form equations*, Ann. of Math. **96** (1972), 526–551.

[Se51] E. Selmer, *The diophantine equation* $ax^3 + by^3 + cz^3 = 0$, Acta Math. **85** (1951), 205–362.

[Sh02] T. N. Shorey, *Powers in arithmetic progression*, in: A Panorama in Number Theory or The View from Baker's Garden (G. Wüstholz ed.), Cambridge University Press, 2002, 341–353.

[ShSt83] T. N. Shorey and C. L. Stewart, *On the diophantine equation* $ax^{2t} + bx^t y + cy^2 = d$ *and pure powers in recurrence sequences*, Math. Scand. **52** (1983), 24–36.

[ShTi86] T. Shorey and R. Tijdeman, *Expontial diophantine equations*, Cambridge University Press, 1986.

[ShTi90] T. Shorey and R. Tijdeman, *Perfect powers in product of terms in an arithmetical progression*, Compositio Math. **75** (1990), 307–344.

[ShTi97] T. Shorey and R. Tijdeman, *Some methods of Erdős applied to finite arithmetic progression*, The Mathematics of Paul Erdős I, Springer, 1997, 251–267.

[Si21] C. L. Siegel, *Approximation algebraischer Zahlen*, Math. Z. **10** (1921), 173–213.

[Sm93] SIMATH manual, Universität des Saarlandes, Saarbrücken, Germany, 1993.

[StTz94] R. J. Stroeker and N. Tzanakis, *Solving elliptic diophantine equations by estimating linear forms in elliptic logarithms*, Acta Arith. **67** (1994), 177–196.

[Te08] Sz. Tengely, *Note on a paper „An extension of a theorem of Euler" by Hirata-Kohno et al.*, Acta Arith. **134** (2008), 329–335.

[Ti76a] R. Tijdeman, *Diophantine equations and diophantine approximations*, in: Number Theory and Applications (R. A. Mollin, ed.), North-Holland, 1976, 399–416.

[Ti76b] R. Tijdeman, *On the equation of Catalan*, Acta Arith. **29** (1976), 197–209.

[Ti89] R. Tijdeman, *Applications of the Gelfond-Baker method to rational number theory*, in: Topics in Number Theory (P. Turán ed.), Kluwer Acad. Publ., 1989, 215–243.

[Ti98] R. Tijdeman, *Exponential diophantine equations 1986-1996*, in: Number Theory: Diophantine, Computational and Algebraic Aspects (K. Győry, A. Pethő and V. T. Sós, eds.), Walter de Gruyter, Berlin-New York, 1998, 523–540.

[vdW27] B. L. van der Waerden, *Beweis einer Baudetschen Vermutung*, Nieuw Archief voor Wiskunde **19** (1927), 212–216.

[W95] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Ann. Math. **141** (1995), 443–551.

[Za87] D. Zagier, *Large integral points on elliptic curves*, Math. Comp. **48** (1987), 425–436.

[Ze54] D. Zelinsky, *Every linear transformation is a sum of nonsingular ones*, Proc. Am. Math. Soc. **5** (1954), 627–630.

I. Számtani sorozatot alkotó n-edik hatványok

I.1 [FH01]: The resolution of the diophantine equation

$$x(x+d)\dots(x+(k-1)d) = by^2 \text{ for fixed } d$$

Acta Arith. **98** (2001), 151–154.

THE RESOLUTION OF THE DIOPHANTINE EQUATION $x(x+d)\dots(x+(k-1)d) = by^2$ FOR FIXED d

P. Filakovszky and L. Hajdu*

Abstract. In this paper we provide an algorithm for the resolution of the title equation, which works for any d. To illustrate the simplicity of the method, we extend a result of Saradha by giving all solutions with $23 \leq d \leq 30$, $k \geq 3$, $(x,d) = 1$ and $P(b) \leq k$, in positive integers x, d, k, b, y.

1. Introduction

A classical problem of Number Theory is to determine those finite arithmetical progressions, for which the product of the terms yields a perfect power, or an 'almost' perfect one. Erdős and Selfridge in 1975 (cf. [2]) proved that the product of two or more consecutive positive integers is never a perfect power, i.e. the equation

$$x(x+1)\dots(x+k-1) = y^l$$

has no solutions with $k, l \geq 2$ and $x \geq 1$. There are many results in the literature concerning the various generalizations of the above equation, see e.g. the extensive survey papers [8], [9], [10], [11], or the very recent papers [1], [4], [5], [6], [7], and the references given there.

Let $P(b)$ denote the greatest prime factor of a positive integer $b > 1$, and put $P(1) = 1$. In this paper we investigate the following equation:

$$(1) \qquad x(x+d)\dots(x+(k-1)d) = by^2 \text{ with } d > 1, k \geq 3,\ (x,d) = 1,\ P(b) \leq k,$$

in positive integers x, d, k, b, y. In [7] Saradha proved that equation (1) has only the solutions

$$(x,d,k,b,y) = (2,7,3,2,12), (18,7,3,1,120), (64,17,3,2,504),$$

provided that $d \leq 22$ holds. In fact she gave an algorithm for the resolution of (1) for fixed values of d, and used her method to compute all solutions with $1 < d < 23$. The main steps of her method are the following. Put $C = (k-1)^2 d^2/4$, and suppose first that for a solution (x,d,k,b,y) of (1) $x \geq C$ holds. For such a solution Saradha derived an upper bound $k_0(d)$ for k, which varies between 18 and 314 as d ranges through the interval $[7, 22]$. It is not guaranteed that her method provides an upper

2000 Mathematics Subject Classification: 11D41.

*Research supported in part by the Hungarian Academy of Sciences, and by Grants F023800 and T29330 from the Hungarian National Foundation for Scientific Research.

bound $k_0(d)$ for an arbitrary value of d. Subsequently she proved that $4 \leq k \leq 6$ if $d = 7$, $4 \leq k \leq 8$ if $d \in \{11, 13, 17, 19\}$, respectively, and that (1) has no solutions for other values of d with $1 < d < 23$. The remaining cases were verified by numerical calculations.

In [1] Brindza, Hajdu and Ruzsa proved the following result.

Theorem A. *If (x, d, k, b, y) is a solution to (1) with $k \geq 8$, then $x < D$, where $D = 4d^4(\log d)^4$.*

This implies that we can take $k_0(d) = 8$ if $x \geq D$. This uniform bound makes it possible, at least in principle, to resolve equation (1) for any fixed d. This paper provides an algorithm to do so. We shall illustrate the algorithm by determining all solutions of (1) with $23 \leq d \leq 30$.

2. Result and description of the algorithm

The main steps of our method for the resolution of (1) with fixed d are the following. First we provide a simple search algorithm to find the solutions with small x. According to Theorem A we have $k \leq 7$ for the large solutions. We show that each such solution corresponds to a point on one among 16 elliptic curves. The elliptic equations can be resolved by a mathematical software package.

Theorem. *Suppose that $23 \leq d \leq 30$. The only solutions to equation (1) are the following ones:*
$d = 23$, $k = 3$: $(x, b, y) = (2, 6, 20)$, $(4, 6, 30)$, $(75, 6, 385)$, $(98, 2, 924)$, $(338, 3, 3952)$, $(3675, 6, 91805)$,
$d = 23$, $k = 4$: $(x, b, y) = (75, 6, 4620)$,
$d = 24$, $k = 3$: $(x, b, y) = (1, 1, 35)$.

Remark. The above theorem provides a solution to (1) with $k > 3$, namely $(x, d, k, b, y) = (75, 23, 4, 6, 4620)$. This is not surprising, as it was pointed out by F. Beukers that equation (1) has infinitely many solutions with $k = 4$.

Proof of the Theorem. Suppose first that (x, d, k, b, y) is a solution to (1) with $23 \leq d \leq 30$ and $x < D$, where D is defined in Theorem A. Using the estimate $k < 4d(\log d)^2$ due to Saradha [7], the left hand side of equation (1) is bounded by a constant depending only on d. Hence after fixing d, all solutions to (1) can be found by a simple search. However, as a huge amount of computation is needed, it is worth to be more economical.

Let d be fixed. A positive integer a is called a *bad number*, if some prime p with $p \geq 4d(\log d)^2$ occurs in the prime factorization of a on an odd exponent. Suppose that $x + id$ is a bad number for some i with $0 \leq i \leq k - 1$, and choose a prime p with the above properties for $a = x + id$. Then by Saradha's result we have $p > k$. By the condition $(x, d) = 1$, there is no other factor $x + jd$ which is divisible by p. Hence p divides the left-hand side on an odd exponent, which yields a contradiction with $P(b) \leq k$. This argument shows that no factor $x + id$ is bad.

We work with the residue classes (mod d) separately. Let m be a positive integer with $(m, d) = 1$, $m < d$. We make a list L_3 consisting of all those positive integers $x' < D$ with $x' \equiv m \pmod{d}$ for which none of the numbers x', $x' + d$, $x' + 2d$ is bad. Then we make a list L_4 of all the numbers $x' \in L_3$ with $x' + d \in L_3$. Subsequently we make a list L_5 of all the numbers $x' \in L_4$ with $x' + d \in L_4$ and so on. For $23 \leq d \leq 30$ the process stops around L_{15}. Observe that $x' \in L_i$ if and

only if none of the numbers $x', x'+d, \dots, x'+(i-1)d$ is bad. Hence every solution (x, d, k, b, y) of (1) with $x < D$ satisfies $x \in L_k$. Finally, for each number $x' \in L_k$ we check if $x'(x'+d)\dots(x'+(k-1)d)$ has a square-free part which has a greatest prime factor $\leq k$, for all lists L_k. The numbers which pass this last test provide all the solutions with $x \equiv m \pmod{d}$. Finally we take the union over all m to collect all solutions of (1) with $x < D$.

Now suppose that (x, d, k, b, y) is a solution to (1) with $x \geq D$. Then, by Theorem A, $k \leq 7$. Write now $x + id = a_i x_i^2$ $(i = 0, \dots, k-1)$ with square-free a_i's and suppose that $P(a_i) > k$ for some i. By the assumption $(x, d) = 1$ this implies $P(b) > k$, which is a contradiction. This shows that $P(a_i) \leq k$. Hence we get

$$x(x+d)(x+2d) = cz^2, \tag{2}$$

where c and z are positive integers with $P(c) \leq k$, c square-free. Moreover, by the assumption $(x, d) = 1$ we get that $(c, d) = 1$ in (2). Hence $c \in \{1, 2, 3, 5, 6, 7, 10, 14, 15, 21, 30, 35, 42, 70, 105, 210\}$. Thus for each d we have to resolve 16 elliptic equations of the form

$$u^3 - c^2 d^2 u = v^2 \quad \text{in} \quad u, v \in \mathbb{Z},$$

where u and v are given by $u = c(x+d)$ and $v = c^2 z$, respectively. Using the program package SIMATH (cf. [12]) these elliptic equations can be resolved easily. For a detailed description of the algorithm implemented in SIMATH, see e.g. [3].

The simple search method already yielded all the solutions mentioned in the theorem. As in these solutions $k \leq 7$, all of them, but no more were also provided by the resolution of the elliptic equations. □

3. Acknowledgements

The authors are grateful to Professors K. Győry and R. Tijdeman for their valuable remarks.

References

[1] B. Brindza, L. Hajdu and I. Z. Ruzsa, *On the equation* $x(x+d)\dots(x+(k-1)d) = by^2$, Glasgow Math. J. (to appear).

[2] P. Erdős and J. L. Selfridge, *Note on products of consecutive integers*, Illinois J. Math. **19** (1975), 292–301.

[3] J. Gebel, A. Pethő and H. G. Zimmer, *Computing integral points on elliptic curves*, Acta Arith. **68** (1994), 171–192.

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

[5] K. Győry, *Power values of products of consecutive integers and binomial coefficients*, Number Theory and its Applications, Kluwer Acad. Publ., 1999, pp. 145–156.

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

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

[8] T. N. Shorey, *Exponential diophantine equations involving products of consecutive integers and related equations*, (to appear).

[9] T. N. Shorey and R. Tijdeman, *Some methods of Erdős applied to finite arithmetic progressions integers and related equations*, The Mathematics of Paul Erdős, I, Springer, 1997, pp. 251–267.

[10] R. Tijdeman, *Diophantine equations and diophantine approximations*, in "Number Theory and Applications" (R. A. Mollin, ed.), Kluwer Acad. Publ., 1989, pp. 215–243.

[11] R. Tijdeman, *Exponential diophantine equations 1986-1996*, Number Theory: Diophantine, Computational and Algebraic Aspects (K. Győry, A. Pethő and V. T. Sós, eds.), Walter de Gruyter, Berlin–New York, 1998, pp. 523–540.
[12] *SIMATH Manual*, Universität des Saarlandes, Saarbrücken, Germany, 1993.

Péter Filakovszky

Šoltésovej 21
94059 Nové Zámky
Slovakia

Lajos Hajdu

University of Debrecen
Institute of Mathematics and Informatics
P.O. Box 12
H-4010 Debrecen
Hungary

E-mail address:
hajdul@math.klte.hu

I.2 [GyHP09]: Perfect powers from products of consecutive terms in arithmetic progression

Compositio Math. **145** (2009), 845–864.

Perfect powers from products of consecutive terms in arithmetic progression

K. Győry, L. Hajdu and Á. Pintér

Abstract

We prove that for any positive integers x, d, k with $\gcd(x, d) = 1$ and $3 < k < 35$ the product $x(x + d) \dots (x + (k - 1)d)$ cannot be a perfect power. This yields a considerable extension of previous results of Győry, Hajdu, Saradha, and Bennett, Bruin, Győry, Hajdu which covered the cases $k \leq 11$. We also establish more general theorems for the case when x can also be a negative integer and the product yields an almost perfect power. As in the proofs of the earlier theorems, for fixed k we reduce the problem to systems of ternary equations. However, our results do not follow as a mere computational sharpening of the approach utilized previously, but instead require the introduction of fundamentally new ideas. For $k > 11$, a great number of new ternary equations arise that we solve by combining the Frey curve and Galois representation approach with local and cyclotomic considerations. Furthermore, the number of systems of equations grows so rapidly with k that, in contrast with the previous proofs, it is practically impossible to handle the different cases in the usual manner. The main novelty of this paper is that we algorithmize our proofs which enables us to use a computer. We apply an efficient, iterated combination of our procedure for solving the arising new ternary equations with several sieves based on the ternary equations already solved. In this way we are able to exclude the solvability of the enormous number of systems of equations under consideration. Our general algorithm seems to work for larger k as well, but there is of course a computational time limit.

1. Introduction and new results

A classical theorem of Erdős and Selfridge [ES] asserts that the product of consecutive positive integers is never a perfect power. A natural generalization is the Diophantine equation

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

in non-zero integers x, d, k, b, y, n with $\gcd(x, d) = 1$, $d \geq 1$, $k \geq 3$, $n \geq 2$ and $P(b) \leq k$. Here $P(u)$ denotes the largest prime divisor of a non-zero integer u, with the convention that $P(\pm 1) = 1$.

Equation (1) has an extremely rich literature. For $d = 1$, equation (1) has been completely solved by Saradha [Sar] (for $k \geq 4$) and Győry [Gy1] (for $k < 4$). Instead of trying to overview all branches of related results for $d > 1$ (which seems to be an enormous task), we refer to the excellent survey papers of Tijdeman [Ti] and Shorey [S1], [S2]. Here we mention only those contributions which are closely related to the results of the present paper, that is which provide the complete solution of (1) when the number k of terms is fixed.

If $(k, n) = (3, 2)$, equation (1) has infinitely many solutions even with $b = 1$. Euler (see [Di])

2000 Mathematics Subject Classification 11D61, 11B25

Keywords: Perfect powers, arithmetic progression, ternary diophantine equations, modular forms

Research supported in part by the Hungarian Academy of Sciences, by the János Bolyai Research Fellowship, and by the OTKA grants T48791 and T67580.

showed that (1) has no solutions if $b = 1$ and $(k, n) = (3, 3)$ or $(4, 2)$. A similar result was obtained by Obláth [O1], [O2] for $(k, n) = (3, 4)$, $(3, 5)$ and $(5, 2)$. By a conjecture of Erdős equation (1) has no solutions in positive integers when $k > 3$ and $b = 1$. In other words, the product of k consecutive terms in a coprime positive arithmetic progression with $k > 3$ can never be a perfect power. By coprime positive progression we mean one of the form

$$x, x + d, \ldots, x + (k - 1)d,$$

where x, d are positive integers with $\gcd(x, d) = 1$.

Erdős' conjecture has recently been verified for certain values of k in a more general form. In the following Theorem A the case $k = 3$ is due to Győry [Gy2], the cases $k = 4, 5$ to Győry, Hajdu and Saradha [GyHS], and the cases $6 \le k \le 11$ to Bennett, Bruin, Győry and Hajdu [BBGyH].

Theorem A. *Suppose that k and n are integers with $3 \le k \le 11$, $n \ge 2$ prime and $(k, n) \ne (3, 2)$, and that x and d are coprime integers. If, further, b is a non-zero integer with $P(b) \le P_{k,n}$ where $P_{k,n}$ is given in Table 1, then the only solutions to (1) are with (x, d, k) in the following list:*

$$(-9, 2, 9), (-9, 2, 10), (-9, 5, 4), (-7, 2, 8), (-7, 2, 9),$$

$$(-6, 1, 6), (-6, 5, 4), (-5, 2, 6), (-4, 1, 4), (-4, 3, 3),$$

$$(-3, 2, 4), (-2, 3, 3), (1, 1, 4), (1, 1, 6).$$

k	$n = 2$	$n = 3$	$n = 5$	$n \ge 7$
3	–	2	2	2
4	2	3	2	2
5	3	3	3	2
6	5	5	5	2
7	5	5	5	3
8	5	5	5	3
9	5	5	5	3
10	5	5	5	3
11	5	5	5	5

Table 1.

It is a routine matter to extend Theorem A to arbitrary (that is, not necessarily prime) values of n. Further, we note that knowing the values of the unknowns on the left-hand side of (1), one can easily determine all the solutions (x, d, k, b, y, n) of (1).

Very recently, for $k = 5, 6$ and $n \ge 7$ the bounds $P_{k,n}$ have been improved to 3 by Bennett [B2]. Further, for $n = 2$ and positive x, Theorem A has been extended by Hirata-Kohno, Laishram, Shorey and Tijdeman [HLST]. In fact they did not handle (1) for some exceptional values of $b > 1$ for which (1) has been solved later by Tengely [Te]. Putting together the results in [HLST] and [Te], the following theorem holds.

Theorem B. *Equation (1) with $n = 2$, $d > 1$ and $5 \le k \le 100$ has no solution in positive integer x.*

In case of $b = 1$, the assumption $k \le 100$ can be replaced by $k \le 109$ in Theorem B (see [HLST]). When $n = 3$, Hajdu, Tengely and Tijdeman [HTT] obtained the following extension of Theorem A.

Theorem C. *Suppose that $n = 3$ and that (x, d, k, b, y) is a solution to equation (1) with $k < 32$*

such that $P(b) \le k$ *if* $4 \le k \le 12$ *and* $P(b) < k$ *if* $k = 3$ *or* $k \ge 13$. *Then* (x, d, k) *belongs to the following list:*

$$(-10, 3, 7), (-8, 3, 7), (-8, 3, 5), (-4, 3, 5), (-4, 3, 3), (-2, 3, 3),$$
$$(-9, 5, 4), (-6, 5, 4), (-16, 7, 5), (-12, 7, 5),$$
$$\text{and } (x, 1, k) \text{ with } -30 \le x \le -4 \text{ or } 1 \le x \le 5,$$
$$(x, 2, k) \text{ with } -29 \le x \le -3.$$

Further, if $b = 1$ *and* $k < 39$, *then we have*

$$(x, d, k, y) = (-4, 3, 3, 2), (-2, 3, 3, -2), (-9, 5, 4, 6), (-6, 5, 4, 6).$$

Theorems A, B and C confirm the conjecture of Erdős for the corresponding values of k and n. Moreover, under the additional assumptions made on $P(b)$ they provide the complete solution of (1) for $b > 1$ as well.

In the present paper we considerably extend Theorem A, up to $k < 35$. Our main result is the following theorem which proves Erdős' conjecture for $k < 35$.

Theorem 1.1 *The product of* k *consecutive terms in a coprime positive arithmetic progression with* $3 < k < 35$ *is never a perfect power.*

When $n \le 3$ or $k \le 11$, Theorem 1.1 follows from the above mentioned results. The remaining cases are covered by the following theorems.

Theorem 1.2 *Equation* (1) *has no solutions with* $n \ge 7$ *prime,* $12 \le k < 35$ *and* $P(b) \le P_{k,n}$, *where*

$$P_{k,n} = \begin{cases} 7, & \text{if } 12 \le k \le 22, \\ \frac{k-1}{2}, & \text{if } 22 < k < 35. \end{cases}$$

Theorem 1.3 *The only solutions to equation* (1) *with* $n = 5$, $8 \le k < 35$ *and* $P(b) \le P_{k,5}$, *with*

$$P_{k,5} = \begin{cases} 7, & \text{if } 8 \le k \le 22, \\ \frac{k-1}{2}, & \text{if } 22 < k < 35 \end{cases}$$

are given by

$$(k, d) = (8, 1),\ x \in \{-10, -9, -8, 1, 2, 3\}; \quad (k, d) = (8, 2),\ x \in \{-9, -7, -5\};$$
$$(k, d) = (9, 1),\ x \in \{-10, -9, 1, 2\}; \quad (k, d) = (9, 2),\ x \in \{-9, -7\};$$
$$(k, d) = (10, 1),\ x \in \{-10, 1\}; \quad (k, d, x) = (10, 2, -9).$$

Note that in the case $n = 5$ Theorem 1.3 yields an extension of Theorem A already for $8 \le k \le 11$.

Similarly as in [GyHS] and [BBGyH], results on equation (1) have a simple consequence for the rational solutions of equations of the form

$$u(u + 1) \dots (u + k - 1) = v^n. \tag{2}$$

More precisely, we have the following

Corollary 1.1 *Suppose that* $n \ge 2$, $1 < k < 35$ *and* $(k, n) \ne (2, 2)$. *Then equation* (2) *has no solutions in positive rational numbers* u, v.

For $k \leq 11$, this was proved in [BBGyH]. When $k > 11$, the statement is a straightforward consequence of Theorem 1.1, see [GyHS] and [BBGyH] for the necessary arguments. We note that equation (2) has been first studied by Sander [San].

In the case $k \leq 11$ and $n \geq 5$, equation (1) was reduced in Győry [Gy2], Győry, Hajdu and Saradha [GyHS], Bennett, Bruin, Győry and Hajdu [BBGyH] and Bennett [B2] to finitely many ternary equations of signature (n, n, n), $(n, n, 2)$ or $(n, n, 3)$. In our proofs we start with the same reduction strategy. However, for $k > 11$ and $n \geq 5$ prime, numerous new ternary equations arise which must be solved under certain arithmetic conditions. On solving these equations, in the case $n \geq 7$ we combine the Frey curve and modular Galois representation approach with local methods and some classical work on cyclotomic fields. Our results concerning ternary equations, which may be of independent interest, do not follow from straightforward application of the modularity of Galois representations attached to Frey curves, it is also necessary to understand the reduction types of these curves at certain small primes.

For $n = 5$, hardly any new information is available through the theory of "general" modular forms. In this case we make use of some classical and new results concerning equations of the shape $AX^5 + BY^5 = CZ^5$. The proof of these new results involves some cyclotomic and local considerations.

For increasing k, the number of possible k-tuples $(a_0, \ldots, a_{k-1})$ introduced in (3) below and hence also the number of arising systems of ternary equations grow so rapidly with k that, in contrast with the cases $k \leq 11$ treated in [Gy2], [GyHS], [BBGyH], [B2], practically it is already impossible to handle all cases one-by-one without using computer. The principal novelty of our paper is that we algorithmize our proof. For fixed k, we combine our algorithm for solving the new ternary equations with several sieves based on the arising ternary equations already solved, and we use a computer to exclude the solvability of enormous number of systems of ternary equations. Our general method seems to work for larger k as well, we do not see any theoretical obstacle to extend the results even further. However, the time consumption of the method increases rather rapidly, that is why we stopped at $k = 34$. As it can be of some interest, we give a few details here.

We have used a 2.4 MHz PC with a Quad processor to execute the calculations. To establish our new results for ternary equations of signature $(n, n, 2)$ (see Proposition 2.2) we have implemented our algorithm in Magma [BCP]. The total running time to prove Proposition 2.2 was about two weeks. The proof of Theorem 1.1 goes via proving Theorems 1.2 and 1.3. To verify the latter results, we have implemented our sieving procedures in Maple, separately for the cases $n \geq 7$ and $n = 5$. The program codes utilized in our computations are available from the authors on request. In both cases $n \geq 7$ and $n = 5$ the running time of the program was the following: a few seconds up to $k = 19$, a few minutes up to $k = 23$, a few hours up to $k = 29$, a few days for $k = 30, 31$ and about a week for $k = 32, 33, 34$ each. Altogether, after having Proposition 2.2 the calculations to prove Theorems 1.2 and 1.3 took about a month each. We mention that because of the extremely huge number of cases to be looked after, having only the "ternary" results it is hopeless to attack the problem without some additional, new "sieving" ideas. Vice versa, using only the sieving procedures with the previously known "ternary" results, one would be left with a lot of cases which are not handled. So to prove our theorems, we need to find a balanced and efficient combination of both techniques.

The organization of the paper is as follows. In the next section we introduce notation and summarize some old and establish some new results about ternary equations which we shall use in the proofs of Theorems 1.1, 1.2 and 1.3. The final section is devoted to the proofs of our theorems.

2. Notation and auxiliary results

For integers d, x, k with $k \geq 3$ and for indices $0 \leq i_1 < \cdots < i_l < k$ put

$$\Pi(i_1, \ldots, i_l) = (x + i_1 d) \ldots (x + i_l d)$$

and

$$\Pi_k = \Pi(0, 1, \ldots, k-1) = x(x+d) \ldots (x + (k-1)d).$$

Assume that (1) has a solution in non-zero integers x, d, k, b, y, n with the requested properties. Further, we may assume that n is an odd prime. From (1) one can then deduce that

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

where x_i is a non-zero integer and a_i is an nth power free positive integer with $P(a_i) \leq k$. For given k, there are only finitely many and effectively determinable such k-tuples $(a_0, a_1, \ldots, a_{k-1})$.

For brevity, we introduce the following notation. Write

$$[i_1, i_2, i_3]: \quad c_{i_1} a_{i_1} x_{i_1}^n + c_{i_3} a_{i_3} x_{i_3}^n = c_{i_2} a_{i_2} x_{i_2}^n \tag{4}$$

where $0 \leq i_1 < i_2 < i_3 < k$ and $c_{i_1} = (i_3 - i_2)/D, c_{i_2} = (i_3 - i_1)/D, c_{i_3} = (i_2 - i_1)/D$ with $D = \gcd(i_3 - i_2, i_3 - i_1, i_2 - i_1)$. Further, if $0 \leq j_1 < j_2 \leq j_3 < j_4 < k$ with $j_1 + j_4 = j_2 + j_3$, then let

$$[j_2, j_3] \times [j_1, j_4]: \quad a_{j_2} a_{j_3} (x_{j_2} x_{j_3})^n - a_{j_1} a_{j_4} (x_{j_1} x_{j_4})^n = (j_2 j_3 - j_1 j_4) d^2.$$

Given a k-tuple $(a_0, a_1, \ldots, a_{k-1})$, we obtain in this way a complicated system of ternary equations to be solved.

In the proofs of our theorems we use several results concerning ternary equations to solve the arising systems of equations. In this section we collect some earlier theorems and establish two new results for ternary equations which we need later on. We start with ternary equations of signature $(n, n, 2)$.

Proposition 2.1 *Let $n \geq 7$ be prime, u, v nonnegative integers, and A and B coprime positive integers. Then the following Diophantine equations have no solutions in pairwise coprime non-zero integers X, Y, Z with $XY \neq \pm 1$:*

$$X^n + 2^u Y^n = 3^v Z^2, \ u \neq 1 \tag{5}$$

$$X^n + Y^n = C Z^2, \ C \in \{2, 6\} \tag{6}$$

$$X^n + 5^u Y^n = 2Z^2 \ \textit{with } n \geq 11 \ \textit{if } u > 0 \tag{7}$$

$$AX^n + BY^n = Z^2, \ AB = 2^u p^v, \ u \neq 1, \ p \in \{11, 19\}. \tag{8}$$

Proof. This result is due to Bennett, Bruin, Győry and Hajdu [BBGyH]. □

The following result is new. For its formulation, we need a further standard notation. If m is a positive integer, let $\mathrm{rad}(m)$ denote the *radical* of m, i.e. the product of distinct prime divisors of m with the convention that $\mathrm{rad}(1) = 1$.

Set

$$I_1 = \{(2,1), (2,3), (2,5), (2,7), (6,1), (6,5), (10,1), (10,3), (14,1), (14,3), (22,1), (26,1), (30,1), (34,1), (38,1), (42,1), (46,1), (66,1), (70,1), (78,1), (102,1), (114,1), (130,1), (138,1)\},$$

$$I_2 = \{(3,1), (3,5), (5,1), (5,3), (7,1), (13,1), (15,1), (17,1), (21,1), (23,1), (33,1), (35,1), (39,1), (51,1), (57,1), (69,1), (165,1)\}$$

and

$$I_3 = \{(3,2),(5,6),(7,2),(11,2),(13,2),(15,2),(17,2),(19,2),(21,2),(23,2),(33,2),(35,2),(39,2)\}.$$

Proposition 2.2 *Let $n > 31$ be a prime, A, B and C pairwise coprime positive integers with $(rad(AB), C) \in I_1 \cup I_2 \cup I_3$ and $p \in \{11, 13, 17, 19, 23, 29, 31\}$ such that $p \nmid AB$. Then the equation*

$$AX^n + BY^n = CZ^2 \tag{9}$$

has no solutions in pairwise coprime non-zero integers X, Y, Z with $p \mid XY$, unless, possibly, in the cases listed in Table 2.

n	(rad(AB),C,p)
37	(2,7,31), (3,5,31), (6,5,31), (19,2,29), (22,1,31), (46,1,29), (46,1,31),
	(70,1,29)
41	(2,7,11), (21,2,13), (21,2,19), (21,2,29), (22,1,31), (46,1,31), (51,1,13),
	(102,1,13), (165,1,13), (165,1,31)
43	(5,6,13), (6,5,23)
47	(5,6,11), (5,6,29), (6,5,31), (15,2,11), (15,2,29), (33,2,13), (33,2,23), (39,2,31)
59	(3,5,31), (6,5,31), (39,2,23), (165,1,17)
61	(5,6,13), (5,6,29),(14,3,17), (15,2,13), (15,2,29), (39,2,17), (39,2,19)
67	(165,1,29)
71	(33,2,23)
79	(5,6,17), (15,2,17), (165,1,19)
83	(165,1,29)
89	(165,1,29), (165,1,31)
97	(5,6,31), (15,2,31), (165,1,29)
107	(5,6,31), (15,2,31)
127	(33,2,31), (165,1,29)
137	(5,6,23)
193	(5,6,31), (15,2,31)
229	(33,2,31)
239	(33,2,31), (165,1,29)

Table 2.

As we mentioned in the introduction, to prove our results in the case $n \geq 7$ we had to find an efficient combination of the "modular" and "sieving" techniques. A very great number of new ternary equations arose for each $k > 11$. We followed the strategy explained below. We first solved a few well-chosen ternary equations (considering only a small subset I of $I_1 \cup I_2 \cup I_3$ in Proposition 2.2), and using our sieves (which will be detailed in the next section) we tried to reduce each case $(a_0, a_1, \ldots, a_{k-1})$ to ternary equations either treated already in Propositions 2.1, 2.4 or 2.5 or belonging to I. After a while (for larger values of k) there were exceptional cases where such a reduction was unavailable. At that point we enlarged the set I in several steps and gradually we reached the finite sets I_1, I_2, I_3 in Proposition 2.2. By utilizing the equations occurring in Propositions 2.1, 2.4, 2.5 or corresponding to $I_1 \cup I_2 \cup I_3$ in Proposition 2.2 we were able to "cover" all cases $(a_0, a_1, \ldots, a_{k-1})$, i.e. to prove the insolubility of each arising system of equations. For the details we refer to the proof of Theorem 1.2.

Proof of Proposition 2.2. To solve our equations of the form (9) we shall apply the modular approach. Specifically, to a putative nontrivial solution X, Y, Z of (9) one can associate a Frey curve $E/\mathbb{Q}$, with the corresponding mod n Galois representation

$$\rho_n^E : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{F}_n)$$

on the n-torsion $E[n]$ of E. This representation arises from a cuspidal newform $f = \sum_{r=1}^{\infty} c_r q^r$ of weight 2 and trivial Nebentypus character. For details, we refer to [BS]. As usual, for a positive integer m let $\mathrm{rad}_2(m)$ denote the *2-free radical* of m, i.e. the product of distinct odd prime divisors of m, with the convention that $\mathrm{rad}_2(1) = 1$. It can be shown that the level N of the newform considered above is contained in $\{2^\alpha \cdot \mathrm{rad}_2(AB) \cdot \mathrm{rad}_2^2(C), \alpha = 0, 1, 2, 3, 5, 7\}$, $\{2^\alpha \cdot \mathrm{rad}_2(AB) \cdot \mathrm{rad}_2^2(C), \alpha = 1, 5\}$, or $\{256 \cdot \mathrm{rad}_2(AB) \cdot \mathrm{rad}_2^2(C)\}$, according as $(\mathrm{rad}(AB), C) \in I_1, I_2$ or I_3, respectively. The assumption that $p|XY$ for a prime p with $p \in \{11, 13, 17, 19, 23, 29, 31\}$ implies that if p is relatively prime to N then

$$\mathrm{Norm}_{K_f/\mathbb{Q}}(c_p \pm (p+1)) \equiv 0 \pmod{n}, \tag{10}$$

where c_p is the pth Fourier coefficient of f, and K_f is the field generated by the Fourier coefficients of f. This means that if (10) does not hold, we arrive at a contradiction. For the recipes of this technique see [B1] or [C].

We illustrate our approach in the case $(\mathrm{rad}(AB), C) = (38, 1)$. The corresponding levels are $19, 2 \cdot 19, 4 \cdot 19, 8 \cdot 19, 32 \cdot 19$ and $128 \cdot 19$. Suppose that X, Y, Z is a solution of the corresponding equation (9) in pairwise coprime non-zero integers such that $p \mid XY$, where p is a prime with $11 \le p \le 31$. Using a simple Magma program, we calculate the Fourier coefficients c_p of the corresponding one-dimensional newforms f at the levels considered above. Then we have

$$n \mid (c_p - (p+1))(c_p + p + 1) =: B_p. \tag{11}$$

For the corresponding higher dimensional newforms f at the levels under consideration we use a stronger sieve. Let

$$A_m = \mathrm{Norm}_{K_f/\mathbb{Q}}(c_m^2 - (m+1)^2) \prod_{\substack{|a| < 2\sqrt{m} \\ a \text{ is even}}} \mathrm{Norm}_{K_f/\mathbb{Q}}(c_m - a)$$

for $m = 3, 5, 7$. Our method yields now that

$$n \mid \gcd(B_p, A_3, A_5, A_7). \tag{12}$$

Consequently, if for some prime p with $11 \le p \le 31$ (11) and (12) do not hold for any f in question, then in the case $(\mathrm{rad}(AB), C) = (38, 1)$ equation (9) has no solution in pairwise coprime non-zero integers X, Y, Z with $p \mid XY$.

Using the same arguments for each equation considered in Proposition 2.2, we infer that equation (9) may have a solution with the prescribed properties only in the cases listed in Table 2.

We note that the Hasse-Weil bound implies that $B_p \neq 0$. Further, for the pairs $(\mathrm{rad}(AB), C)$ and for the higher dimensional case we omit A_m from the stronger sieve if $A_m = 0$ or $m|ABC$. □

Remark. We can choose further primes m for making a more stronger sieve. For example, in the case $(\mathrm{rad}(AB), C) = (165, 1)$ we can apply the sieve $n| \gcd(B_p, A_7, A_{61}, A_{73})$ for higher dimensional forms and we can exclude the cases

$$\begin{aligned}(n, p) = &(41, 13), (41, 31), (59, 17), (67, 29), (79, 19),\\ &(89, 31), (97, 29), (127, 29), (239, 29)\end{aligned} \tag{13}$$

as well. However, to find such appropriate primes m involves a long computation. Since for our later purposes Table 2 and its refinement excluding the cases listed in (13) are already sufficient, we do not continue this procedure.

We use ternary equations of signature $(n, n, 3)$ via the following result of Bennett [B2]. For a prime p and non-zero integer u, $\mathrm{ord}_p(u)$ denotes as usual the largest integer v for which $p^v \mid u$ holds.

Proposition 2.3 *Let n be a prime with $n \geq 7$. Then the equation*

$$x(x+d)(x+3d)(x+4d) = by^n \tag{14}$$

has the only solutions $(x, d, b, y) = (\pm 2, \mp 1, 4, 1)$ in non-zero integers x, d, b, y with $\gcd(x, d) = 1$ and $P(b) \leq 3$.

Proof. The statement is a simple consequence of a recent result of Bennett [B2]. However, for the sake of completeness we give the main steps of the proof.

Suppose to the contrary that x, d, b, y, n is a solution to (14) with $by \neq 0$. If $3 \nmid x(x+d)$ then using the notation (3) the identity $[1, 3] \times [0, 4]$ gives

$$a_1 a_3 (x_1 x_3)^n - a_0 a_4 (x_0 x_4)^n = 3d^2,$$

and we also have $\gcd(a_1 a_3 x_1 x_3, a_0 a_4 x_0 x_4) = 1$ and $P(a_0 a_1 a_3 a_4) \leq 2$. As either $\mathrm{ord}_2(a_1 a_3) = \mathrm{ord}_2(a_0 a_4) = 0$, or $\mathrm{ord}_2(a_1 a_3) = 0$ and $\mathrm{ord}_2(a_0 a_4) \geq 2$ (or vice versa), the statement follows from (5) of Proposition 2.1 in this case.

Otherwise, if $3 \mid x(x+d)$ then the identity $(x+d)^2(x+4d) - x(x+3d)^2 = 4d^3$ yields

$$a_1^2 a_4 (x_1^2 x_4)^n - a_0 a_3^2 (x_0 x_3^2)^n = 4d^3.$$

After simplifying with a suitable power of 2, we get an equality either of the form

$$X^n + 3^v Y^n = 2^u Z^3, \ u \geq 1, \ v \geq 3, \ \gcd(X, 3Y) = 1,$$

or of the shape

$$AX^n + BY^n = Z^3, \ AB = 2^u 3^v, \ u \geq 1, \ v \geq 3, \ \gcd(AX, BY) = 1.$$

However, using results from [BVY] and [B2] about certain ternary equations of signature $(n, n, 3)$, the statement follows also in this case. □

We will also use results on ternary equations of signature (n, n, n) which have been proved by the method involving Frey curves and modular forms; cf. [W], [K], [DM] and [R].

Proposition 2.4 *Let $n \geq 3$ and $u \geq 0$ be integers. Then the equation*

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

has no solutions in pairwise coprime non-zero integers X, Y, Z with $XYZ \neq \pm 1$.

Proof. This result is essentially due to Wiles [W] (in case $n \mid u$), Darmon and Merel [DM] (if $u \equiv 1 \pmod{n}$) and Ribet [R] (in the remaining cases for $n \geq 5$ prime); see also Győry [Gy2]. □

Proposition 2.5 *Let $n \geq 5$, and let A, B be coprime positive integers with $AB = 2^u 3^v$ or $2^u 5^v$, where u and v are non-negative integers with $u \geq 4$. Then the equation*

$$AX^n + BY^n = Z^n \tag{15}$$

has no solutions in pairwise coprime non-zero integers X, Y and Z.

Proof. This is Lemma 13 in [SS]. □

For $n = 5$, most of the above assertions on ternary equations cannot be applied. Then we shall use the following results as well.

Proposition 2.6 *Let $n \geq 3$ be an integer. All the solutions of the equation*

$$x(x+1)\dots(x+k-1) = by^n \tag{16}$$

in positive integers x, k, b, y with $k \geq 8$ and $P(b) \leq 7$ are given by

$$k \in \{8, 9, 10\} \quad \text{and} \quad x \in \{1, 2, \dots, p^{(k)} - k\}, \tag{17}$$

where $p^{(k)}$ denotes the least prime satisfying $p^{(k)} > k$.

Proof. It follows from a theorem of Saradha [Sar] that, in (16), $P(y) \leq k$. As was seen in Győry [Gy1], we then get $x \in \{1, 2, \dots, p^{(k)} - k\}$, whence $p^{(k)} > x + k - 1$. Denote by $p_{(k)}$ the greatest prime with $p_{(k)} \leq k$. Then, for $k \geq 11$, $p_{(k)} \geq 11$. Further, by Chebyshev's theorem $p^{(k)} < 2p_{(k)}$. In view of $p_{(k)} \leq k$ we have $p_{(k)} \mid x(x+1)\dots(x+k-1)$. But it follows that $2p_{(k)} > x + k - 1$. Hence (16) and $P(b) \leq 7$ give $p_{(k)}^n \mid x(x+1)\dots(x+k-1)$, which implies that $p_{(k)}^n \leq x + k - 1$. Hence we get $p_{(k)}^n \leq 2p^{(k)}$, a contradiction.

It remains to treat the case $k \in \{8, 9, 10\}$. Then $p^{(k)} = 11$ and it is easy to check that the values k, x listed in (17) are the solutions of (16). □

Lemma 2.1 *Let $n = 5$. For $k = 5$, $P(b) \leq 3$, and for $6 \leq k \leq 11$, $P(b) \leq 5$, equation (1) has the only solution $(x, d, k) = (-5, 2, 6)$ with $d \geq 2$.*

Proof. This is a special case of Theorem 1.2 in [BBGyH]. □

Lemma 2.2 *Let $n = 5$. Suppose that x, d, y, b provides a solution to equation (1) with $P(b) \leq 3$ and $k = 4$. Then either $(x, d) = (-3, 2)$, or, up to symmetry, $(a_0, a_1, a_2, a_3) = (4, 3, 2, 1)$ or $(9, 4, 1, 6)$.*

Proof. This is Lemma 6.3 in [BBGyH]. □

Let C be a 5th power free positive integer with $P(C) \leq 7$. Then we can write

$$C = 2^\alpha \cdot 3^\beta \cdot 5^\gamma \cdot 7^\delta \tag{18}$$

with non-negative integers $\alpha, \beta, \gamma, \delta$ not exceeding 4.

Proposition 2.7 *If the equation*

$$X^5 + Y^5 = CZ^5 \tag{19}$$

has solution in pairwise coprime non-zero integers X, Y and Z, then one of the following cases holds:
(i) $C = 2$, $X = Y = \pm 1$,
(ii) $C = 7^\delta$ with $1 \leq \delta \leq 4$, $5 \mid XY$, $5 \nmid Z$ and Z is odd,
(iii) $C \in \{2 \cdot 3^2 \cdot 7^\delta, 2^2 \cdot 3^4 \cdot 7^\delta, 2^3 \cdot 3 \cdot 7^\delta, 2^4 \cdot 3^3 \cdot 7^\delta\}$ with $1 \leq \delta \leq 4$ and $5 \mid Z$.

This implies that if in (19) $5 \nmid XYZ$, then (i) must hold. If in particular $P(C) \leq 5$, then Proposition 2.7 reduces to Proposition 6.1 of [BBGyH].

Proof. Let X, Y, Z be a solution of (19) in pairwise coprime non-zero integers. By results of Dirichlet and Dénes [De], it suffices to deal with the case $C > 2$ and $XYZ \neq \pm 1$. It follows from a theorem of Lebesgue ([Di], p. 738, item 37) that $5 \nmid C$ and

$$C \equiv \pm 1, \pm 7 \pmod{5^2}. \tag{20}$$

First assume that $5 \nmid Z$. We have

$$C^4 \equiv 1 \pmod{5^2} \quad \text{and} \quad 2^4 \not\equiv 1 \pmod{5^2},$$

whence

$$C^4 \not\equiv 2^4 \pmod{5^2}.$$

Applying Lemma 6.1 and Corollary 6.2 of [BGyP] to (19), we deduce that $5 \mid XY$, CZ is odd and

$$r^4 \equiv 1 \pmod{5^2} \tag{21}$$

for each prime divisor r of C. In view of (18) and (21) we infer that only $r = 7$ can hold, and (ii) follows.

Now suppose that $5 \mid Z$. The prime 5 being regular, a theorem of Maillet (see e.g. [Di], p. 759, item 167) implies that C must have at least three distinct prime factors. This means that in (18) $\gamma = 0$ and $\alpha, \beta, \delta \geq 1$. It is easy to check that together with (20) this gives (iii). □

3. Proofs

First we prove Theorems 1.2 and 1.3. As was mentioned already, we need to consider the cases $n = 5$ and $n \geq 7$ separately. The reason is that the theory of ternary equations cannot be efficiently applied in case of $n = 5$. We start with $n \geq 7$.

Proof of Theorem 1.2. To prove the theorem we eventually reduce the problem to the solution of several ternary diophantine equations. We now explain the main ideas of our proof. Suppose that under the assumptions of our theorem equation (1) has a solution. Observe that, by (3), to determine all solutions to (1) with fixed k it is sufficient to characterize the arithmetic progressions of the shape $a_0x_0^n, a_1x_1^n, \ldots, a_{k-1}x_{k-1}^n$, where the x_i are non-zero integers, and the a_i are positive integers such that $\gcd(a_0x_0^n, a_1x_1^n) = 1$,

$$P(a_i) \leq k \text{ and } a_i \text{ is } n\text{th power free for } i = 0, 1, \ldots, k-1. \tag{22}$$

Further, the assumption $P(b) \leq P_{k,n}$ implies that

$$n \mid \operatorname{ord}_p \left(\prod_{i=0}^{k-1} a_i \right) \text{ for all primes } p > P_{k,n}. \tag{23}$$

In particular, if p is a prime and $u \geq 1$ is an integer with $p^u \mid a_ix_i^n$ then $p^u \mid a_jx_j^n$ if and only if $p^u \mid i - j$. This assertion will be used later on without any further reference.

The number of possible k-tuples $(a_0, a_1, \ldots, a_{k-1})$ with properties (22) and (23) grows very rapidly with k, and it is impossible to look at them one-by-one if k is relatively large. So we apply the following strategy. We exclude the possible coefficient k-tuples $(a_0, a_1, \ldots, a_{k-1})$ in several steps, using certain procedures in a well-determined order. A k-tuple will be excluded after assuring that in the corresponding case equation (1) has no solution. We start with arguments with which we can exclude a great number of k-tuples $(a_0, a_1, \ldots, a_{k-1})$. By induction we can exclude a lot of possibilities. Namely, if for some $\ell \geq 3$ $P(a_0 \ldots a_{\ell-1}) \leq P_{\ell,n}$ or $P(a_{k-\ell} \ldots a_{k-1}) \leq P_{\ell,n}$ holds, then the statement follows either by induction, or by Theorem A. By this observation the number of k-tuples to be considered can be reduced drastically. Subsequently, after each step, it will be simpler and simpler to manage and exclude the remaining k-tuples. We shall explain the details later on, at the sieves. Further, we provide examples to illustrate how the sieves work.

In what follows, we always assume that k is fixed with $11 < k < 35$. We use the following convention. Let $2 = p_1 < p_2 < \cdots < p_{\pi(k-1)}$ be the primes $\leq k - 1$, where $\pi(k-1)$ denotes the number of primes not exceeding $k-1$. Observe that as $P_{k,n} < k$ for $n \geq 7$, by (23) we have $P(a_i) < k$ in (22) for all $i = 0, 1, \ldots, k-1$. We indicate the distribution of the primes $p_1, \ldots, p_{\pi(k-1)}$ among the $a_ix_i^n$ resp. a_i (or in other words, the prime divisors $\leq k-1$ of the $a_ix_i^n$ resp. a_i) by the help of

certain $\pi(k-1)$-tuples of the form $(m_{\pi(k-1)},\dots,m_1)$. For $3\le j\le \pi(k-1)$ let

$$m_j\in\{\times,0,1,\dots,p_j-1\} \tag{24}$$

where $m_j=\times$ if $p_j\nmid \Pi_k$ (i.e. p_j does not divide $x(x+d)\dots(x+(k-1)d)$); otherwise, let m_j denote the integer from among $0,1,\dots,p_j-1$ for which $p_j\mid x+m_jd$. In our proof first we consider such cases when it is not specified which terms of the progression $x,x+d,\dots,x+(k-1)d$ are divisible by 2 and 3. Then we write $m_j=*$ for $j=1,2$. In such a case we say that the distribution of $p_1,\dots,p_{\pi(k-1)}$ among the $a_ix_i^n$ resp. a_i corresponds to the $\pi(k-1)$-tuple $(m_{\pi(k-1)},\dots,m_1)$. By means of these $\pi(k-1)$-tuples we shall get information about the location of the coefficients a_i without "large" prime factors which will be of crucial importance in our proof. To each of these $\pi(k-1)$-tuples there correspond a great number of k-tuples $(a_0,a_1,\dots,a_{k-1})$ under consideration. Hence the use of our tests sieving with all $\pi(k-1)$-tuples of the form $(m_{\pi(k-1)},\dots,m_3,*,*)$ will enable us to exclude simultaneously full branches of k-tuples $(a_0,a_1,\dots,a_{k-1})$ at the same time. This makes our algorithm very efficient. Our first three tests below seem to be especially efficient, at least for the range of k under consideration.

Later we shall need to refine our algorithm by specifying also those terms of $x,x+d,\dots,x+(k-1)d$ which are divisible by 2 and/or 3. For $j=1$ and 2, let

$$m_j\in\{\times,0,1,\dots,k-1\} \tag{25}$$

such that, as in the case $j\ge 3$, $m_j=\times$ if $p_j\nmid\Pi_k$; otherwise let m_j be such a number from $\{0,1,\dots,k-1\}$ for which $p_j\mid x+m_jd$ and

$$\operatorname{ord}_{p_j}(x+m_jd)=\max_{0\le\ell\le k-1}\operatorname{ord}_{p_j}(x+\ell d).$$

This will enable us to calculate the exact orders of the primes $p_1=2$ and $p_2=3$ in the numbers $a_ix_i^n$. Then we shall continue our proof with further tests, sieving first with all possible $\pi(k-1)$-tuples of the form $(m_{\pi(k-1)},\dots,m_3,m_2,*)$, $(m_{\pi(k-1)},\dots,m_3,*,m_1)$ and thereafter with tuples $(m_{\pi(k-1)},\dots,m_3,m_2,m_1)$ with m_1,m_2 satisfying (25). Finally, a relatively few number of k-tuples $(a_0,a_1,\dots,a_{k-1})$ will be left with some small exponents n which will be excluded by means of a local sieve.

In our sieves we shall use ternary equations. We shall distinguish between (n,n,n), $(n,n,3)$ and $(n,n,2)$-sieves, according as the ternary equations involved are of signature (n,n,n), $(n,n,3)$ or $(n,n,2)$.

(n,n,n)-sieve I. Suppose that we are dealing with a $\pi(k-1)$-tuple $T=(m_{\pi(k-1)},\dots,m_3,*,*)$. First (by the help of T) we check whether there exists an arithmetic progression i_1,i_2,i_3 with $0\le i_1<i_2<i_3\le k-1$ such that $P(a_{i_1}a_{i_2}a_{i_3})\le 3$ and $i_1\equiv i_2\equiv i_3\pmod 3$. If there are such indices, then by Proposition 2.4 the identity $[i_1,i_2,i_3]$ implies that $3\mid x+i_1d$ (and then consequently $3\mid x+i_2d, x+i_3d$) must be valid, otherwise we are done. Then we apply an exhaustive search for indices i_4,i_5 with which some appropriately chosen identities of the form (4) lead to a contradiction. For example, assume that $P(a_2a_5a_8)\le 3$. Then by $[2,5,8]$ we know that $3\mid x+2d, x+5d, x+8d$. Suppose further that $P(a_4a_6)\le 3$. Then $\gcd(x,d)=1$ shows that $P(a_4a_6)\le 2$. Hence, as exactly one of $\operatorname{ord}_3(x+2d)\ge 2$, $\operatorname{ord}_3(x+5d)\ge 2$, $\operatorname{ord}_3(x+8d)\ge 2$ holds, one of the identities $[2,4,5],[5,6,8],[2,6,8]$ (again by Proposition 2.4) leads to a contradiction.

After having checked all the possible $\pi(k-1)$-tuples T of the form $(m_{\pi(k-1)},\dots,m_3,*,*)$ and all the possible triples (i_1,i_2,i_3) in question, we exclude the tuples T and the corresponding k-tuples $(a_0,a_1,\dots,a_{k-1})$ which lead in this way to a contradiction.

As an example, take $k=15$ and let

$$T=(0,3,0,\times,*,*).$$

Then we have $P(a_2a_4a_5a_6a_8) \leq 3$, and by the previous argument T and the corresponding 15-tuples can be excluded.

$(n, n, 3)$-sieve. Suppose that a $\pi(k-1)$-tuple T survives the previous test. Then we try to find an index i_0 and a difference d_0 with $P(d_0) \leq 3$, $i_0 - 2d_0 \geq 0$ and $i_0 + 2d_0 \leq k-1$ such that

$$P(a_{i_0-2d_0}a_{i_0-d_0}a_{i_0+d_0}a_{i_0+2d_0}) \leq 3. \tag{26}$$

Let $g = \gcd(x + (i_0 - 2d_0)d, d_0d)$. Obviously, $\gcd(x, d) = 1$ and $P(d_0) \leq 3$ imply that $P(g) \leq 3$. Putting $X = (x + (i_0 - 2d_0)d)/g$, $D = d_0d/g$ and using (3) and (26), we infer that for these X, D the equation

$$X(X + D)(X + 3D)(X + 4D) = BY^n$$

has a solution in non-zero integers B, Y with $P(B) \leq 3$. However, this by Proposition 2.3 implies $X + 2D = 0$ which is impossible. We check all the possible i_0, d_0, and exclude again all the T and all the corresponding k-tuples leading in this way to a contradiction.

To see an example, let $k = 15$ and

$$T = (0, 3, 4, 2, *, *).$$

Note that T survives the previous test. We have $P(a_5a_6a_8a_9) \leq 3$, hence we can take $i_0 = 7$ and $d_0 = 1$, and by the above test T and the corresponding 15-tuples can be excluded.

(n, n, n)-sieve II. Consider a $\pi(k-1)$-tuple $T = (m_{\pi(k-1)}, \ldots, m_3, *, *)$ which is not excluded by the previous tests. We let m_1 run through the set $\{\times, 0, 1, \ldots, k-1\}$ and examine all $\pi(k-1)$-tuples of the form $T' = (m_{\pi(k-1)}, \ldots, m_3, *, m_1)$. We perform an exhaustive search to find an identity of the form $[i_1, i_2, i_3]$ leading to a ternary equation of the shape $AX^n + BY^n = Z^n$ such that $\gcd(A, B) = 1$, and AB is either of the form 2^u3^v or 2^u5^v, with $u \geq 4$ in both cases. If we succeed, then the corresponding $\pi(k-1)$-tuple and k-tuples can be excluded by Proposition 2.5.

As an example, choose $k = 15$ and

$$T' = (0, 3, 1, 4, *, 11).$$

Note that this $\pi(k-1)$-tuple cannot be excluded by the previous tests. However, taking the identity $[2, 10, 11]$, after cancelling an appropriate power of 3 we get a ternary equation of the form $AX^n + BY^n = Z^n$ with $\gcd(A, B) = 1$ and $AB = 2^u3^v$, $u \geq 4$. Hence we can exclude T' and the corresponding 15-tuples.

$(n, n, 2)$-sieve I. Suppose that a $\pi(k-1)$-tuple $T' = (m_{\pi(k-1)}, \ldots, m_3, *, m_1)$ passes the previous tests. Then we consider all $\pi(k-1)$-tuples of the form $T^* = (m_{\pi(k-1)}, \ldots, m_2, m_1)$ with $m_2 \in \{\times, 0, 1, \ldots, k-1\}$. We search for an identity of the form $[j_2, j_3] \times [j_1, j_4]$ which leads to a ternary equation of the shape $AX^n + BY^n = CZ^2$ such that $\gcd(A, B, C) = 1$ and one of the following holds: $AB = 2^u$ $(u \neq 1)$, $C = 3^v$; $AB = 1$, $C \in \{2, 6\}$; $AB = 2^up^v$ $(u \neq 1, p \in \{11, 19\})$, $C = 1$. Then applying Proposition 2.1, the corresponding $\pi(k-1)$-tuples T^* and corresponding k-tuples $(a_0, a_1, \ldots, a_{k-1})$ can be excluded.

For example, choose again $k = 15$, and take

$$T^* = (0, 3, 1, 2, 0, 3).$$

Note that T^* passes all the previous sieves. However, the identity $[5, 10] \times [4, 11]$ gives rise to a ternary equation of the form $X^n + 4Y^n = 3Z^2$, which leads to a contradiction, as explained above.

$(n, n, 2)$-sieve II. Assume that a $\pi(k-1)$-tuple T^* survives the previous tests. Then we try to find again an identity of the form $[j_2, j_3] \times [j_1, j_4]$, leading to a ternary equation $AX^n + BY^n = 2Z^2$ with $AB = 5^u$, $u \geq 1$. Then Proposition 2.1 implies that $n = 7$. We collect these $\pi(k-1)$-tuples T^*

to a set S, and make a note that these tuples T^* have to be reconsidered later separately for the exponent $n = 7$.

As an example, let $k = 15$ and let

$$T^* = (0, 3, 4, 1, 8, 3).$$

As one can easily see, T^* survives the previous tests. However, after cancellations, the identity $[5, 6] \times [2, 9]$ leads to a ternary equation of the shape $X^n + 5^u Y^n = 2Z^2$ with $u > 0$. Then Proposition 2.1 gives that $n = 7$ and we can put T^* into S.

$(n, n, 2)$-sieve III. Assume that a $\pi(k-1)$-tuple T^* survives the previous tests. Then we search for an identity $[j_2, j_3] \times [j_1, j_4]$ such that the implied ternary equation satisfies the conditions of Proposition 2.2. Then this proposition and the subsequent Remark yield that n is (explicitly) bounded for the case corresponding to T^*. We put these $\pi(k-1)$-tuples T^* into the set S, and to each of them we attach the list of the corresponding "exceptional" exponents, to be checked later.

For example, let $k = 15$ and

$$T^* = (0, 3, 1, 4, 0, 0).$$

As one can check, this $\pi(k-1)$-tuple passes each earlier sieve. However, the identity $[6, 11] \times [3, 14]$ gives (after cancellations) a ternary equation of the shape $X^n + 5^u Y^n = Z^2$ with $u \geq 1$ and $11 \mid XY$, and by Proposition 2.2 we get that $n \leq 31$. Then we can put T^* into S.

After accomplishing the above procedures one can exclude (or put into S) all the $\pi(k-1)$-tuples $(m_{\pi(k-1)}, \ldots, m_1)$ and the corresponding k-tuples $(a_0, a_1, \ldots, a_{k-1})$ for all values of k, up to very few exceptions. In the remaining cases we proceed as follows. Let $(a_0, a_1, \ldots, a_{k-1})$ be a k-tuple which passes all the above tests. Let $T^* = (m_{\pi(k-1)}, \ldots, m_1)$ be the corresponding $\pi(k-1)$-tuple, with m_j subject to (24) and (25) for $j \geq 3$ and $j = 1, 2$, respectively. We "split" T^* into several $\pi(k-1)$-tuples, according to which indices i, j $\mathrm{ord}_5(x + id)$ and $\mathrm{ord}_7(x + jd)$ is maximal. Then for these "refined" $\pi(k-1)$-tuples we try to find identities either of the form $[i_1, i_2, i_3]$ or of the shape $[j_2, j_3] \times [j_1, j_4]$ such that Proposition 2.1, 2.2, 2.4 or 2.5 yields a contradiction. Obviously, for this purpose we can use the sieves explained above. On these "refined" $\pi(k-1)$-tuples we have more information than about T^*. Hence it often happens that a sieve which did not work for T^* itself excludes a "refined" $\pi(k-1)$-tuple together with the corresponding k-tuples $(a_0, a_1, \ldots, a_{k-1})$. In fact this is exactly what we perform in all the remaining cases. After having gone through all the remaining $\pi(k-1)$-tuples $(m_{\pi(k-1)}, \ldots, m_1)$ and the corresponding k-tuples $(a_0, a_1, \ldots, a_{k-1})$, we are left with the $\pi(k-1)$-tuples in the set S only. All the other $\pi(k-1)$-tuples (and the corresponding k-tuples) are already excluded.

We show an example to illustrate the above method. For this purpose let $k = 24$ (there are no exceptional k-tuples for $k \leq 23$), and let

$$T^* = (m_9, \ldots, m_1) = (0, 0, 6, 10, 3, 1, 2, 4, 7).$$

One can check that this tuple passes all the previous sieves. Then we "split" T^* into 9-tuples of the form $(0, 0, 6, 10, 3, m_4', m_3', 4, 7)$ with

$$m_3' \in \{2, 7, 12, 17, 22\} \quad \text{and} \quad m_4' \in \{1, 8, 15, 22\}.$$

Here for fixed m_j' $(j = 3, 4)$ we assume that

$$\mathrm{ord}_{p_j}(x + m_j' d) = \max_{0 \leq \ell \leq 23} \mathrm{ord}_{p_j}(x + \ell d).$$

We try to find an identity of the form $[i_1, i_2, i_3]$ or $[j_2, j_3] \times [j_1, j_4]$ which by Proposition 2.1, 2.2, 2.4 or 2.5 leads to a contradiction. In the present example, noting that $\mathrm{ord}_2(a_7 x_7^n) \geq 5$, one can easily check that for $m_3' = 2$ and $m_3' \in \{12, 17, 22\}$ the identity $[5, 7, 17]$ and $[2, 5, 7]$, respectively, leads to

a contradiction by Proposition 2.5, regardless of the value of m_4'. Furthermore, for $m_3' = 7$, $[2, 5, 17]$ yields a contradiction by Proposition 2.4, for any m_4'.

It remains to check the $\pi(k-1)$-tuples in S and the corresponding k-tuples $(a_0, a_1, \dots, a_{k-1})$ for the remaining small values of the exponent n. This can be done very easily by the following local argument.

Local sieve. For each element in S and for the corresponding remaining values of n (obtained by Propositions 2.1, 2.2 and the subsequent Remark) we consider the problem locally. For each such n we choose a prime q of the form $q = tn + 1$, with t as small as possible. For example, in the cases $n = 11, 13, 17, 19, 23$ we take $q = 23, 53, 103, 191, 47$, respectively. Then we check the putative arithmetic progressions modulo q in the following way. By the choice of the corresponding modulus, the use of Euler-Fermat theorem guarantees that x_i^n may assume only very few values modulo q. Checking all the cases one-by-one and using that the numbers $a_i x_i^n$ $(i = 0, 1, \dots, k-1)$ should be consecutive terms of an arithmetic progression, we get a contradiction in each case.

To illustrate the local argument, chose $k = 15$, $n = 23$ and take the $\pi(k-1)$-tuple

$$(0, 3, 1, 4, 0, 0)$$

from S. Observe that the 23rd powers modulo 47 are exactly $-1, 0, 1$. Hence in this case the putative progression $a_i x_i^{23}$ $(i = 0, 1, \dots, 14)$ should be of the form

$$\pm 2^{\alpha_0} 3^{\beta_0} 13^{\nu_0}, \pm 7^{\delta_1}, \pm 2, \pm 3 \cdot 11^{\varepsilon_3}, \pm 2^2 \cdot 5^{\gamma_4}, \pm 1, \pm 2 \cdot 3, \pm 1, \pm 2^3 7^{\delta_8}, \pm 3^2 5^{\gamma_9},$$

$$\pm 2, \pm 1, \pm 2^2 3, \pm 13^{\nu_{13}}, \pm 2 \cdot 5^{\gamma_{14}} 11^{\varepsilon_{14}}$$

modulo 47 with non-negative exponents smaller than 23 and with the possible diversion that at most one of the terms can be equal to 0. However, as one can easily check even by hand, such an arithmetic progression does not exist. In all other cases a similar argument works, and this completes the proof. □

Proof of Theorem 1.3. Let (x, d, k, b, y) be a solution of (1) with $n = 5$. For $d = 1$, each factor $x + id$ in (1) must be positive or negative. Then we can reduce equation (1) to the case $x > 0$, and Proposition 2.6 applies to obtain the solutions listed in the theorem.

In what follows, we assume that $d \geq 2$. Further, if $k \leq 11$, in view of Lemma 2.1 we can restrict ourselves to the case $7 \mid a_0 \dots a_{k-1}$.

For $8 \leq k \leq 13$, most of our work in proving Theorem 1.3 is concentrated on the case $k = 8$. For the values $9 \leq k \leq 13$ we can then proceed by induction on k. We note that the above sieves can be utilized to prove our theorem for larger values of k only. For $k \leq 13$, too many exceptions would remain after using our sieves. Hence for these values of k we shall handle the arising k-tuples $(a_0, a_1, \dots, a_{k-1})$ without using sieves, tests and computer.

The case $k = 8$. If $7 \mid a_0, a_7$ then omitting in (1) x and $x + 7d$, we arrive at the case $k = 6$, and by Lemma 2.1 we get $x + d = -5$, $d = 2$. This yields the solution $(x, d) = (-7, 2)$. If $7 \mid a_1$ or $7 \mid a_6$, then we omit the factors $x, x + d$ resp. $x + 6d, x + 7d$ and we obtain in a similar way the solutions $(x, d) = (-9, 2), (-5, 2)$.

It remains the case $7 \mid a_2 \dots a_5$. By symmetry it suffices to consider the case $7 \mid a_2 a_3$.

First suppose that $7 \mid a_2$. If $5 \nmid a_0 \dots a_7$, then Lemma 2.1 applied to $\Pi(3, 4, 5, 6, 7)$ shows that there is no solution. If $5 \mid x + 2d$, then $5 \mid x + 7d$ and for $(i_1, i_2, i_3, i_4) = (3, 4, 5, 6)$ we get

$$\Pi(i_1, i_2, i_3, i_4) = b_1 y_1^5, \tag{27}$$

where b_1, y_1 are non-zero integers with $P(b_1) \leq 3$. Then Lemma 2.2 gives that either $(x + 3d, d) =$

$(-3,2)$ which leads to the solution $(x,d)=(-9,2)$ or, up to symmetry,

$$(a_3,a_4,a_5,a_6)=(4,3,2,1) \quad \text{or} \quad (9,4,1,6).$$

If (a_3,a_4,a_5,a_6) equals $(4,3,2,1)$ or $(1,2,3,4)$, then applying Proposition 2.7 to $[0,3,6]$ we arrive at a contradiction. In the remaining cases Proposition 2.7 can be applied to $[1,3,5]$ or $[0,1,3]$ and we get again a contradiction.

Next assume that $5 \mid x$. If $3 \nmid \Pi_8$ or $3 \mid x$, we can apply Proposition 2.7 to $[1,4,7]$. Otherwise, to obtain a contradiction Proposition 2.7 can be applied to $[1,3,7]$, $[4,6,7]$ or $[1,3,4]$ if $3 \mid x+d$, and to $[1,4,7]$ if $3 \mid x+2d$.

Let $5 \mid x+d$. If $3 \nmid \Pi_8$ or $3 \mid x$, one of the equations $[3,4,5]$, $[0,3,4]$, $[5,6,7]$, $[4,5,7]$ leads to a contradiction by Proposition 2.7. In the remaining cases at least one of the equations $[3,4,5]$, $[0,1,3]$, $[4,5,7]$, $[0,3,6]$, $[3,5,7]$, $[0,2,4]$ is not solvable by Proposition 2.7.

Let now $5 \mid x+3d$. If $3 \nmid \Pi_8$ or $3 \mid x(x+2d)$, then using Proposition 2.7, equation $[1,4,7]$ leads to a contradiction. If $3 \mid x+d$, we get the equation (27) with $(i_1,i_2,i_3,i_4)=(4,5,6,7)$. Then Lemma 2.2 gives that either $(x+4d,d)=(-3,2)$ which does not yield any solution of (1) or, up to symmetry,

$$(a_4,a_5,a_6,a_7)=(4,3,2,1) \quad \text{or} \quad (9,4,1,6).$$

It is easy to verify that only the second option can occur. Then $[0,3,6]$ or $[1,4,5]$ has no solution, according as (a_4,a_5,a_6,a_7) equals $(9,4,1,6)$ resp. $(6,1,4,9)$.

Finally assume that $5 \mid x+4d$. Then applying Lemma 2.2 to equation (27) with $(i_1,i_2,i_3,i_4)=(1,3,5,7)$ we get that either $(x+d,d)=(-3,2)$ which yields the solution $(x,d)=(-5,2)$ of (1) or, up to symmetry,

$$(a_1,a_3,a_5,a_7)=(4,3,2,1) \quad \text{or} \quad (9,4,1,6).$$

It follows that in each case $x+d, x+3d, x+5d$ and $x+7d$ are all divisible by 4 which contradicts the assumption that $\gcd(x,d)=1$.

Next consider the case $7 \mid x+3d$. If $5 \nmid a_0 \dots a_7$ or if $5 \mid x+3d$ then we have (27) with $(i_1,i_2,i_3,i_4)=(4,5,6,7)$. Then, by Lemma 2.2, (a_4,a_5,a_6,a_7) equals $(4,3,2,1)$, $(1,2,3,4)$, $(9,4,1,6)$ or $(6,1,4,9)$. Now Proposition 2.7 proves that $[1,4,7]$, $[2,3,4]$ or $[1,3,5]$, $[0,1,2]$ resp. $[1,4,5]$ is not solvable.

Let now $5 \mid x$. If $3 \nmid x+d$ then Proposition 2.7 applies to $[1,4,7]$, leading to a contradiction. If $3 \mid x+d$, then by Proposition 2.7 at least one of the equations $[2,4,6]$, $[1,4,7]$, $[4,6,7]$, $[1,2,4]$ has no solution.

Assume now that $5 \mid x+d$. If $3 \nmid \Pi_8$ or $3 \mid x$, then by Proposition 2.7 at least one of the equations $[0,2,4]$, $[2,3,4]$ and $[5,6,7]$ has no such a solution which would yield a solution of (1). Let now $3 \mid x+d$. If x is odd then equation $[0,1,2]$ is not solvable by Proposition 2.7. Otherwise, if x is even then by $\gcd(x,d)=1$ d is odd, whence $2^2 \mid x$ or $2^2 \mid x+2d$. If $3^2 \nmid x+7d$ or $3^2 \mid x+7d$ and $2^2 \mid x$ then Proposition 2.7 shows that $[4,5,7]$ resp. $[2,4,5]$ is not solvable. When $3^2 \mid x+7d$ and $2^2 \mid x+2d$, then using the fact that

$$X^5 \equiv 0, \pm 1 \pmod{11} \tag{28}$$

for any integer X, we deduce that $x_1 \equiv x_4 \equiv x_5 \equiv 0$ is the only solution of $[1,4,5] \pmod{11}$ which leads to a contradiction.

Next let $3 \mid x+2d$. If x is odd or $\mathrm{ord}_2(x)=\mathrm{ord}_2(x+4d)$, then in view of Proposition 2.7 $[0,2,4]$ has no solution. As $\gcd(x,d)=1$, it remains the case when $2^3 \mid x$ or $2^3 \mid x+4d$. If $3^2 \nmid x+2d$ and $3^2 \nmid x+5d$, then $[2,4,5]$ is not solvable by Proposition 2.7.

Assume that $3^2 \mid x+2d$. If $2^3 \mid x$, then $[4,5,7]$ yields the only solution

$$x_4^5 \equiv x_5^5 \equiv x_7^5 \equiv \pm 1 \pmod{11}.$$

Together with (3) this gives $d \equiv \mp 1 \pmod{11}$ and $x \equiv \pm 8 \pmod{11}$. Then $x+d \equiv 5x_1^5 \pmod{11}$ with $5 \nmid x_1$ cannot hold. Thus $5^2 \mid x+d$, whence $\mathrm{ord}_5(x+6d)=1$, and $[5,6,7]$ yields a contradiction $\pmod{11}$. If $2^3 \mid x+4d$, then $[0,5,7]$ is not solvable $\pmod{11}$. Finally, consider the case $3^2 \mid x+5d$. If $2^3 \mid x+4d$, then Proposition 2.5 shows that equation $[1,4,7]$ is not solvable. By assumption we have $5 \mid x+6d$. If $2^3 \mid x$, then $[1,4,7]$ or $[2,4,6]$ is not solvable $\pmod{11}$, according as $5^2 \mid x+6d$ or not.

Let now $5 \mid x+2d$. If $3 \nmid \Pi_8$, then solving $[4,5,6]$ by means of Proposition 2.7 we do not get any solution for (1). First assume that $3 \mid x+d$. Then, by Proposition 2.7 and $5 \nmid x(x+6d)$, $[0,3,6]$ or $[4,5,6]$ has no solution, according as $2^2 \nmid x$ or $2^2 \mid x$. Next let $3 \mid x+2d$. Then Proposition 2.7 implies that $[0,1,4]$, $[0,4,6]$ or $[1,2,4]$ is not solvable, according as $2^3 \mid x$, $2^3 \mid x+4d$ or $\mathrm{ord}_2(x) = \mathrm{ord}_2(x+4d)$. Assume now that $3 \mid x$. If $\mathrm{ord}_2(x+d) = \mathrm{ord}_2(x+5d)$ then $[1,3,5]$ is not solvable in view of Proposition 2.7. It remains the case $2^3 \mid x+d$ or $2^3 \mid x+5d$. Then Proposition 2.5 proves that $[0,1,4]$ has no solution.

Finally, assume that $5 \mid x+4d$. If $3 \nmid \Pi_8$ or $3 \mid x+2d$, then at least one of the equations $[0,3,6]$, $[1,4,7]$ is not solvable by Proposition 2.7. If $3 \mid x$, then, by Proposition 2.7, $[1,2,5]$, $[1,5,7]$ or $[1,3,5]$ is not solvable, according as $2^3 \mid x+d$, $2^3 \mid x+5d$ or $\mathrm{ord}_2(x+d) = \mathrm{ord}_2(x+5d)$. If $3 \mid x+d$, then $[0,2,6]$, $[2,5,6]$ or $[2,4,6]$ has no solution, according as $2^3 \mid x+2d$, $2^3 \mid x+6d$ or $\mathrm{ord}_2(x+2d) = \mathrm{ord}_2(x+6d)$. This completes the proof of the case $k=8$.

The cases $k = 9, 10, 11$. In view of $P(b) \le 7$, (1) implies (3) with $P(a_i) \le 7$ for each i. Hence we deduce from (1) that

$$\Pi(0,1,\dots,k-2) = b_2 y_2^5 \tag{29}$$

where b_2, y_2 are non-zero integers with $P(b_2) \le 7$. We can now proceed by induction on k. For $k=9$, we apply to (29) our results proved above in the case $k=8$ and we infer that all the solutions of (1) with $d \ge 2$ are given by $d=2$, $x \in \{-9,-7\}$. For $k=10$, we obtain similarly that $d=2$, $x=-9$, while, for $k=11$, we do not get any solution for (1).

The cases $k = 12, 13$. First suppose that at most one factor, say $x+id$, is divisible by 11. Then $11 \nmid a_i$, and we get (29). Using again induction on k, we infer that in these cases (1) has no solution. If two factors, say $x+id$ and $x+jd$ with $i<j$, are divisible by 11 then we deduce from (1) that

$$\Pi(i+1,\dots,j-1) = b_3 y_3^5, \tag{30}$$

where $j = i+11$ and b_3, y_3 are non-zero integers with $P(b_3) \le 7$. We can now apply our results obtained for $k=10$ and it follows that no new solutions of (1) arise.

The cases $k \ge 14$. From this point on it is definitely worth algorithmizing the proof and using a computer. We execute the following tests. As they are rather similar to those used in case of $n \ge 7$, we apply the same notation.

$(5,5,5)$-sieve I-II. We apply the sieves **(n,n,n)-sieve I** and **(n,n,n)-sieve II** like in case of $n \ge 7$, but consecutively. As the underlying Propositions 2.4 and 2.5 are valid also for $n=5$, this can be done without any restrictions.

$(5,5,5)$-sieve III. This is a new sieve. From this point on we work with $\pi(k-1)$-tuples T^* of the same type $(m_{\pi(k-1)},\dots,m_1)$ as in **$(n,n,2)$-sieve I** in the proof of Theorem 1.2, that is m_j satisfies (24) for $j \ge 3$ and (25) for $j=1,2$. For each such $\pi(k-1)$-tuple T^* we check whether it is possible to find three terms of the arithmetic progressions under consideration such that their corresponding

linear combination leads to an equation of the form

$$X^5 + Y^5 = CZ^5$$

with $P(C) \leq 5$. If we can find such terms, then the corresponding $\pi(k-1)$-tuple T^* and the k-tuples $(a_0, a_1, \ldots, a_{k-1})$ can be excluded by Proposition 2.7. (We can easily take care of the cases corresponding to part (i) of the proposition.) If a $\pi(k-1)$-tuple T^* cannot be excluded in this way, we put it into a set S.

Sieve modulo 11. Similarly as in **Local sieve**, we test all elements of S locally. In this case we can obviously use the prime 11 because of (28). By the help of the same method as in the proof of Theorem 1.2, all $\pi(k-1)$-tuples in S and hence all the k-tuples $(a_0, a_1, \ldots, a_{k-1})$ can be excluded, and the proof is complete. □

Proof of Theorem 1.1. We must prove that for $3 < k < 35$ and $b = 1$, equation (1) has no solution in positive integers x, d, y and n. Suppose that such a solution exists. By the result of Erdős and Selfridge we have $d > 1$. Further, as was mentioned earlier, we may assume without loss of generality that n is prime. If $n = 2$ or $n = 3$, then the statement immediately follows from Theorem B and Theorem C, respectively. In case of $n = 5$, Theorem 1.1 is a consequence of Theorem A and Theorem 1.3. Finally, for any prime $n \geq 7$ Theorem A together with Theorem 1.2 imply the assertion. □

Acknowledgements

The authors wish to thank Professor M. A. Bennett for the stimulating correspondence and for making a few corrections of grammatical nature in the manuscript. Further, the authors are indebted to the referee for calling their attention to some inaccuracies and typos.

References

B1 M. A. Bennett, *Recipes for ternary Diophantine equations of signature* (p, p, k), Proc. RIMS Kokyuroku (Kyoto) **1319** (2003), 51–55.

B2 M. A Bennett, *Powers from five terms in arithmetic progression*, in: Diophantine Equations, Narosa Publ. House, New Delhi, 2008. pp. 53–57.

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

BGyP M. A Bennett, K. Győry and Á. Pintér, *On the diophantine equation* $1^k + 2^k + \cdots + x^k = y^n$, Compositio Math. **140** (2004), 1417–1431.

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

BVY M. A. Bennett, V. Vatsal and S. Yazdani, *Ternary Diophantine equations of signature* $(p, p, 3)$, Compositio Math. **140** (2004), 1399–1416.

BCP W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), 235–265.

C H. Cohen, *Number theory. Vol. II. Analytic and modern tools*, Graduate Texts in Mathematics, **240**, Springer, New York, 2007. xxiv+596 pp.

DM H. Darmon and L. Merel, *Winding quotients and some variants of Fermat's Last Theorem*, J. Reine Angew. Math. **490** (1997), 81–100.

De P. Dénes, *Über die diophantische Gleichung* $x^l + y^l = cz^l$, Acta Math. **88** (1952), 241–251.

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

ES P. Erdős and J. L. Selfridge, *The product of consecutive integers is never a power*, Illinios J. Math. **19** (1975), 292–301.

Gy1 K. Győry, *On the diophantine equation* $n(n+1)\dots(n+k-1) = bx^l$, Acta Arith. **83** (1998), 87–92.

Gy2 K. Győry, *Power values of products of consecutive integers and binomial coefficients*, Number Theory and Its Applications, Kluwer Acad. Publ. 1999, 145–156.

GyHS K. Győry, L. Hajdu and N. Saradha, *On the Diophantine equation* $n(n+d)\dots(n+(k-1)d) = by^l$, Canad. Math. Bull. **47** (2004), 373–388. Correction: Canad. Math. Bull. **48** (2005), 636.

HTT L. Hajdu, Sz. Tengely and R. Tijdeman, *Cubes in products of terms in arithmetic progression* (to appear).

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

K A. Kraus, *Majorations effectives pour l'équation de Fermat généralisée*, Canad. J. Math. **49** (1997), 1139–1161.

O1 R. Obláth, *Über das Produkt fünf aufeinander folgender Zahlen in einer arithmetischen Reiche*, Publ. Math. Debrecen **1** (1950), 222–226.

O2 R. Obláth, *Eine Bemerkung über Produkte aufeinander folgender Zahlen*, J. Indian Math. Soc. **15** (1951), 135–139.

R K. Ribet, *On the equation* $a^p + 2^\alpha b^p + c^p = 0$, Acta Arith. **79** (1997), 7–16.

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

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

SS N. Saradha and T.N. Shorey, *Almost perfect powers in arithmetic progression*, Acta Arith. **99** (2001), 363–388.

S1 T. N. Shorey, *Powers in arithmetic progression*, in: A Panorama in Number Theory (G. Wüstholz, ed.), Cambridge University Press, Cambridge, 2002, 325–336.

S2 T. N. Shorey, *Powers in arithmetic progression (II)*, in: New Aspects of Analytic Number Theory, Kyoto 2002, 202–214.

Te Sz. Tengely, *Note on the paper "An extension of a theorem of Euler" by Hirata-Kohno et al.*, Acta Arith. **134** (2008), 329–335.

Ti R. Tijdeman, *Diophantine equations and diophantine approximations*, in: Number Theory and Applications, Kluwer Acad. Press, 1989, 215–243.

W A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Ann. Math. **141** (1995), 443–551.

K. Győry gyory@math.klte.hu
University of Debrecen, Institute of Mathematics and the Number Theory Research Group of the Hungarian Academy of Sciences, Debrecen, P.O. Box 12., H-4010, Hungary

L. Hajdu hajdul@math.klte.hu
University of Debrecen, Institute of Mathematics and the Number Theory Research Group of the Hungarian Academy of Sciences, Debrecen, P.O. Box 12., H-4010, Hungary

Á. Pintér apinter@math.klte.hu
University of Debrecen, Institute of Mathematics and the Number Theory Research Group of the Hungarian Academy of Sciences, Debrecen, P.O. Box 12., H-4010, Hungary

I.3 [BBGyH06]: Powers from products of consecutive terms in arithmetic progression

Proc. London Math. Soc. **92** (2006), 273–306.

POWERS FROM PRODUCTS OF CONSECUTIVE TERMS IN ARITHMETIC PROGRESSION

M. A. BENNETT, N. BRUIN, K. GYŐRY, AND L. HAJDU

Dedicated to Professor R. Tijdeman on the occasion of his sixtieth birthday

Abstract. We show that if k is a positive integer, then there are, under certain technical hypotheses, only finitely many coprime positive k-term arithmetic progressions whose product is a perfect power. If $4 \leq k \leq 11$, we obtain the more precise conclusion that there are, in fact, no such progressions. Our proofs exploit the modularity of Galois representations corresponding to certain Frey curves, together with a variety of results, classical and modern, on solvability of ternary Diophantine equations. As a straightforward corollary of our work, we sharpen and generalize a theorem of Sander on rational points on superelliptic curves.

1. Introduction

A celebrated theorem of Erdős and Selfridge [14] states that the product of consecutive positive integers is never a perfect power. A more recent and equally appealing result is one of Darmon and Merel [11] who proved an old conjecture of Dénes to the effect that there do not exist three consecutive nth powers in arithmetic progression, provided $n \geq 3$. One common generalization of these problems is to ask whether it is possible to have a product of consecutive terms in arithmetic progression equal to a perfect power. In general, the answer to this question is yes, as the Diophantine equation

$$n(n+d)\cdots(n+(k-1)d) = y^l, \quad k \geq 3,\ l \geq 2 \tag{1}$$

may have infinitely many solutions in positive integers n, d, k, y and l if either the integers n and d have suitable common factors (as in the example $9 \cdot 18 \cdot 27 \cdot 36 = 54^3$), or $(k, l) = (3, 2)$ and $\gcd(n, d) = 1$ (e.g. $1 \cdot 25 \cdot 49 = 35^2$). If, however, we restrict our attention to progressions with

$$\gcd(n, d) = 1, \quad k \geq 3, \quad l \geq 2, \quad (k, l) \neq (3, 2), \tag{2}$$

Research supported in part by grants from NSERC (M.B. and N.B.), the Erwin Schrödinger Institute in Vienna (M.B. and K.G.), the Netherlands Organization for Scientific Research (NWO) (K.G. and L.H.), the Hungarian Academy of Sciences (K.G. and L.H.), by FKFP grant 3272-13/066/2001 (L.H.) and by grants T29330, T42985 (K.G. and L.H.), T38225 (K.G.) and F34981 (L.H.) of the Hungarian National Foundation for Scientific Research.

a number of special finiteness results are available in the literature. Euler (see e.g. [13]) showed that then (1) has no solutions if $(k, l) = (3, 3)$ or $(4, 2)$; a similar statement was obtained by Obláth [26], [27] for the cases $(k, l) = (3, 4), (3, 5)$ or $(5, 2)$. It has been conjectured by Erdős (as noted in [37]; see also Darmon and Granville [10]) that (1) (with (2)) has, in fact, no solutions whatsoever. This conjecture has been recently established by Győry [18] for $k = 3$ (and $l \geq 3$ arbitrary) and by Győry, Hajdu and Saradha [19], in case $k = 4$ or 5. Unfortunately, the arguments of [19] are invalid if $l = 3$; we correct these in Section 5 of the paper at hand.

In general, however, it appears to be a very hard problem to prove even that the number of solutions to (1), with (2), is finite. As a rough indication of its depth, this does not seem to be a consequence of the ABC Conjecture of Masser and Oesterlé, unless we further assume that $l \geq 4$; see Theorem 7 of [19]. Further work in this direction, under restrictive hypotheses, includes that of Marszalek [23] (in case d is fixed), Shorey and Tijdeman [37] (if l and the number of prime divisors of d is fixed) and Darmon and Granville [10] (if both k and l are fixed). For a broader sample of the abundant literature in this area, the reader may wish to consult the survey articles of Tijdeman [42] and Shorey [35], [36].

In this paper, we will address the problem of establishing finiteness results for equation (1), under the sole assumption that k is fixed. One of the principal results of this paper is an extension of the aforementioned work of Győry [18] and Győry, Hajdu and Saradha [19] to $k \leq 11$ (with a requisite correction of the latter work, in case $l = 3$).

Theorem 1.1. *The product of k consecutive terms in a coprime positive arithmetic progression with $4 \leq k \leq 11$ can never be a perfect power.*

By coprime progression, we mean one of the form

$$n, n + d, \cdots, n + (k - 1)d$$

with $\gcd(n, d) = 1$. We should emphasize that this does not follow as a mere computational sharpening of the approach utilized in [18] or [19], but instead necessitates the introduction of fundamentally new ideas. Indeed, the principal novelty of this paper is the combination of a new approach for solving ternary Diophantine equations under additional arithmetic assumptions, via Frey curves and modular Galois representations, with classical (and not so classical!) results on lower degree equations representing curves of small (positive) genus. Further, for the most part, our results do not follow from straightforward application of the modularity of Galois representations attached to Frey curves, but instead require additional understanding of the reduction types of these curves at certain small primes.

Theorem 1.1 is, in fact, an immediate consequence of a more general result. Before we state this, let us introduce some notation. Define, for integer m with $|m| > 1$, $P(m)$ and $\omega(m)$ to be the largest prime dividing m and the number of distinct prime divisors of m, respectively (where we take $P(\pm 1) = 1$, $\omega(\pm 1) = 0$). Further, let us write

$$\Pi\,(i_1, i_2, \ldots, i_t) = (n + i_1 d)(n + i_2 d) \cdots (n + i_t d) \tag{3}$$

and

$$\Pi_k = \Pi(0, 1, 2, \ldots, k-1) = n(n+d)(n+2d) \cdots (n+(k-1)d). \tag{4}$$

With these definitions, we have the following theorem.

Theorem 1.2. *Suppose that k and l are integers with $3 \le k \le 11$, $l \ge 2$ prime and $(k, l) \ne (3, 2)$, and that n and d are coprime integers with $d > 0$. If, further, b and y are nonzero integers with $P(b) \le P_{k,l}$ where $P_{k,l}$ is as follows :*

k	$l = 2$	$l = 3$	$l = 5$	$l \ge 7$
3	–	2	2	2
4	2	3	2	2
5	3	3	3	2
6	5	5	5	2
7	5	5	5	3
8	5	5	5	3
9	5	5	5	3
10	5	5	5	3
11	5	5	5	5

then the only solutions to the Diophantine equation

$$\Pi = \Pi_k = by^l \tag{5}$$

are with (n, d, k) in the following list :

$$(-9, 2, 9), (-9, 2, 10), (-9, 5, 4), (-7, 2, 8), (-7, 2, 9), (-6, 1, 6), (-6, 5, 4),$$
$$(-5, 2, 6), (-4, 1, 4), (-4, 3, 3), (-3, 2, 4), (-2, 3, 3), (1, 1, 4), (1, 1, 6).$$

For $k = 3$, this theorem was proved in [18]. Our Theorem 1.2 sharpens and generalizes the corresponding results of [19], which treated the cases $k = 4$ and 5 (with $l \ne 3$). Note that the upper bound on $P(b)$ in the above theorem may be replaced in all cases by the slightly stronger but simpler bound

$$P(b) < \max\{3, k/2\}, \tag{6}$$

leading to a cleaner but weaker theorem. Further, in cases $(k, l) = (4, 2)$ and $(3, 3)$, the result is best possible (in the sense that $P_{k,l}$ cannot be replaced by a larger value). This is almost certainly not true for other values of (k, l).

It is a routine matter to extend Theorem 1.2 to arbitrary (i.e. not necessarily prime) values of l. For $(k,l) = (3,4)$, equation (5) has no solutions with (6), cf. Theorem 8 of [19]. For all other pairs (k,l) under consideration, Theorem 1.2 yields the following result.

Corollary 1.3. *Suppose that n, d and k are as in Theorem 1.2, and that $l \geq 2$ is an integer with $(k,l) \neq (3,2)$. If, further, b and y are nonzero integers with (6), then the only solutions to equation (5) are with (n,d,k) in the following list :*

$$(-9,2,9), (-9,2,10), (-9,5,4), (-7,2,8), (-7,2,9),$$
$$(-6,5,4), (-5,2,6), (-4,3,3), (-3,2,4), (-2,3,3).$$

Note that knowing the values of the unknowns on the left hand side of (5), one can easily determine all the solutions (n,d,k,b,y,l) to (5).

In the special case $d = 1$, the set of solutions of equation (5), for $k \geq 2$ fixed, has been described in [17], [20] and [31], under less restrictive assumptions upon b. For further partial results on (5), we refer again to the survey papers [18], [35] [36] and [42].

For fixed values of $k \geq 3$ and $l \geq 2$ with $k + l > 6$, equation (5) has at most finitely many solutions in positive integers (n,d,b,y) with $\gcd(n,d) = 1$ and $P(b) \leq k$; see Theorem 6 of [19].

If we turn our attention to $k > 11$, we may prove a number of results of a similar flavour to Theorem 1.2, only with a corresponding loss of precision. If k is slightly larger than 11, we have the following theorem.

Theorem 1.4. *If $12 \leq k \leq 82$, then there are at most finitely many nonzero integers n, d, l, b and y with $\gcd(n,d) = 1$, $l \geq 2$ and satisfying (5), with $P(b) < k/2$. Moreover, for all such solutions to (5), we have*

$$\log P(l) < 3^k.$$

For arbitrary values of k, we may deduce finiteness results for equations (1) and (5), only under certain arithmetic assumptions. Write

$$D_k = \prod_{k/2 \leq p < k} p \tag{7}$$

where the product is over prime p.

Theorem 1.5. *If $k \geq 4$ is fixed, then the Diophantine equation (5) has at most finitely many solutions in positive integers n, d, b, y and l with*

$$\gcd(n,d) = 1, \quad y > 1, \quad l > 1, \quad P(b) < k/2 \quad \text{and} \quad d \not\equiv 0 \pmod{D_k}.$$

For each such solution, we necessarily have $\log P(l) < 3^k$.

A corollary of this which yields a finiteness result for (1), provided k is suitably large (relative to the number of prime divisors of d), is the following.

Corollary 1.6. *Let D be a positive integer and suppose that k is a fixed integer satisfying*

$$k \geq \begin{cases} 4 & \text{if } D \in \{1,2\} \\ 6D\log D & \text{if } D \geq 3. \end{cases} \tag{8}$$

Then the Diophantine equation (5) has at most finitely many solutions in positive integers n, d, b, y and l with

$$\gcd(n,d) = 1, \quad y > 1, \quad l > 1, \quad \omega(d) \leq D, \quad \text{and} \quad P(b) < k/2.$$

We remark that a sharp version of this result, in the special case $l = 2$ and $b = D = 1$, was recently obtained by Saradha and Shorey [33].

Finally, we mention an application of Theorem 1.2 to a family of superelliptic equations first studied by Sander [30]. Specifically, let us consider equations of the form

$$x(x+1)\dots(x+k-1) = \pm 2^{\alpha} z^{l} \tag{9}$$

where x and z are rational numbers with $z \geq 0$, and k, l and α are integers with $k, l \geq 2$ and $-l < \alpha < l$. If $-l < \alpha < 0$, by replacing α and z in (9) with $l + \alpha$ and $z/2$, respectively, we may restrict ourselves to the case where α is nonnegative.

If x and z are further assumed to be integers and $\alpha = 0$, then, by the result of Erdős and Selfridge [14], we have that the only solutions to (9) are with $z = 0$. Since these are also solutions of (9) for each α, we will henceforth refer to them as *trivial*; in what follows, we shall consider only non-trivial solutions. Let us return to the more general situation when $x, z \in \mathbb{Q}$. By putting $x = n/d$ and $z = y/u$ with integers n, d, y, u such that $\gcd(n,d) = \gcd(y,u) = 1$, $d > 0$, $y \geq 0$ and $u > 0$, we see that (9) reduces to equation (5) with $P(b) \leq 2$ and (by comparing denominators) satisfying the additional constraint that $u^l = 2^{\gamma} d^k$ for some nonnegative integer γ. An almost immediate consequence of Theorem 1.2 is the following.

Corollary 1.7. *Let $2 \leq k \leq 11$ and $l \geq 2$ with $(k,l) \neq (2,2)$ (and, if $\alpha > 0$, $(k,l) \neq (2,4)$). Then the only non-trivial solutions of (9) with $0 \leq \alpha < l$ are those (x,k) in the following list :*

$$(-9/2, 9), (-9/2, 10), (-7/2, 8), (-7/2, 9), (-5/2, 6), (-2, 2),$$
$$(-3/2, 4), (-4/3, 3), (-2/3, 3), (-1/2, 2), (1, 2).$$

This result follows easily from Theorem 1.2; the reader is directed to [19] for the necessary arguments. Indeed, in [19], our Corollary 1.7 is established for $l \geq 4$, $k = 3, 4$ and, if $\alpha = 0$, $k = 5$. If $2 \leq k \leq 4$, $l > 2$ and $\alpha = 0$, Sander [30] completely solved equation (9) and noted that, for $(k,l) = (2,2)$, there are, in fact, infinitely many solutions. We remark, however, that the solutions listed in Corollary 1.7 for $k = 3$ and 4 are missing from Sander's result. Further, as discussed in [19],

the assumption $(k,l) \neq (2,4)$ (if $\alpha > 0$) is necessary, since, in that case, equation (9) has, again, infinitely many solutions.

The structure of this paper is as follows. In the second section, we will indicate how the problem of solving equation (5) may be translated to a question of determining solutions to ternary Diophantine equations. In Sections 3–6, we prove Theorem 1.2 for, respectively, prime $l \geq 7$, $l = 2$, $l = 3$ and $l = 5$. In many cases, for $l = 2$ or 3, the problem may be reduced to one of finding the torsion points on certain rank 0 elliptic curves $E/\mathbb{Q}$. In a number of situations, however, this approach proves inadequate to deduce the desired result. We instead turn to recent explicit Chabauty techniques due to Bruin and Flynn [5]; we encounter some interesting variations between the cases with $l = 2$ and those with $l = 3$. If $l = 5$, we depend on either classical results of Dirichlet, Lebesgue, Maillet (cf. [13]), Dénes [12] and Győry [16] on generalized Fermat equations of the shape $X^l + Y^l = CZ^l$, or recent work of Kraus [21]. For $l \geq 7$, we apply recent results of the first author and Chris Skinner [1], together with some refinements of these techniques; our proofs are based upon Frey curves and the theory of Galois representations and modular forms. Section 7 is devoted to the proof of Theorem 1.5. Finally, we conclude the paper by considering values of k with $12 \leq k \leq 82$.

2. The transition to ternary equations

For virtually every argument in this paper, we will rely heavily on the fact that a "nontrivial" solution to (5) implies a number of similar solutions to related ternary Diophantine equations which we may, if all goes well, be able to treat with the various tools at our disposal. The only situation where we will not follow this approach is in Section 4 (i.e. when $l = 2$). From equation (5) and the fact that $\gcd(n,d) = 1$, we may write

$$n + id = b_i y_i^l \text{ for } 0 \leq i \leq k-1, \tag{10}$$

where b_i and y_i are integers with $P(b_i) < k$. We note that, in terms of b_i, such a representation is not necessarily unique. We will thus assume, unless otherwise stated, that each b_i is lth power free and, if l is odd, positive.

Let us first observe that any three of the linear forms $n + id$, $0 \leq i \leq k-1$, are linearly dependent. In particular, given distinct integers $0 \leq q, r, s \leq k-1$, we may find relatively prime non-zero integers λ_q, λ_r, λ_s, for which

$$\lambda_q(n + qd) + \lambda_r(n + rd) = \lambda_s(n + sd). \tag{11}$$

It follows from (10) that, writing $A = \lambda_q b_q$, $B = \lambda_r b_r$, $C = \lambda_s b_s$, $(u,v,z) = (y_q, y_r, y_s)$, we have

$$Au^l + Bv^l = Cz^l, \tag{12}$$

where it is straightforward to show that $P(ABC) < k$. This is a ternary Diophantine equation of signature (l, l, l). In case $l = 3, 5$ and, sometimes, $l \geq 7$, we will prove Theorem 1.2 through analysis of such equations. In the sequel, we will employ the shorthand $[q, r, s]$ to refer to an identity of the form (11) (and hence a corresponding equation (12)) – for given distinct integers q, r and s, coprime nonzero integers λ_q, λ_r and λ_s satisfying (11) are unique up to sign.

A second approach to deriving ternary equations from a solution to (5) proves to be particularly useful for larger values of (prime) l. If p, q, r and s are integers with

$$0 \leq p < q \leq r < s \leq k - 1 \text{ and } p + s = q + r,$$

then we may observe that

$$(n + qd)(n + rd) - (n + pd)(n + sd) = (qr - ps)d^2 \neq 0. \tag{13}$$

It follows that identity (13) implies (nontrivial) solutions to Diophantine equations of the form

$$Au^l + Bv^l = Cz^2 \tag{14}$$

with $P(AB) < k$, for each quadruple $\{p, q, r, s\}$. This is a ternary Diophantine equation of signature $(l, l, 2)$. Henceforth, we will use the shorthand $\{p, q, r, s\}$ to refer to an identity of the form (13).

Our arguments will rely upon the fact that a triple $[q, r, s]$ or quadruple $\{p, q, r, s\}$ can always be chosen such that the resulting equation (12) or (14) is one that we may treat with techniques from the theory of Galois representations and modular forms, or, perhaps, with a more classical approach. In essence, once we have established certain results on the equations (12) and (14), as we shall see, this can be regarded as a purely combinatorial problem.

3. Proof of Theorem 1.2 in case $l \geq 7$

We will primarily treat equation (5) with prime exponent $l \geq 7$ by reducing the problem to one of determining the solvability of equations of the shape (14). For a more detailed discussion of these matters, the reader is directed to [1], [11], [22] and [25]. We begin by cataloguing the required results on such ternary equations :

Proposition 3.1. *Let $l \geq 7$ be prime, α, β be nonnegative integers, and let A and B be coprime nonzero integers. Then the following Diophantine equations have no solutions in nonzero coprime integers (x, y, z)*

with $xy \neq \pm 1$ *:*

$$x^l + 2^\alpha y^l = 3^\beta z^2,\ \alpha \neq 1 \tag{15}$$

$$x^l + 2^\alpha y^l = z^2 \text{ with } p \mid xy \text{ for } p \in \{3,5,7\} \tag{16}$$

$$x^l + 2^\alpha y^l = 3z^2 \text{ with } p \mid xy \text{ for } p \in \{5,7\} \tag{17}$$

$$x^l + y^l = Dz^2,\ D \in \{2,6\} \tag{18}$$

$$x^l + 3^\alpha y^l = 2z^2 \text{ with } p \mid xy \text{ for } p \in \{5,7\},\ l \geq 11 \tag{19}$$

$$x^l + 5^\alpha y^l = 2z^2 \text{ with } l \geq 11 \text{ if } \alpha > 0 \tag{20}$$

$$Ax^l + By^l = z^2,\ AB = 2^\alpha p^\beta,\ \alpha \geq 6,\ p \in \{3,5,13\} \tag{21}$$

$$Ax^l + By^l = z^2,\ AB = 2^\alpha p^\beta,\ \alpha \neq 1,\ p \in \{11,19\} \tag{22}$$

$$Ax^l + By^l = z^2,\ P(AB) \leq 3,\ \text{with } p \mid xy \text{ for } p \in \{5,7\} \tag{23}$$

$$Ax^l + By^l = z^2,\ P(AB) \leq 5,\ \text{with } 7 \mid xy \text{ and } l \geq 11. \tag{24}$$

In each instance where we refer to a prime p, we further suppose that the exponent $l > p$.

Proof. We begin by noting that the stated results for equations (15), (18), (20) and (22) are, essentially, available in Bennett and Skinner [1]. The cases of equation (21) with $p = 3$ or 5, and $\beta \geq 1$, while not all explicitly treated in [1], follow immediately from the arguments of that paper, upon noting that the modular curves $X_0(N)$ have genus 0 for all N dividing 6 or 10.

For the remaining equations, we will begin by employing the approach of [1]. Specifically, to a putative nontrivial solution of one of the preceding equations, we associate a Frey curve $E/\mathbb{Q}$ (see [1] for details), with corresponding mod l Galois representation

$$\rho_l^E : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_l)$$

on the l-torsion $E[l]$ of E. Via Lemmata 3.2 and 3.3 of [1], this representation arises from a cuspidal newform f of weight 2 and trivial Nebentypus character. The level N of this newform may be shown to satisfy

$$N \in \{20, 24, 30, 40, 96, 120, 128, 160, 384, 480, 640, 768, 1152, 1920\}$$

(for example, a nontrivial solution to (16) with $\alpha = 1$ and x, y odd necessarily leads to a newform of level 128; for details, the reader is directed to Lemma 3.2 of [1]). The assumption that $p \mid xy$ for $p \in \{3,5,7\}$ implies, if p is coprime to lN, that

$$\mathrm{trace}\ \rho_l^E\,(\mathrm{Frob}_p) = \pm(p+1).$$

It follows, if f has Fourier coefficents a_n in a number field K_f, that

$$\mathrm{Norm}_{K_f/\mathbb{Q}}\,(a_p \pm (p+1)) \equiv 0 \pmod{l}. \tag{25}$$

Using William Stein's "Modular Forms Database" [38], we find a_p, $p \in \{3,5,7\}$, for each newform at the levels N of interest, provided p is coprime to N. In most cases the corresponding Fourier coefficients are even integers: from the Weil bounds, $a_3 \in \{0, \pm 2\}$ (if $3 \nmid N$), $a_5 \in \{0, \pm 2, \pm 4\}$ (if 5 is coprime to N) and $a_7 \in \{0, \pm 2, \pm 4\}$ (if 7 fails to divide N). Congruence (25) thus implies a contradiction for these forms. The only forms f encountered with $K_f \neq \mathbb{Q}$ are (in Stein's notation) form 3 at level 160, forms 9–12 at level 640, forms 9–12 at level 768 and forms 25–28 at level 1920. In the case of form 3, $N = 160$, we find that $a_7 = \pm 2\sqrt{2}$ and so $2\sqrt{2} \equiv \pm 8 \pmod{\mathcal{P}}$ for some prime $\mathcal{P}$ lying over l. It follows that $l \mid 56$ and so $l = 7$. Similarly, form 9 at level 672 has $a_7 = -\vartheta - 2$ where $\vartheta^2 + 2\vartheta - 4 = 0$. From $a_7 \equiv \pm 8 \pmod{\mathcal{P}}$ we thus have $\vartheta \equiv 6 \pmod{\mathcal{P}}$ (whereby $l = 11$) or $\vartheta \equiv -10 \pmod{\mathcal{P}}$ (whence $l = 19$). On the other hand, $a_3 = \vartheta$ and hence, from the Weil bounds, $\vartheta \equiv 0, \pm 2, \pm 4 \pmod{\mathcal{P}}$, a contradiction in each case. Arguing in a like fashion for the remaining forms completes the proof. □

We will also need a result on equations of signature (l, l, l). Specifically, we apply the following.

Proposition 3.2. *Let $l \geq 3$ and $\alpha \geq 0$ be integers. Then the Diophantine equation*

$$X^l + Y^l = 2^\alpha Z^l \tag{26}$$

has no solutions in coprime nonzero integers X, Y and Z with $XYZ \neq \pm 1$.

Proof. This is essentially due to Wiles [43] (in case $l \mid \alpha$), Darmon and Merel [11] (if $\alpha \equiv 1 \pmod{l}$) and Ribet [28] (in the remaining cases for $l \geq 5$ prime); see also Győry [18]. □

Let us begin the proof of Theorem 1.2. For the remainder of this section, we will suppose that there exists a solution to equation (5) in nonzero integers n, d, k, y, l and b with n and $d > 0$ coprime, $3 \leq k \leq 11$, and $l \geq 7$ prime. We suppose further that b satisfies (6). We treat each value $3 \leq k \leq 11$ in turn.

3.1. **The case k=3.** If $k = 3$, the identity $\{0, 1, 1, 2\}$ yields solutions to an equation of the shape (15) with $\beta = 0$ and $\alpha = 0$ (if Π is odd) or $\alpha \geq 2$ (if Π is even). By Proposition 3.1, after a modicum of work, we obtain the solutions $(n, d, k) = (-4, 3, 3)$ and $(-2, 3, 3)$ listed in the statement of Theorem 1.2.

3.2. **The case k=4.** If n is coprime to 3, we may use the same identity as for $k = 3$ to deduce that there is no solution to (5). If $3 \mid n$, then $\{0, 1, 2, 3\}$ gives an equation of type (18) with $D = 2$ (if Π is odd), and one of the form (16) with $p = 3$ (if Π is even). In either case, we infer from Proposition 3.1 that equation (5) has no solution.

3.3. **The case k=5.** Considering the product of the first or the last four terms of Π, according as $3 \mid n$, or not, we may reduce this to the preceding case and reach the desired conclusion.

3.4. **The case k=6.** If $k = 6$ and 5 fails to divide n, then we may apply what we have for the case $k = 4$ to the product of the first, middle or last four terms of Π, to obtain that there is no solution to (5). Similarly, if $3 \nmid n(n + 5d)$, the middle four terms lead to a contradiction. Thus we may suppose that $5 \mid n$, and, by symmetry, that also $3 \mid n$. Considering the identity $\{0, 1, 4, 5\}$ (if Π is odd) or $\{0, 2, 3, 5\}$ (if Π is even), we obtain an equation of the shape (23) with $p = 5$. We can thus apply Proposition 3.1 to conclude that (5) has no solution with $k = 6$ and $l \geq 7$ prime.

3.5. **The case k=7.** Next, let $k = 7$. If $5 \nmid n(n + d)$, then we may apply $\{1, 2, 4, 5\}$ (if $3 \mid n$) or $\{0, 3, 3, 6\}$ (if $3 \nmid n$). These lead to equations of type (15). Next, suppose that $5 \mid n(n + d)$; by symmetry, we may assume $5 \mid n$. Suppose first that $6 \mid \Pi$, and consider the identity $\{0, 2, 3, 5\}$. If $3 \mid n + d$, we are led to an equation of the shape (16) or (17), with $p = 5$. On the other hand, if $3 \mid n(n + 2d)$, then the same identity induces an equation of the form (23), again with $p = 5$.

Assume now that $6 \nmid \Pi$, and consider $\{0, 1, 4, 5\}$. If $\gcd(\Pi, 6) = 3$, this identity gives equation (23) with $p = 5$. If, however, $\gcd(\Pi, 6) = 2$, then the same identity leads either to (16) with $p = 5$ or to (18), with $D = 2$. Finally, if $\gcd(\Pi, 6) = 1$, then again employing the identity $\{0, 1, 4, 5\}$, we find a solution to (15) with $\alpha = \beta = 0$. In all cases, we conclude from Proposition 3.1 that (5) has no solution, in the situation under consideration.

3.6. **A diversion.** In case $k \geq 8$, in a number of instances, Proposition 3.1 enables us to prove our statement only for $l \geq 11$ prime. We are thus forced to deal with the exponent $l = 7$ separately. As we shall observe, in each case where we encounter difficulties for $l = 7$, there are precisely two distinct factors in Π which are divisible by 7. By our assumptions, we have that $7 \mid \nu_7(\Pi)$ where, here and henceforth, we write $\nu_p(m)$ for the largest integer t such that p^t divides a nonzero integer m. It follows that one of these two factors is necessarily divisible by 7^2. We will use the following argument to finish the proof in this case.

Choose three factors $n+qd$, $n+rd$ and $n+sd$ of Π, such that one of them, $n+qd$ say, is divisible by 7^2, but 7 fails to divide $(n+rd)(n+sd)$. The identity $[q, r, s]$ thus yields

$$\lambda_r b_r y_r^7 \equiv \lambda_s b_s y_s^7 \pmod{7^2},$$

whence, upon taking sixth powers, it follows that

$$u^6 \equiv v^6 \pmod{7^2}, \tag{27}$$

where $u = \lambda_r b_r$ and $v = \lambda_s b_s$. If we choose $n + qd$, $n + rd$ and $n + sd$ appropriately, then we can use the fact that, for $a \equiv uv^{-1} \pmod{7^2}$,

$$a^6 \equiv 1 \pmod{7^2} \Longleftrightarrow a \equiv \pm 1, \pm 18, \pm 19 \pmod{7^2} \tag{28}$$

to obtain a contradiction, thereby verifying that (5) has no solution in the case in question.

3.7. **The case k=8.** Let us return to our proof. Suppose $k = 8$. If $7 \nmid n$, then we may reduce to the preceding case by considering the first or last seven terms of Π. Suppose, then, that $7 \mid n$. Notice that if $\gcd(\Pi, 15) = 1$, then we may apply our results with $k = 6$ to the middle six terms of Π to conclude that (5) has no solution. If $5 \nmid \Pi$, it therefore follows that $3 \mid \Pi$. If $3 \mid n$ or $3 \mid n + d$, using $\{1, 2, 4, 5\}$ or $\{2, 3, 5, 6\}$ respectively, we are led to an equation of the shape (15) with $\beta = 1$, contradicting Proposition 3.1. If $3 \mid n + 2d$, then the identity $\{0, 1, 6, 7\}$ gives rise to an equation of the form (18) with $D = 6$, if Π is odd, and of the form

$$x^l + 2^\alpha y^l = 3z^2, \tag{29}$$

if Π is even. We may apply Proposition 3.1 again, unless $\alpha = 1$, i.e. unless $\nu_2(n + id) = 2$ for one of $i = 0, 1, 6, 7$. If this last condition occurs, it follows that $\nu_2(n + jd) \geq 3$ for one of $j = 2, 3, 4, 5$. For this j, the identity $\{j - 1, j, j, j + 1\}$ leads to an equation of the form (21) with $p = 3$. By Proposition 3.1, we infer that (5) has no solution in this case.

We may thus suppose that $5 \mid \Pi$. If $3 \nmid \Pi$, then we may apply our results obtained for $k = 3$ to $\Pi(i, i + 1, i + 2)$ with an appropriate $i = 1, 3$ or 4 to conclude that there is no solution in this case. We may therefore assume that $15 \mid \Pi$. Further, if $5 \mid (n + 3d)(n + 4d)$, we can argue as previously to obtain a contradiction. Hence we may suppose that $5 \mid n(n + d)(n + 2d)$. Assume first that $5 \mid n + d$. If Π is odd, then the identity $\{1, 2, 5, 6\}$ leads to (23) with $p = 5$ and so, via Proposition 3.1, a contradiction. If Π is even, then we consider the identity $\{1, 3, 4, 6\}$. If $3 \mid n + 2d$, we are led to an equation of the form (17) with $p = 5$. On the other hand, if $3 \mid n(n + d)$, then we find a nontrivial solution to (23) with $p = 5$. In either case, we contradict Proposition 3.1.

To complete the proof of Theorem 1.2, in case $k = 8$, we may thus, by symmetry, suppose that $5 \mid n$. We divide our proof into two parts. First suppose that $l \geq 11$ prime.

We begin with the case where $3 \mid n$. Necessarily one of $n, n + 3d$ or $n + 6d$ is divisible by 9. If $9 \mid n$, then $\{1, 3, 4, 6\}$ gives rise to an equation of the form (18) with $D = 2$, at least provided Π is odd. When Π is even, the identity $\{0, 2, 5, 7\}$ yields (24) and hence a contradiction. If $9 \mid n + 3d$, $\{0, 1, 6, 7\}$ leads to (20), if Π is odd. If Π is even, from the same identity we have (24). By Proposition 3.1, in each case, we

conclude that there is no solution to (5). Finally, if $9 \mid n+6d$, then the identity $\{0,3,4,7\}$ provides either (20) or (24). In both cases, we have a contradiction, at least for $l \geq 11$ prime.

We argue in a similar fashion if $3 \mid n+d$ or $3 \mid n+2d$. In the first of these cases, one of the identities $\{0,3,4,7\}$, $\{0,1,6,7\}$, $\{1,3,4,6\}$ or $\{0,2,5,7\}$, necessarily implies solutions to either (20) or (24). In the second, either $\{1,3,4,6\}$ yields a solution to (18) with $D=6$, or $\{0,2,5,7\}$ provides one to equation (24). By Proposition 3.1, we thus derive a contradiction, in all cases, for $l \geq 11$ prime.

Now suppose that $l=7$. We use the argument outlined in subsection 3.6; i.e. we appeal to identities of the form (11), corresponding to triples $[q,r,s]$.

Assume first that, together with $5 \mid n$, we have $3 \mid n$. Since, necessarily, either n or $n+7d$ is divisible by 7^2, we distinguish two cases. Suppose first that $7^2 \mid n$, and consider the identity $[0,2,4]$. This implies a congruence of the form

$$\left(2^{\nu_2(b_2)+1}\right)^6 \equiv \left(2^{\nu_2(b_4)}\right)^6 \pmod{7^2},$$

whereby, from (28), $(\nu_2(b_2),\nu_2(b_4)) = (0,1)$ or $(1,2)$. From the identity $\{1,2,2,3\}$, if $\nu_2(n+2d) \geq 3$, we derive a nontrivial solution to (21) with $p=3$, contrary to Proposition 3.1. We conclude, then, that $\nu_2(n+2d)=1$ (and hence $\nu_2(n+6d)=1$). It thus follows, from $[0,3,6]$, that

$$\left(3^{\nu_3(b_3)}\right)^6 \equiv \left(3^{\nu_3(b_6)}\right)^6 \pmod{7^2}$$

and so $\nu_3(b_3)=\nu_3(b_6)=1$. The identity $[3,4,6]$ thus leads to a nontrivial solution to equation (26), with $n=7$ and $\alpha=1$, contradicting Proposition 3.2.

We next suppose that $7^2 \mid n+7d$. If $2 \nmid \Pi$, then $[1,4,7]$ immediately contradicts (28). If $2 \mid n$, arguing as previously, we find, from $[1,3,7]$, that $\nu_3(b_3)=4$ and hence $[2,3,7]$ implies that $\nu_2(b_2)=6$. If, however, $2 \mid n+d$, $[4,6,7]$ gives that $\nu_3(b_6)=6$ whence, from $[3,6,7]$, $\nu_2(b_3)=6$. In either case, $[3,4,7]$ now contradicts (28).

Assume next that $3 \mid n+d$. Suppose first that $7^2 \mid n$. The identity $[0,2,6]$ implies that

$$\left(3 \cdot 2^{\nu_2(b_2)}\right)^6 \equiv \left(2^{\nu_2(b_6)}\right)^6 \pmod{7^2}$$

and so

$$\nu_2(b_6) - \nu_2(b_2) \in \{-4,3\}. \tag{30}$$

On the other hand, $[0,3,6]$ implies that $\nu_2(b_6)=1$, contradicting (30) (since we have $\min\{\nu_2(n+2d),\nu_2(n+6d)\} \leq 2$).

Next, let $7^2 \mid n+7d$. In this case, the identity $[2,6,7]$ plays the role of $[0,2,6]$ in the previous situation. We have that

$$_2(b_2) - \nu_2(b_6) \in \{-4,3\}$$

and hence, since $[3, 6, 7]$ implies that $\nu_2(b_6) = 5$, again a contradiction.

Finally, suppose that $3 \mid n + 2d$. As the situation with Π odd was covered previously for $l = 7$, we need distinguish only two cases. If $2 \mid n$, then $[0, 1, 3]$ (if $7^2 \mid n$) or $[1, 3, 7]$ (if $7^2 \mid n + 7d$) each contradict (28). If, however, $2 \mid n + d$, the identities $[0, 4, 6]$ and $[4, 6, 7]$ play a like role. This completes the proof of Theorem 1.2 for $k = 8$ and $l \geq 7$ prime.

3.8. **The case k=9.** Next, consider $k = 9$. Symmetry allows us to assume that $7 \mid n$, otherwise we can reduce to the preceding situation. We may also assume that $5 \mid n+3d$, or, by applying our results with $k = 8$ to the first eight terms of Π, again obtain a contradiction. If 3 fails to divide the product Π, then we may use what we have proved already for $k = 3$, via consideration of $\Pi(4, 5, 6)$, to deduce a contradiction. If $3 \mid n$, then $\{1, 2, 4, 5\}$ yields (15) with $\beta = 1$. Similarly, if $3 \mid n + d$, $\{3, 5, 6, 8\}$ provides (18) with $D = 6$, if Π is odd, and (17) with $p = 5$, if Π is even. Using Proposition 3.1, we obtain contradictions in either case. If $3 \mid n+2d$, then the identity $\{0, 1, 6, 7\}$ gives rise to an equation of the shape (18) with $D = 6$, if Π is odd, while $\{3, 5, 6, 8\}$ leads to an equation of the form (23) with $p = 5$, if Π is even. Applying Proposition 3.1 thus completes the proof of Theorem 1.2, in case $k = 9$ and $l \geq 7$ prime.

3.9. **The case k=10.** When $k = 10$, we reduce to the preceding case unless either $7 \mid n$, $5 \mid n+9d$, or $5 \mid n$, $7 \mid n+9d$. By symmetry, we may suppose that the first of these occurs. Then, if $3 \nmid \Pi$, we may apply our result with $k = 3$ for $\Pi(1, 2, 3)$ to obtain a contradiction. In case $3 \mid n(n+d)$, $\{2, 5, 5, 8\}$ yields (15) with $\beta = 0$, providing a contradiction by Proposition 3.1. We thus suppose that $3 \mid n + 2d$. To complete the proof of Theorem 1.2 in this case, we will utilize Proposition 3.2. Necessarily, precisely one of $n + 2d$, $n + 5d$ or $n + 8d$ is divisible by 9. If $9 \mid n + 2d$, the identity $[5, 6, 8]$ implies a nontrivial solution to (26), contradicting Proposition 3.2. Similarly, if $9 \mid n + 5d$ or $9 \mid n + 8d$, application of $[2, 3, 8]$ or $[2, 3, 5]$, respectively, leads to a contradiction. We conclude, then, that equation (5) has no solution, with $k = 10$ and, again, prime $l \geq 7$.

3.10. **The case k=11.** Finally, let $k = 11$. If $5 \nmid \Pi$, then we may apply the results from the preceding case to the first or last ten terms of Π, to obtain a contradiction. If $5 \mid \Pi$, we will, as when $k = 10$, repeatedly appeal to Proposition 3.2 to complete the proof. In what follows, we will assume, via symmetry, that either $7 \nmid \Pi$ or $7 \mid (n + 4d)(n + 5d)(n + 6d)$, or that $7 \mid n(n + d)$. The last case is the only one in which $7 \mid b_i$ for some $0 \leq i \leq 10$.

Let us begin by supposing that $5 \mid n$. From the identity $\{3, 6, 6, 9\}$, we deduce a solution to (15) unless $3 \mid n$. If $3 \mid n$, then 9 divides

exactly one of $n, n+3d$ or $n+6d$. If $9 \mid n$, then $[3,4,6]$ thus implies a (nontrivial) solution to (26), contrary to Proposition 3.2. Similarly, $[6,7,9]$ (if $7 \mid n+d$) and $[6,8,9]$ (in the remaining cases) lead to the same conclusion if $9 \mid n+3d$. Finally, if $9 \mid n+6d$, we may apply $[3,7,9]$ (if $7 \mid n+d$) and $[1,3,9]$ (in the remaining cases) to reach a contradiction.

In case $5 \mid n+id$ for $i = 1, 2$ or 4, we argue similarly. In the first of these cases, either $\{4,7,7,10\}$ (if $7 \mid n+d$) or $\{2,5,5,8\}$ (otherwise) implies that $3 \mid n+d$ (respectively, $3 \mid n+2d$). The identities $[4,5,7]$, $[7,9,10]$ and $[2,4,10]$ (respectively, $[2,3,5]$, $[5,7,8]$ and $[2,4,8]$) thus combine to contradict Proposition 3.2. If $5 \mid n+2d$, $\{3,6,6,9\}$ leads to the conclusion that $3 \mid n$, whereby $[3,4,6]$, $[3,5,9]$ and either $[0,4,6]$ (if $7 \mid n+d$) or $[6,8,9]$ (in all other cases) provide the desired conclusion. If $5 \mid n+4d$, we combine the identities $\{2,5,5,8\}$, $[2,3,5]$, $[5,6,8]$ and $[2,8,10]$ (if $7 \mid n$), or $\{0,3,3,6\}$, $[0,2,3]$, $[3,5,6]$ and $[0,2,6]$ (in all other cases) to obtain a contradiction.

It remains, then, to deal with the possibility that $5 \mid n+3d$. In this situation, we require a somewhat more involved argument. If n is not divisible by 7, then $\{4,7,7,10\}$, together with Proposition 3.1, implies that $3 \mid n+d$, whereby one of $[4,6,7]$, $[7,9,10]$ or $[2,4,10]$ contradicts Proposition 3.2. We may thus suppose that $7 \mid n$. In this case, $\{1,2,4,5\}$ yields a solution to (15) unless $3 \mid (n+d)(n+2d)$. If $3 \mid n+2d$, $\{0,1,6,7\}$ implies a solution to either (15) or (18) (with $D = 6$), unless

$$\max\{\nu_2(n+id) : i = 0,1,6,7\} = 2. \tag{31}$$

In the latter case, from $\{0,1,6,7\}$, we have a solution to (17) (with $p = 7$) and hence may conclude further that $l = 7$. If $7^2 \mid n$, the identity $[0,1,9]$ implies that

$$\left(9 \cdot 2^{\nu_2(b_1)}\right)^6 \equiv \left(2^{\nu_2(b_9)}\right)^6 \pmod{7^2},$$

contrary to (31). If $7^2 \mid n+7d$, then, from $[1,7,9]$,

$$\left(3 \cdot 2^{\nu_2(b_9)}\right)^6 \equiv \left(2^{\nu_2(b_1)}\right)^6 \pmod{7^2},$$

again contradicting (31).

Finally, if $3 \mid n+d$, from $\{2,5,6,9\}$, we deduce solutions to either (15) or (18) (with $D = 6$), unless

$$\max\{\nu_2(n+id) : i = 2,5,6,9\} = 3. \tag{32}$$

In this case, $\{0,1,6,7\}$ implies solutions to equation (24) and so, via Proposition 3.1, we may assume further that $l = 7$. If $7^2 \mid n$, $[0,2,6]$ gives

$$\left(3 \cdot 2^{\nu_2(b_2)}\right)^6 \equiv \left(2^{\nu_2(b_6)}\right)^6 \pmod{7^2},$$

contradicting (32). If $7^2 \mid n+7d$, $[2,6,7]$ yields

$$\left(5 \cdot 2^{\nu_2(b_6)}\right)^6 \equiv \left(2^{\nu_2(b_2)}\right)^6 \pmod{7^2},$$

again contrary to (32). This completes the proof of Theorem 1.2, in case $l \geq 7$ is prime.

4. Proof of Theorem 1.2 in case $l = 2$

Having disposed of the possibility of equation (5) having solutions with l divisible by a large prime, we are now left with the task of dealing with the primes $l = 2, 3$ and 5. In this section, we treat the first of these cases. For $l = 2$ and fixed $k \geq 4$, a solution to (5) corresponds to a rational point on one of finitely many hyperelliptic curves. Our argument will essentially rely upon the fact that, with the given restrictions on b, the curves in question may often be shown to cover elliptic curves of rank 0 over $\mathbb{Q}$.

4.1. **The case k=4.** In case $k = 4$, we actually deduce a stronger result, which will prove useful for larger values of k :

Lemma 4.1. *The only solutions in coprime nonzero integers n and d, with $d > 0$, and nonzero integer y, to the Diophantine equations*

$$\Pi(0,1,2,3) = by^2, \quad b \in \{\pm 1, \pm 2, \pm 3, 5, -6, 15, -30\} \tag{33}$$

$$\Pi(0,1,2,4) = by^2, \quad b \in \{-1, \pm 2, \pm 3, 5, 6, \pm 10, -15, -30\} \tag{34}$$

$$\Pi(0,1,3,4) = by^2, \quad b \in \{\pm 1, \pm 2, \pm 3, -5, 6, -15, 30\} \tag{35}$$

$$\Pi(0,1,2,5) = by^2, \quad b \in \{-1, \pm 2, 3, \pm 5, 6, \pm 10, \pm 15\} \tag{36}$$

correspond to the identities

$$(-3)\cdot(-1)\cdot 1\cdot 3 = 3^2 \quad \textit{and} \quad (-2)\cdot(-1)\cdot 1\cdot 2 = 2^2.$$

We remark that, by symmetry, results for $\Pi(0,1,2,4)$ and $\Pi(0,1,2,5)$ lead to similar statements for $\Pi(0,2,3,4)$ and $\Pi(0,3,4,5)$, respectively. Further, we may translate a claim for $\Pi(0,p,q,r)$ to one for $\Pi(i, p+i, q+i, r+i)$, for any $i \in \mathbb{Z}$.

Proof. Via the change of variables

$$X = pqb\left(\frac{rd+n}{n}\right), \quad Y = \frac{pqryb^2}{n^2},$$

if p, q and r are integers with

$$0 < p < q < r,$$

solutions in nonzero integers n, d, y to

$$\Pi(0,p,q,r) = by^2 \tag{37}$$

correspond to rational points (X, Y) on the elliptic curve

$$E \; : \; Y^2 = X(X + p(r-q)b)(X + q(r-p)b).$$

The lemma follows from the observation that, for the choices of p, q, r and b described above, the curves $E = E(p,q,r,b)$ have rank 0 over $\mathbb{Q}$ (together with a routine calculation to ensure that the torsion points

yield only the stated solutions to (37)). For the given triples (p, q, r) and all other values of b dividing 30, the curves E have positive rank (and hence the equations (37) have, for these p, q, r and b, infinitely many solutions in nonzero coprime integers n and d). To verify these facts requires a routine computation in, say, mwrank (though Magma or other symbolic computation packages would be equally suitable). By way of example, if $(p, q, r) = (1, 2, 3)$, the elliptic curves corresponding to (37) are birational to the following curves (where we adopt the notation of Cremona [9]) :

b	Cremona	b	Cremona	b	Cremona	b	Cremona
1	$24A$	3	$144B$	6	$576I$	15	$3600K$
-1	$48A$	-3	$72A$	-6	$576D$	-15	$1800S$
2	$192C$	5	$600D$	10	$4800C$	30	$14400SSSS$
-2	$192D$	-5	$1200A$	-10	$4800BBB$	-30	$14400X$

If $b \in \{\pm 1, \pm 2, \pm 3, 5, -6, 15, -30\}$, then it is readily checked that the corresponding curves have rank 0. In all cases, except for $b = 1$, we have $E(\mathbb{Q})_{\text{tors}}$ isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, where the torsion points map back to only the trivial solutions to (37), with $n/d = 0, -p, -q, -r$ and $y = 0$. If $b = 1$, then there are additional torsion points given by $(X, Y) = (-2, \pm 2)$ and $(2, \pm 6)$. The latter of these corresponds to a solution to (37) with $d = 0$, while the former yields $(n, d) = (-3, 2)$.

For the remaining triples (p, q, r), we argue similarly. In all cases, for the stated values of b, we find rank 0 curves with

$$E(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},$$

unless $(p, q, r, b) = (1, 3, 4, 1)$, in which case

$$E(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}.$$

The additional torsion points, on this model of Cremona's 48A, correspond to, again, a trivial solution to (5), and to the case $(n, d) = (-2, 1)$. □

4.2. **The case k=5.** Next, let $k = 5$. By the above results for equation (33), if we write $S(m)$ for the square-free integer of maximum modulus dividing m, it follows, recalling (10), that

$$S(b_0 b_1 b_2 b_3) = S(b_1 b_2 b_3 b_4) = 6.$$

Multiplying these two terms together, we conclude that $S(b_0 b_4) = 1$ and so, since $d > 0$ implies that the sequence $\text{sign}(b_i)$ is nondecreasing in i, necessarily the b_i are all of the same sign. On the other hand, Lemma 4.1, as applied to (35), leads to the conclusion that $S(b_0 b_1 b_3 b_4) = -6$, a contradiction.

4.3. **The case k=6.** The great majority of our work, if $l = 2$, is devoted to the situation when $k = 6$. The easy part of this case is the following result.

Lemma 4.2. *The Diophantine equation*

$$\Pi(0, 1, 2, 3, 4, 5) = by^2, \quad b \in \{\pm 1, \pm 2, \pm 3, -5, \pm 6, \pm 10, \pm 15, 30\} \tag{38}$$

has no solutions in coprime nonzero integers n and d, with $d > 0$ and nonzero integer y.

Proof. Writing

$$n/d = (x - 5)/2, \quad y = d^3 v/2^3,$$

we find that solutions to (38) correspond to rational points on the genus 2 curve

$$(x^2 - 1)(x^2 - 9)(x^2 - 25) = bv^2.$$

This genus 2 curve obviously covers the elliptic curves

$$(X - 1)(X - 9)(X - 25) = bY^2 \text{ and } (1 - X)(1 - 9X)(1 - 25X) = bY^2.$$

It is easily checked with a suitable computer algebra package that for each of the values of b mentioned in the lemma, at least one of these curves has rank 0 and that its rational points are only the 4 rational 2-torsion points with $Y = 0$ or $Y = \infty$. These points correspond to solutions with $y = 0$. □

To complete the proof of Theorem 1.2 in case $k = 6$ and $l = 2$, it remains to deal with the values

$$b \in \{-30, 5\}.$$

First assume that $b = -30$. By symmetry, we may suppose that $5 \mid b_0 b_1 b_2$ (and consequently, $5 \nmid b_3 b_4 b_5$). We start with the case where $5 \mid b_0$. By Lemma 4.1 (equation (36)),

$$S(b_0 b_1 b_2 b_5) = \pm 30 \quad \text{and} \quad S(b_0 b_3 b_4 b_5) = \pm 30.$$

Thus $S(b_1 b_2 b_3 b_4) = \pm 1$ which, by Lemma 4.1, gives a contradiction. If $5 \mid b_1$ then Lemma 4.1 leads to the conclusion that $S(b_2 b_3 b_4 b_5) = 6$, whence, from the fact that $b < 0$, $n < 0$ and $n + d > 0$. From (34), we thus have $S(b_0 b_2 b_3 b_4) = -6$, $S(b_0 b_1 b_2 b_4) = -5$ and so $S(b_0 b_5) = -1$, whereby $b_0 = -1$, $b_5 = 1$. From Lemma 4.1, as applied to (33), we thus have $b = -30$, $S(b_1 b_2 b_3 b_4) = 30$. It follows, then, that $b_1 = 5$ and so $S(b_2 b_4) = 1$ and $b_3 = 6$, whence

$$S(b_0 b_1 b_2 b_3) = -30,$$

contradicting Lemma 4.1. If $5 \mid b_2$ then by Lemma 4.1, as applied to (35), $S(b_0 b_1 b_3 b_4) = -6$. As $n+5d > 0$, we have $n+2d > 0$. Hence $n < 0$ and $n+d > 0$. By Lemma 4.1, we have $S(b_0 b_1 b_2 b_4) = S(b_0 b_2 b_3 b_4) = -5$. Thus $3 \nmid b_0 b_1 b_3 b_4$, which contradicts $S(b_0 b_1 b_3 b_4) = -6$.

Finally, let $b = 5$. In this case, the equation $\Pi_6 = by^2$ defines a hyperelliptic curve of genus 2, which fails to cover a rank 0 elliptic

curve over $\mathbb{Q}$. Further, since the Jacobian of this curve has Mordell-Weil rank 2, traditional Chabauty-type methods do not suffice to find the rational points in question. To deal with this situation, we will apply recent techniques of Bruin and Flynn [5] (cf. [3] and [4]). For our purposes, it will be preferable to consider the isomorphic curve

$$C \ : \ Y^2 = (X-60)(X-30)(X+20)(X+30)(X+60).$$

To see how this is obtained from a solution to $\Pi_6 = 5y^2$, write $x = n/d$ and $t = 5y/d^3$, so that, after homogenizing,

$$t^2z^4 = 5x^6 + 75x^5z + 425x^4z^2 + 1125x^3z^3 + 1370x^2z^4 + 600xz^5.$$

The change of variables

$$x = -2X + 60Z, \ \ t = -60Y, \ \ z = X$$

thus leads to

$$\begin{aligned} Y^2Z^3 \ &= \ X^5 + 20X^4Z - 4500X^3Z^2 - 90000X^2Z^3 \\ &\quad +3240000XZ^4 + 64800000Z^5 \end{aligned}$$

or, dehomogenizing, the curve C.

Proposition 4.3. *The only rational solutions* (X, Y) *to the equation*

$$Y^2 = (X-60)(X-30)(X+20)(X+30)(X+60)$$

are with

$$X \in \{-60, -30, -20, -15, 20, 30, 60\}.$$

Proof. Begin by observing that a rational point on C gives rise to a rational solution to the system of equations

$$\begin{aligned} X - 60 &= \delta_1 Y_1^2 \\ X - 30 &= \delta_2 Y_2^2 \\ X + 20 &= \delta_3 Y_3^2 \\ X + 30 &= \delta_4 Y_4^2 \\ X + 60 &= \delta_5 Y_5^2, \end{aligned}$$

for some 5-tuple $(\delta_1, \ldots, \delta_5)$ where $\delta_i \in \mathbb{Q}^*/\mathbb{Q}^{*2}$. In fact, since the roots of the linear factors are all distinct modulo any prime p outside the set $\{2, 3, 5\}$, it can easily be shown that these $\{\delta_i\}$ can be taken to be $\{2, 3, 5\}$-units. A straightforward 2-descent on $\mathrm{Jac}_C(\mathbb{Q})$ (see e.g. [7], [40]) shows that the $\{\delta_i\}$ lie in a group isomorphic to $(\mathbb{Z}/2\mathbb{Z})^6$, generated by

$$\begin{aligned} &(-3, -5, 5, 15, 5), \ (3, 1, -1, -15, 5), \ (2, 5, 1, 5, 2), \\ &(3, 6, 1, 15, 30), \ (15, 15, 10, 3, 30), \ (3, 1, 5, 30, 2). \end{aligned}$$

This group corresponds to the 2-Selmer group of the Jacobian of our curve. Since the torsion part of the Mordell-Weil group of $\mathrm{Jac}_C(\mathbb{Q})$ is generated by

$$\{[(60, 0) - \infty], [(30, 0) - \infty], [(-20, 0) - \infty], [(-30, 0) - \infty]\},$$

this implies, upon noting the (independent) divisors $[(-15, 3375) - \infty]$ and $[(20, 8000) - \infty]$, of infinite order, that the rank of $\mathrm{Jac}_C(\mathbb{Q})$ is 2. As mentioned earlier, this fact ensures that a direct application of traditional Chabauty methods is not a viable option. To proceed, we will consider covers of C, as in [3], [4].

Note that if the system above has a solution, then this gives rise to a solution to, say,

$$(X - 60)(X - 30)(X + 20) = \delta_1\delta_2\delta_3(Y_1Y_2Y_3)^2.$$

Since this equation describes a genus 1 curve and there are obvious rational points on it, it models an elliptic curve, the Mordell-Weil rank of which we may bound via 2-descent. If this rank turns out to be zero, then we automatically find only a finite number of candidate solutions to our original system.

Applying this argument with all choices of 3 or 4 equations from the above system enables us to greatly reduce the possibilities for the 5-tuples $\{\delta_i\}$. We readily verify that, for the choices of $\{\delta_i\}$ which lead to coverings of rank 0 elliptic curves over $\mathbb{Q}$, the corresponding torsion points produce no points on C other than those with $Y = 0$. Carrying out this procedure for all 64 potential $\{\delta_i\}$, there remain only 2 possible 5-tuples that lead, in all cases, to elliptic curves of positive rank, namely

$$(-3, -5, 5, 15, 5) \text{ and } (-10, -10, 10, 2, 5).$$

They correspond to the solutions $(X, Y) = (-15, 3375)$ and $(X, Y) = (20, 8000)$, respectively. This is to be expected: these are non-trivial solutions and, on each of the covered genus 1 curves, they have no particular reason to map to a torsion point. Indeed, in each case, they correspond to points of infinite order.

Note also that the original equation has an extra automorphism given by $(X, Y) \mapsto (6 - X, Y)$ and that these two rational points are interchanged under this automorphism. Therefore, if we show that the values $(X, Y) = (-15, \pm 3375)$ are the only solutions corresponding to the 5-tuple $(-3, -5, 5, 15, 5)$, then we may reach a similar conclusion, via symmetry, for $(X, Y) = (20, \pm 8000)$ and $(-10, -10, 10, 2, 5)$. We will therefore specialize the δ_i to $(-3, -5, 5, 15, 5)$.

From consideration of the system of equations

$$\begin{aligned} -3X + 180 &= Z_1^2 \\ -5X + 150 &= Z_2^2 \\ 5X + 100 &= Z_3^2 \\ 15X + 450 &= Z_4^2 \\ 5X + 300 &= Z_5^2, \end{aligned}$$

let us therefore adopt the strategy suggested in [5] and analyze the fibre product of the following two covers of the X-line :

$$(-5X + 150)(5X + 100)(15X + 450) = (Z_1Z_2Z_3)^2 \tag{39}$$

and

$$5X + 300 = Z_5^2.$$

This gives us a V_4-extension of the X-line. The fibre-product D is a new curve of genus 2 with Jacobian isogenous to the product of the elliptic curve (39) and the quadratic subcover

$$(-5X + 150)(5X + 100)(15X + 450)(5X + 300) = (Z_1Z_2Z_3Z_5)^2$$

(each of these genus 1 curves has rank 1). Substituting

$$X = \left(Z_5^2 - 300\right)/5$$

into (39), we obtain a curve isomorphic to

$$D: \ -(u^2 - 2)(9u^2 - 8)(3u^2 - 2) = v^2.$$

Arguing as previously, a rational point (u, v) on this curve gives rise to a solution of the system of equations

$$\begin{aligned} 3u^2 - 2 &= v_1^2 \\ 9u^2 - 8 &= v_2^2 \\ u^2 - 2 &= -v_3^2. \end{aligned}$$

Again, we might, via products of pairs of these equations, be led to consider elliptic covers E over $\mathbb{Q}$. The presence of the points $(\pm 1, \pm 1)$ on each of these curves, however, suggests that they will have positive rank and, indeed, it is easy to verify that they do. On the other hand, by factoring the above equations, we may obtain elliptic curves over a suitable ground field extension. This is a useful observation at this stage because, in such a situation, a rank 1 curve may still permit a successful Chabauty-type argument.

Let us choose α with $\alpha^2 = 2$ and set $K = \mathbb{Q}(\alpha)$. Consider the equations

$$Q(u) = (u - \alpha)(3u + 2\alpha)$$

and

$$R(u) = -9u^4 - 3\alpha u^3 + 18u^2 + 2\alpha u - 8.$$

Since $\mathrm{Norm}_{K/\mathbb{Q}}(Q) = (u^2-2)(9u^2-8)$, if, for $u \in \mathbb{Q}$, there are $v_1, v_2, \delta \in K^*$ satisfying

$$\begin{aligned} Q(u) &= \delta v_1^2 \\ R(u) &= \delta v_2^2, \end{aligned}$$

we must have that $-\mathrm{Norm}_{K/\mathbb{Q}}(\delta)$ is a square in $\mathbb{Q}$. Furthermore, it is clear that δ can be taken to be a square-free $\{2, 3, 5\}$-unit in K^* (or perhaps, to be more precise, we should say a $\{\alpha, 3, 5\}$-unit).

Applying local arguments, restricting u to values in $\mathbb{Q}_p$ and seeing if there are $v_1, v_2 \in K \otimes \mathbb{Q}_p$ satisfying the equations above, we find that, in fact, we can restrict attention to either $\delta = -\alpha - 1$ or $\delta = \alpha + 1$. These are readily seen to correspond to the points $(1, \pm 1)$ and $(-1, \pm 1)$, respectively. Again, the automorphism $(u, v) \mapsto (-u, v)$ interchanges these points. It thus suffices, by symmetry, to consider only the case where $\delta = \alpha + 1$.

We find, after a little work, that the curve defined by the equation $R(u) = (\alpha+1)v_2^2$ is isomorphic to

$$E \;:\; y^2 = x^3 + 18(1-\alpha)x^2 + 4(3-2\alpha)x.$$

In these coordinates,

$$u = \frac{(2\alpha-3)x + (-2\alpha-2)y - 4\alpha - 19}{7x + (2\alpha+2)y + (-15\alpha-36)/2}.$$

The group $E(K) = \mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ is generated (up to a finite index, prime to $2\cdot 41$) by $g = (4\alpha+6, 10\alpha+10)$ and $T = (0,0)$. A standard Chabauty-type argument (see [3], [4]) using the prime 41 shows that 0 and $-2g$ are the only two points in $E(K)$ that yield a rational value for u, namely -1. Tracing this backwards, we find that this corresponds to the point $(X,Y) = (-15, \pm 3375)$, as claimed. This completes the proof of Proposition 4.3. □

With this proposition in place, it is a simple matter to check that the equation $\Pi_6 = 5y^2$ has only the nontrivial solutions $n \in \{-1, 6\}$ and $d = 1$, concluding the proof of Theorem 1.2 for $(k,l) = (6,2)$.

4.4. **The cases k = 7, 8, 9, 10 and 11.** To treat the cases $7 \le k \le 11$, it is enough to observe that either there exists an i with $0 \le i \le k-8$ for which $7 \mid n+id$ (so that 7 divides precisely two terms of the product Π), or that no such i exists (whence, 2 divides $\nu_7(n+jd)$ for $0 \le j \le k-1$). In the former case, we may apply our result for $k=6$ to the product $\Pi(i+1, i+2, \ldots, i+6)$ to reach the desired conclusion. In the latter, considering $\Pi(0,1,2,3,4,5)$ suffices. In particular, we find only the solutions corresponding to $(n,d) = (-7,2)$ (with $k = 8$ or 9) and to $(n,d) = (-9,2)$ (with $k = 9$ or 10). This completes the proof of Theorem 1.2, in case $l = 2$.

5. Proof of Theorem 1.2 in case $l = 3$

As noted in Section 2, given l and k, finding all coprime solutions n, d to equation (1) can be accomplished by determining the rational points on a finite number of algebraic curves. Up to this point, we have essentially relied upon equation (10) to derive single curves of, for instance, the shape (12). In this section, we will use all the information at our disposal, noting that a solution to (1), via elimination of n and d in the corresponding equations (10), implies the existence of a rational point on the non-singular curve (in $\mathbb{P}^{k-1}$) $C_{\underline{b},k,l}$, defined by the equations

$$(s-t)b_r y_r^l + (t-r)b_s y_s^l + (r-s)b_t y_t^l = 0,$$

where $\{r,s,t\}$ runs through all 3-element subsets of $\{0,\ldots,k-1\}$. Here, we write $\underline{b}$ as shorthand for $(b_0,\ldots,b_{k-1})$. We will suppress the dependence on k and l in the notation, and merely write $C_{\underline{b}}$. For the

rest of this section we take $l = 3$. For any given triple $\{r, s, t\} \subset \{0, \dots, k-1\}$, we have, as noted previously, a morphism

$$\begin{array}{rccc} \pi_{\{r,s,t\}} : & C_{\underline{b}} & \to & D_{\{r,s,t\},\underline{b}} \\ & (y_0 : \cdots : y_{k-1}) & \mapsto & (y_r : y_s : y_t) \end{array}$$

where $D_{\{r,s,t\},\underline{b}}$ is a smooth diagonal plane cubic of the form

$$D_{\{r,s,t\},\underline{b}} : Au^3 + Bv^3 + Cw^3 = 0.$$

It is convenient, for our purposes, to consider a second morphism

$$\begin{array}{rccc} \phi : & D_{\{r,s,t\},\underline{b}} & \to & E_{abc} \\ & (u : v : w) & \mapsto & (a^3buvw : a^3b^2v^3 : a^2w^3), \end{array}$$

to the curve

$$E_d \ : \ y^2z + dyz^2 = x^3.$$

Since E_d and $E_{d'}$ are isomorphic if and only if d/d' is a cube and, for our applications, we only need to consider d with $P(d) \leq 5$, the following lemma thus classifies the ranks of $E_d(\mathbb{Q})$ we encounter.

Lemma 5.1. *Let* $d = 2^{e_2}3^{e_3}5^{e_5}$ *for* $e_2, e_3, e_5 \in \{0, 1, 2\}$. *For*

$$d \in \{6, 9, 12, 15, 20, 50, 75, 90, 180, 450, 900\}$$

we have $\operatorname{rk} E_d(\mathbb{Q}) = 1$. *For other values of* d *we have* $\operatorname{rk} E_d(\mathbb{Q}) = 0$.

Proof. For each of the 27 possible values of d, the statement is easily checked with any of the computer algebra systems capable of bounding ranks of elliptic curve using 2-descent. Alternatively, one could compute the analytic ranks of these curves and, since we find them to be at most 1, conclude they must equal the actual ranks. □

For each $C_{\underline{b}}$, it thus suffices to find an elliptic curve E_d of rank 0 which it covers. For each such rank 0 curve encountered, we may analyze each of the (finitely many) torsion points $T \in E_d(\mathbb{Q})$ and determine the rational points in the 0-dimensional fibre $(\phi \circ \pi)^{-1}(T)$. This is easily done with any modern computer algebra package; for a Magma [2] transcript of these computations, see [6].

We will now treat the cases $3 \leq k \leq 11$ in turn. For $3 \leq k \leq 5$ and $l = 3$, we note that Theorem 1.2 appears to be a consequence of Theorems 8 and 9 of [19]. Unfortunately, as we have previously noted, the proofs of these theorems require modification as they depend upon an incorrect result (Lemma 6 of [19]).

5.1. **The case k=3.** To begin, we need to determine the solutions to the equation

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

for $b = 1, 2$ and 4. The coprimality of n and d implies that $\gcd(b_i, b_j) \mid (i - j)$, yielding 10 possible values for $\underline{b}$.

Note that, in this case, $C_{\underline{b}}$ is the same as the curve $D_{\{0,1,2\},\underline{b}}$. Furthermore, each corresponding E_d is of rank 0. The points corresponding

to the rational torsion of E_d lead, after a little work, to the arithmetic progressions (modulo reversion and $(n,d) \mapsto (-n,-d)$)

$$(-2,1,4),(0,1,2),(-1,0,1) \text{ and } (1,1,1).$$

5.2. **The case k=4.** Here, we have to consider

$$b \in \{1,2,4,3,6,12,9,18,36\}.$$

Using the coprimality of n and d, these lead to 180 values of $\underline{b}$. For most choices of $\underline{b}$, one of the curves $D_{\{0,1,2\}}, D_{\{0,1,3\}}, D_{\{0,2,3\}}$ or $D_{\{1,2,3\}}$ corresponds to an E_d of rank 0. A straightforward computation shows that those values of $\underline{b}$ lead only to the arithmetic progressions

$$(0,1,2,3),(-1,0,1,2),(1,1,1,1) \text{ and } (-3,1,1,3).$$

However, for $\underline{b} = (1,2,3,4)$ or $(-6,-1,4,9)$, we find that all corresponding genus 1 subcovers of $C_{\underline{b}}$ have infinitely many rational points. Furthermore, since $(1:1:1:1) \in C_{\underline{b}}(\mathbb{Q})$, local considerations also fail to rule out these possibilities. To proceed, we need to consider other quotients of $C_{\underline{b}}$.

Let us write ζ for a primitive cube root of unity and define morphisms

$$\begin{array}{rccl} \zeta_0: & (y_0:y_1:y_2:y_3) & \mapsto & (\zeta y_0:y_1:y_2:y_3) \\ \zeta_1: & (y_0:y_1:y_2:y_3) & \mapsto & (y_0:\zeta y_1:y_2:y_3) \\ \zeta_2: & (y_0:y_1:y_2:y_3) & \mapsto & (y_0:y_1:\zeta y_2:y_3). \end{array}$$

Obviously, we have

$$\langle \zeta_0, \zeta_1, \zeta_2 \rangle \subset \mathrm{Aut}_{\overline{\mathbb{Q}}}(C_{\underline{b}}).$$

Writing C for one of $C_{(1,2,3,4)}$ or $C_{(-6,-1,4,9)}$, we note that quotients of C by subgroups defined over $\mathbb{Q}$ yield curves covered by C. For instance, $D_{\{1,2,3\}} \simeq C/\langle \zeta_0 \rangle$ and the corresponding E_d is isomorphic to $C/\langle \zeta_0, \zeta_1\zeta_2^2 \rangle$.

For our purposes, we will focus on the order 9 subgroup

$$H = \langle \zeta_0\zeta_1, \zeta_0\zeta_2 \rangle.$$

To derive a model for the curve $D = C/H$, we consider the H-invariant functions $y_0y_1^2y_2y_3^2$, y_2^3, y_3^3 on C. In fact, for $\underline{b} = (1,2,3,4)$ and

$$\begin{array}{rcl} x & = & 2y_0^2y_1y_2^2y_3/(9y_2^6 - 8y_2^3y_3^3) \\ y & = & (-27y_2^6 + 36y_2^3y_3^3 - 16y_3^6)/(9y_2^6 - 8y_2^3y_3^3), \end{array}$$

we obtain

$$D \ : \ y^2 = x^6 - 3x^3 + 9.$$

Via a 2-descent in the style of [8], implemented by Stoll in Magma as described in [40], together with a point search and some canonical height computations (see [39], [41]), we find that

$$\mathrm{Jac}(D)(\mathbb{Q}) \simeq \mathbb{Z}/3 \times \mathbb{Z}/3 \times \mathbb{Z}.$$

Using the identification $\mathrm{Jac}(D)(\mathbb{Q}) = \mathrm{Pic}^0(D/\mathbb{Q})$ and the convention that ∞^+, ∞^- denote the two branches of D above $x = \infty$, we write

$$\mathrm{Jac}(D)(\mathbb{Q}) = \langle [\infty^+ - \infty^-], [(0,3) - \infty^-], [(2,7) - \infty^-] \rangle,$$

where the first two generators are of order 3 and the last generates the free part.

Via a standard application of explicit Chabauty-type methods in the style of [15], implemented in Magma by Stoll, and using $p = 7$, we compute that $D(\mathbb{Q})$ has at most 6 elements and that, in fact,

$$D(\mathbb{Q}) = \{\infty^+, \infty^-, (0,3), (0,-3), (2,7), (2,-7)\}.$$

When we pull back these points along the map

$$\pi : (y_0 : y_1 : y_2 : y_3) \mapsto (x, y),$$

we see that only $(2,-7)$ lifts to a rational point $(1:1:1:1) \in C(\mathbb{Q})$. This completes the first part of the proof.

For $\underline{b} = (6,1,4,9)$ we proceed similarly and, in fact, writing

$$\begin{aligned} x &= 2y_0y_1^2y_2y_3^2/(8y_2^3y_3^3 - 9y_3^6) \\ y &= (16y_2^6 - 36y_2^3y_3^3 + 27y_3^6)/(8y_2^3y_3^3 - 9y_3^6), \end{aligned}$$

find that $C_{(6,1,4,9)}$ covers the same curve D. Lifting the rational points of D along the map π yields, again, that only $(2,-7)$ gives rise to a rational point on $C_{\underline{b}}$. This completes the proof of Theorem 1.2 provided $k = 4$ and $l = 3$.

5.3. **The case k=5.** If $k = 5$, dividing Π by one of n or $n + 4d$ necessarily reduces the problem to the case $k = 4$. A short calculation shows that no new solutions to (5) accrue.

5.4. **The case k=6.** Let $k = 6$. If $5 \nmid (n + 2d)(n + 3d)$, then we may apply our result for $k = 4$ to $\Pi(i, i+1, i+2, i+3)$ for one of $i = 0, 1$ or 2, to conclude that the only solutions to (5), in this case, are given by

$$(n,d) = (-5,2), (-6,1) \text{ and } (1,1).$$

By symmetry, we may suppose that $5 \mid n + 2d$. This leads to 1976 possible values for $\underline{b}$. For each of these, one of the 20 elliptic curves covered by $C_{\underline{b}}$ is of rank 0, whereby we can employ our previous approach. To cut down on the amount of computation required, however, it is worth noting that one can eliminate most $\underline{b}$ from consideration by testing if $C_{\underline{b}}(\mathbb{Q}_p)$ is nonempty for, say, $p = 2, 3$ and 7. This reduces the number of $\underline{b}$ to treat to 18 and, for each of these, $C_{\underline{b}}$ indeed has a rational point. These all correspond to the arithmetic progression

$$(-2, -1, 0, 1, 2, 3).$$

5.5. **The cases k = 7, 8, 9, 10 and 11.** For the cases $7 \le k \le 11$, we argue exactly as when $l = 2$; in all situations, consideration of one of $\Pi(i+1, i+2, \ldots, i+6)$ suffices to reduce the problem to the previously treated $k = 6$. This completes the proof of Theorem 1.2 when $l = 3$.

6. Proof of Theorem 1.2 in case $l = 5$

We begin this section by proving a pair of results on ternary Diophantine equations of signature $(5, 5, 5)$. The first follows from a variety of classical arguments. The second is a consequence of work of a much more recent vintage, due to Kraus [21].

Proposition 6.1. *Let C be a positive integer with $P(C) \leq 5$. If the Diophantine equation*

$$X^5 + Y^5 = CZ^5 \tag{40}$$

has solutions in nonzero coprime integers X, Y and Z, then $C = 2$ and $X = Y = \pm 1$.

Proof. Without loss of generality, we may suppose $C = 2^\alpha 3^\beta 5^\gamma$ with $0 \leq \alpha, \beta, \gamma \leq 4$. By old results of Dirichlet, Lebesgue (see e.g. [13], p. 735, item 20 and p. 738, item 37), and P. Dénes (c.f. [12]), for (40) to have a solution in coprime nonzero integers with $XYZ \neq \pm 1$, we require $C > 2$ and

$$C^4 \equiv 1 \pmod{5^2}.$$

This implies that $\gamma = 0$ and

$$(\alpha, \beta) \in \{(1, 2), (2, 4), (3, 1), (4, 3)\}.$$

From the fact that both 2 and 3 are primitive roots modulo 5, and the exponent 5 is a regular prime, a classical result of E. Maillet (see e.g. [13], p. 759, item 167) leads to the conclusion that $5 \nmid Z$. Since, for each remaining value of C, we have

$$C^4 \not\equiv 2^4 \pmod{5^2},$$

Theorem 1 of Győry [16] thus implies that

$$r^4 \equiv 1 \pmod{5^2},$$

for every divisor r of C. The parity of the remaining C (whereby we are free to choose $r = 2$ above) provides an immediate contradiction and hence the desired result. □

Proposition 6.2. *Let A and B be coprime positive integers with $AB = 2^\alpha 3^\beta$ for nonnegative integers α and β with $\alpha \geq 4$. Then the Diophantine equation*

$$AX^5 + BY^5 = Z^5 \tag{41}$$

has no solutions in coprime nonzero integers X, Y and Z.

Proof. This is a result of Kraus [21] and is essentially a consequence of the fact that there are no weight 2, level N cuspidal newforms of trivial character, for N dividing 6. □

We suppose throughout this section that $l = 5$. In what follows, our arguments will typically rely upon the fact that a careful choice of identity $[q, r, s]$ leads to an equation of the form (40). In other cases, such identities imply equations which may be proven insoluble modulo 11 or 25. We shall employ the trivial observation that, for $k \leq 11$, at most one factor of Π_k is divisible by 11.

6.1. **The case k=3.** From the identity $[0, 1, 2]$, we deduce a solution in nonzero integers to equation (40), with $P(C) \leq 2$ (and hence $C = 2$). A short calculation leads to the conclusion that $(n, d) = (-2, 3)$ or $(-4, 3)$.

6.2. **The case k=4.** The following lemma is a more precise version of Theorem 1.2 in case $k = 4$. It will prove useful in analyzing larger values of k.

Lemma 6.3. *Suppose that there exist nonzero integers n, d, y and b with b, d positive and $\gcd(n, d) = 1$, satisfying*

$$\Pi_4 = by^5 \quad \textit{with} \quad P(b) \leq 3. \tag{42}$$

Then either $(n, d) = (-3, 2)$ or, up to symmetry,

$$(b_0, b_1, b_2, b_3) = (4, 3, 2, 1) \textit{ or } (9, 4, 1, 6). \tag{43}$$

It is likely that $(n, d) = (-9, 5), (-6, 5), (-4, 1), (-3, 2)$ and $(1, 1)$ are the only solutions of (42).

Proof. Let us suppose we have a solution to (42) in nonzero integers n, d, y and b, with $b, d > 0$ and $\gcd(n, d) = 1$. If 3 fails to divide the product $b_i b_{i+1} b_{i+2}$ for either $i = 0$ or $i = 1$, we may reduce immediately to the case $k = 3$. We may thus assume, via symmetry, that either $3 \mid b_0$ and $3 \mid b_3$, or that $3 \mid b_1$. In the first case, if $\nu_3(b_0 b_3) = 2$, the identity $[0, 1, 3]$ implies a nontrivial solution to an equation of the form $X^5 + Y^5 = 2^\alpha Z^5$ and hence, after a little work, a contradiction via Proposition 6.1. We may thus suppose, again by symmetry, that $9 \mid b_0$. Further, unless $2 \mid n + d$, we may apply the same identity $[0, 1, 3]$ to deduce a nontrivial solution to

$$X^5 + Y^5 = 2^\alpha 3^\beta Z^5, \tag{44}$$

contrary to Proposition 6.1. Combining the identities $[0, 1, 2]$ and $[0, 2, 3]$ with Proposition 6.2, we may assume that $\nu_2((n+d)(n+3d)) = 3$. If $\nu_2(n + d) = 1$, $[1, 2, 3]$ leads to a solution to (44) with $\alpha = \beta = 1$. If, on the other hand, $\nu_2(n + 3d) = 1$, from the fact that

$$t^5 \equiv 0, \pm 1 \pmod{11}, \text{ for } t \in \mathbb{Z},$$

the identity $[1, 2, 3]$ implies that $\Pi(1, 2, 3)$ is not divisible by 11. It follows from $[0, 1, 3]$ that $\nu_3(n) = 2$ (whereby (b_0, b_1, b_2, b_3) is just $(9, 4, 1, 6)$).

If, however, $3 \mid b_1$, $[0,1,2]$ and Proposition 6.1 imply that we may suppose $2 \mid n$, whereby, again combining $[1,2,3]$, $[0,1,3]$ and Proposition 6.2, we may assume that $\nu_2(n(n+2d)) = 3$. In case $\nu_2(n) = 1$, $[0,2,3]$ leads to a solution to (44) with $\beta = 1$, a contradiction. If $\nu_2(n) = 2$, the same identity $[0,2,3]$ implies that 11 fails to divide $n + 2d$ and so, modulo 11, from $[0,1,2]$, we are able to conclude that $\nu_3(b_1) = 1$, whence

$$(b_0, b_1, b_2, b_3) = (4, 3, 2, 1).$$

□

6.3. **The case k=5.** Let $k = 5$ and suppose that we have a nontrivial solution to (5). Then applying Lemma 6.3 to $\Pi(0,1,2,3)$ and $\Pi(1,2,3,4)$, it follows that either $n + id = -3$, $d = 2$ for $i = 0$ or 1 (which fails to yield a solution to (5)) or that both 4-tuples (b_0, b_1, b_2, b_3) and (b_1, b_2, b_3, b_4) are in the set :

$$\{(1,2,3,4), (4,3,2,1), (6,1,4,9), (9,4,1,6)\}.$$

Since this is readily seen to be impossible, we conclude that equation (5) has no solutions in this case.

6.4. **The case k=6.** As in case $l = 2$ or 3, most of our work in proving Theorem 1.2 is concentrated, if $l = 5$, in treating $k = 6$. Let us suppose we have a nontrivial solution to (5) with $P(b) \leq 5$. If 5 fails to divide the product $b_0b_1b_2b_3b_4b_5$, then, omitting the factor $n + 5d$ in Π_6, we reduce to the case $k = 5$ and hence find no new solutions.

By symmetry, it suffices to deal with the cases when $5 \mid n$, $5 \mid n + d$ or $5 \mid n + 2d$. We consider them in turn.

6.4.1. $5 \mid n$. First assume that $5 \mid n$ and hence also $5 \mid n + 5d$. Then, applying Lemma 6.3 to $\Pi(1,2,3,4)$, we infer that either $n + d = -3$, $d = 2$ (which gives the solution $(n, d) = (-5, 2)$), or we have, again up to symmetry,

$$(b_1, b_2, b_3, b_4) = (4, 3, 2, 1) \text{ or } (9, 4, 1, 6).$$

Consider the identity

$$3(n+d)(n+4d) - 2(n+2d)(n+3d) = n(n+5d). \tag{45}$$

If $(b_1, b_2, b_3, b_4) = (4, 3, 2, 1)$, (45) implies a nontrivial solution to (40), contradicting Proposition 6.1. If, however, $(b_1, b_2, b_3, b_4) = (9, 4, 1, 6)$, (45) leads to an equation of the form

$$3^4X^5 + 2^2Y^5 = 5^tZ^5$$

where $t \geq 2$ and $5 \nmid XY$. Working modulo 25 and taking 4th powers, we deduce the congruence

$$3^{16} \equiv 2^8 \pmod{5^2},$$

and hence a contradiction.

6.4.2. $5 \mid n+d$. Consider now the case when $5 \mid n+d$. We apply Lemma 6.3 to $\Pi(2,3,4,5)$. It is clear that $n+2d=-3$, $d=2$ does not provide a further solution to (5). We thus have

$$(b_2,b_3,b_4,b_5) \in \{(4,3,2,1),(1,2,3,4),(9,4,1,6),(6,1,4,9)\}.$$

In the first of these cases, necessarily $b_0 = 2\cdot 3^t$ for a nonnegative integer t. From the identity $[2,3,4]$, we find that

$$2y_2^5 + y_4^5 = 3y_3^5$$

and hence 11 fails to divide $y_2y_3y_4$. Similarly, $[1,3,4]$ yields the conclusion that y_1 is coprime to 11, whereby, from $[1,2,3]$ and its companion equation

$$5^{\nu_5(b_1)}y_1^5 + 3y_3^5 = 8y_2^5,$$

we may conclude not only that $\nu_5(b_1)=1$ (so that $b_1=5$), but also

$$y_2^5 \equiv y_3^5 \equiv \pm 1 \pmod{11}.$$

Applying $[0,2,3]$, then, we obtain a solution to the equation

$$3^{\nu_3(b_0)-1}y_0^5 + y_3^5 = 2y_2^5, \tag{46}$$

and find, working modulo 11, that necessarily $\nu_3(b_0)=1$. Applying Proposition 6.1 to (46), we have that $XYZ=\pm 1$. From this, we obtain the solution $(n,d)=(-6,1)$ to (5) (together with the symmetrical solution $(1,1)$).

If we have (b_2,b_3,b_4,b_5) equal to either $(1,2,3,4)$ or $(9,4,1,6)$, then the identities $[0,1,2]$ and $[0,2,4]$, respectively, lead to nontrivial solutions to (40), contradicting Proposition 6.1. Finally, if $(b_2,b_3,b_4,b_5) = (6,1,4,9)$, then $[0,1,5]$ implies that

$$2^{\nu_2(b_0)+2}y_0^5 \equiv 9y_5^5 \pmod{25}$$

and so, taking 4th powers, we conclude that $\nu_2(b_0)=2$. This, together with $[0,2,4]$, contradicts Proposition 6.1.

6.4.3. $5 \mid n+2d$. Finally, consider the case where $5 \mid b_2$. In light of the identity $\{0,1,3,4\}$ and Proposition 3.1, we may suppose that $3 \mid n(n+d)$. First, assume that $3 \mid n$. The identity $[1,3,5]$ implies a nontrivial solution to (40) unless $4 \mid n+d$. Under this assumption, $[0,3,4]$ and Proposition 6.1 yield the conclusion that $\nu_3(n) \geq 2$, whence $\nu_3(n+3d)=1$ (and so $b_3=6$). From $[2,3,4]$, we deduce that

$$5^{\nu_5(b_2)}y_2^5 + y_4^5 = 12y_3^5,$$

whereby, upon consideration modulo 5^2, $\nu_5(n+2d)=1$. Analyzing the same equation, modulo 11, implies that $11 \mid y_2$. It follows, then, from the identity $[0,2,4]$, that

$$3^{\nu_3(b_0)}y_0^5 + y_4^5 = 10y_2^5.$$

Modulo 11, we therefore have that $\nu_3(b_0)=0$ and hence contradict Proposition 6.1.

The last case to consider in this subsection is when $5 \mid b_2$ and $3 \mid n+d$. From [3, 4, 5] and Proposition 6.1, we may assume that $2 \mid n+d$, whence, applying a like argument with [0, 1, 3], we necessarily have $\nu_2(n+d) = 1$. Identity [0, 1, 4], again with Proposition 6.1, gives $\nu_3(n + 4d) \geq 2$ (so that $\nu_3(n + d) = 1$ and $b_1 = 6$). Applying [0, 1, 2] thus leads to the equation

$$y_0^5 + 5^{\nu_5(b_2)} y_2^5 = 12 y_1^5.$$

Modulo 5^2 and 11, we again find that $\nu_5(b_2) = 1$ and that $11 \mid y_2$. To conclude, then, we apply the identity [0, 2, 4] which yields

$$y_0^5 + 3^{\nu_3(b_4)} y_4^5 = 10 y_2^5.$$

This implies, modulo 11, that $\nu_3(b_4) = 0$ and so, via Proposition 6.1, a contradiction.

6.5. **The cases k = 7, 8, 9, 10 and 11.** Again, we argue as for $l = 2$ or 3, applying our results for $k = 6$ to one of $\Pi(i, i+1, \cdots, i+5)$. This completes the proof of Theorem 1.2.

7. Proofs of Theorem 1.5 and Corollary 1.6

Having dispatched Theorem 1.2, we will now present the proof of Theorem 1.5. The reason we proceed in this order is that the techniques introduced in this section will prove useful in the subsequent treatment of Theorem 1.4.

Proof of Theorem 1.5. If $k \leq 11$, Theorem 1.5 is an immediate consequence of Theorem 1.2 (without any conditions upon d). We thus assume that $k \geq 12$ and that $l \geq 2$ is prime. For the $\pi(k)$ prime values of $l \leq k$, we may apply Theorem 6 of [19] (a slight generalization of Corollary 2.1 of [10], itself a nice application of Falting's Theorem) to conclude that (5) has finitely many solutions as claimed. We may thus suppose that $l > k$.

Since $d \not\equiv 0 \pmod{D_k}$ (recall definition (7)), there exists a prime in the interval $[k/2, k)$ which is coprime to d and hence divides y. Define p to be the largest such prime. From (5), since $\gcd(n, d) = 1$ and $P(b) < k/2$, it follows that either

(i) $p \mid n + id$ for precisely one i with $1 \leq i \leq k - 2$, or

(ii) $p \mid n + id$ and $p \mid n + (i + p)d$, for some i with $0 \leq i \leq k - 1 - p$.

In case (i), the identity $\{i-1, i, i, i+1\}$ leads to a ternary equation of the form (14) where $C = 1$ and A, B, u and v are nonzero integers with $P(AB) < p$ and $p \mid uv$. We associate to this equation, as in the proof of Proposition 3.1, a Frey elliptic curve $E/\mathbb{Q}$, with corresponding mod l Galois representation ρ_l^E. Again, this arises from a cuspidal newform

f of weight 2, trivial Nebentypus character and level N. Here, from Lemma 3.2 of [1], N divides

$$N_1 = 64 \cdot \prod_{q<p} q,$$

where the product is over prime q. Since $p \mid uv$ and p is coprime to lN, our Frey curve E has multiplicative reduction at p and so we may conclude, as in the proof of Proposition 3.1, that

$$\mathrm{Norm}_{K_f/\mathbb{Q}}\,(a_p \pm (p+1)) \equiv 0 \pmod{l},$$

where K_f is the field of definition for the Fourier coefficients a_n of f. By the Weil bounds for a_p, we have

$$l \leq (p+1+2\sqrt{p})^{g_0^+(N)} \tag{47}$$

where $g_0^+(N)$ denotes the dimension of the space of weight 2, level N cuspidal newforms of trivial character (as a $\mathbb{C}$-vector space).

Similarly, in case (ii), we have the identity $\{i, i+j, i+p-j, i+p\}$, where we are free to choose any j with $1 \leq j \leq (p-1)/2$. If $n(n+d)$ is odd, $p = 7$ and $k = 12$ or 13, we will take $j = 3$ whereby the above identity leads to a ternary equation of the shape (14) with coprime A, B, C satisfying $ABC \equiv 1 \pmod 2$, $P(AB) < 7$, $C \in \{1, 3\}$ and $7 \mid uv$. Otherwise, we take $j = 2$ (if $n(n+d)$ is even) or $j = 4$ (if $n(n+d)$ is odd). These choices lead to equations (14) with $P(AB) < p$, $p - j$ is divisible by C, $\gcd(AB, C) = 1$ and $p \mid uv$. Since $l > k$, in each case we may argue as previously to deduce the existence of a cuspidal newform f of weight 2, trivial Nebentypus character and level N dividing either 1440 or

$$N_2 = 64 \cdot \prod_{q_1<p} q_1 \cdot \prod_{q_2 \mid p-j} q_2$$

where again the products are over q_i prime. Arguing as before, we once more obtain inequality (47).

From Martin [24], we have, for any N, that

$$g_0^+(N) \leq \frac{N+1}{12}$$

and, via Schoenfeld [34],

$$\sum_{p \leq x} \log p < 1.000081x,$$

valid for all $x > 0$. It follows, by routine computation, that

$$g_0^+(N) < e^{1.05p}$$

and hence, from (47), that

$$\log l < 3^p < 3^k.$$

Since k is fixed, this leaves us with finitely many pairs (k, l) to consider. Again, via Theorem 6 of [19], we may conclude that, for each pair

$(k,l) \neq (3,2)$, equation (5) has at most finitely many coprime solutions with (6). This therefore completes the proof of Theorem 1.5. □

Proof of Corollary 1.6. To deduce Corollary 1.6, suppose now that $d \equiv 0 \pmod{D_k}$ (and, again, that $l > k$). Since it is easy to show that the left hand side of (5) is divisible by every prime $q \leq k$ coprime to d, it follows, writing

$$P_k = \pi(k-1) - \pi\left(\frac{k-1}{2}\right),$$

that

$$P_k \leq \omega(d) \leq D. \tag{48}$$

By the Prime Number Theorem, P_k is asymptotically $\frac{k}{2\log k}$, as $k \to \infty$. Applying Chebyshev-type estimates for $\pi(x)$, say those of Rosser and Schoenfeld [29], we may show that

$$P_k \geq \frac{k}{3\log k}, \quad \text{if } \ k \geq 18.$$

From our lower bound (8) for k, we therefore have

$$P_k \geq \frac{2D\log D}{\log(6D\log D)} > D,$$

for $k \geq 18$, contradicting (48). For $12 \leq k \leq 17$ and (via inequality (8)) $D \in \{1,2\}$, we check to see if inequality (48) is satisfied, obtaining a contradiction in all cases except when $D = 2$ and $k = 12, 13, 15, 16$ or 17. For each of these, $P_k = 2$ and so the fact that y fails to have a prime divisor p with $k/2 \leq p < k$ implies

$$d = \begin{cases} 7^\alpha 11^\beta & \text{if } k = 12, 13 \\ 11^\alpha 13^\beta & \text{if } k = 15, 16, 17, \end{cases}$$

where α and β are positive integers. Theorem 2 of Saradha and Shorey [32], however, shows that d necessarily has a prime divisor congruent to 1 (mod l). It follows that $l \in \{2,3,5\}$, contradicting $l > k$. This completes the proof of Corollary 1.6. □

8. Finiteness results for $12 \leq k \leq 82$

In this section, we will present the proof of Theorem 1.4. We begin by noting that, if P and Q are consecutive primes and if we know that equation (5) has finitely many solutions with $k = 2P+1$ and (6), then a similar result is immediately obtained for

$$k = 2P+2, 2P+3, \ldots, 2Q.$$

Indeed, for any of these values of k, if Π_k is divisible by a prime in the interval $[Q,k]$, then Theorem 1.5 implies the desired result. We may thus suppose, if $p \mid \Pi_k$, that either $p > k$ or $p \leq P$. It follows that we can write

$$\Pi(0,1,\cdots,2P+1) = BY^l$$

for nonzero integers B and Y with $P(B) \leq P$, whereby the result follows, as claimed, from the case $k = 2P + 1$. To prove Theorem 1.4, we may, in light of Theorem 1.2, restrict attention to

$$k \in \{15, 23, 27, 35, 39, 47, 59, 63, 75\},$$

where we further suppose that Π_k is coprime to D_k. Now, for each prime $3 \leq p \leq P$, there are $p + 1$ possibilities : either $p \mid n + sd$ for some $0 \leq s \leq p - 1$, or p fails to divide Π (i.e. $p \mid d$). Analyzing these

$$N(P) = \prod_{3 \leq p \leq P} (p + 1) \tag{49}$$

cases, for each k under consideration (actually, symmetry allows us to reduce this number somewhat), we note that if we can find integers $i \geq 0$ and $j \geq 1$ such that $6j + i \leq k - 1$ and

$$\gcd\left(\Pi(i, 3j + i, 6j + i), \prod_{3 \leq p \leq P} p\right) \in \{1, 11, 19\}, \tag{50}$$

then $\{i, 3j + i, 3j + i, 6j + i\}$ leads to an equation of the form (22). We obtain a like conclusion if there exist $i \geq 0$, $j \geq 1$ with $10j + i \leq k - 1$, for which

$$\gcd\left(\Pi(i, j + i, 9j + i, 10j + i), \prod_{3 \leq p \leq P} p\right) \in \{1, 11, 19\} \tag{51}$$

(where we employ the identity $\{i, j + i, 9j + i, 10j + i\}$).

8.1. **The case $k = 15$.** For $k = 15$ (i.e. if $P = 7$), a short search indicates that we can find i and j for which (50) or (51) holds, unless $p \mid n + i_p d$ for $p \in \{3, 5, 7\}$ where i_p are as follows :

case	(i_3, i_5, i_7)	case	(i_3, i_5, i_7)	case	(i_3, i_5, i_7)
(i)	$(2, 4, 6)$	(v)	$(0, 3, 4)$	(ix)	$(2, 4, 0)$
(ii)	$(1, 3, 5)$	(vi)	$(2, 2, 3)$	(x)	$(1, 3, 6)$
(iii)	$(0, 2, 4)$	(vii)	$(1, 1, 2)$	(xi)	$(1, 1, 1)$
(iv)	$(2, 1, 3)$	$(viii)$	$(0, 0, 1)$	(xii)	$(0, 0, 0)$

By symmetry, we may suppose that we are in one of the cases (i), (ii), (iii), (iv), (ix) or (x). In case (i), $\{1, 3, 10, 12\}$ implies an equation of the form (18) with $D = 2$, if Π is odd, and (15) with $\beta = 0$, if Π is even, unless, in this latter case, we have

$$\max\{\nu_2(n + id) : i = 1, 3, 10, 12\} = 2. \tag{52}$$

It follows, in this situation, that $\{2, 3, 11, 12\}$ leads to equation (15) with $\alpha \geq 2$, unless $9 \mid n + 2d$. If we assume, then, that $9 \mid n + 2d$, $\{5, 7, 8, 10\}$ implies an equation of the form (15) with $\beta = 0$, unless

$$\max\{\nu_2(n + id) : i = 5, 7, 8, 10\} = 2. \tag{53}$$

Combining (52) and (53), we may thus assume $\nu_2(n+10d) = 2$, whereby $\{5, 8, 9, 12\}$ leads to an equation of the form (20), completing the proof, in case (i).

In cases (ii), (ix) and (x), we argue in an identical fashion as for case (i), only with the identities

$$\{1, 3, 10, 12\},\ \{2, 3, 11, 12\},\ \{5, 7, 8, 10\} \text{ and } \{5, 8, 9, 12\}$$

replaced by

$$\{0, 2, 9, 11\},\ \{1, 2, 10, 11\},\ \{4, 6, 7, 9\},\ \{4, 7, 8, 11\}, \text{ in case (ii)},$$

$$\{1, 3, 10, 12\},\ \{2, 3, 11, 12\},\ \{3, 5, 6, 8\},\ \{1, 4, 5, 8\}, \text{ in case (ix)}$$

and

$$\{0, 2, 9, 11\},\ \{1, 2, 10, 11\},\ \{2, 4, 5, 7\},\ \{0, 3, 4, 7\}, \text{ in case (x)}.$$

In case (iii) (respectively case (iv)), the identity $\{1, 5, 10, 14\}$ (respectively $\{0, 4, 9, 13\}$) leads to the conclusion that

$$\max\{\nu_2(n + id) : i = 1, 5, 10, 14\} = 3$$

whence $\{8, 9, 9, 10\}$, $\{2, 5, 5, 8\}$, $\{7, 10, 10, 13\}$ and $\{3, 6, 6, 9\}$ (respectively $\{7, 8, 8, 9\}$, $\{1, 4, 4, 7\}$, $\{6, 9, 9, 12\}$ and $\{2, 5, 5, 8\}$) lead to equations of the shape (21) with $p \in \{3, 5\}$. This completes the proof of Theorem 1.4, if $k = 15$ (i.e. for $k \leq 22$).

8.2. **The cases $k \in \{23, 27, 35, 39\}$.** A (reasonably) short calculation reveals that for each of the $N(P)$ possibilities with $P \in \{11, 13, 17\}$, we can always find i and j satisfying (50) or (51). If $P = 19$ (so that $k = 39$), then we are left with, up to symmetry, the following cases to consider (where, as previously, $p \mid n + i_p d$) :

case	i_3	i_5	i_7	i_{11}	i_{13}	i_{17}	i_{19}
(i)	1	0	3	6	1	9	6
(ii)	1	0	4	1	8	9	17
(iii)	0	4	3	0	7	8	16
(iv)	2	3	2	10	6	7	15

In the first of these $\{8, 11, 33, 36\}$ leads immediately to an equation of the shape (15) with $\beta = 1$. In the remaining three,

$$\{2 - i, 6 - i, 29 - i, 33 - i\}$$

(for $i = 0, 1$ or 2, respectively) implies a solution to equation (15) with $(\alpha, \beta) = (0, 1)$, if Π is odd. If, however, Π is even, the identity

$$\{28 - i, 29 - i, 37 - i, 38 - i\}$$

leads to equation (15) with $\alpha \geq 2$ and $\beta = 1$, unless $9 \mid n + (28 - i)d$. In this case, the identity

$$\{13 - i, 14 - i, 16 - i, 17 - i\}$$

thus leads to equation (22) with $p = 19$. This completes the proof for $k = 39$ (and hence for $k \leq 46$).

8.3. **The cases $k \in \{47, 59, 63, 75\}$.** We verify via Maple that, for each of the $N(P)$ possibilities with $P \in \{23, 29\}$, we can always find i and j satisfying (50) or (51). For $P = 31$ (i.e. $k = 63$), there are again some possibilities that elude our sieve (the computation is now becoming rather more substantial). These 28 cases correspond, after symmetry, to $p \mid n + i_p d$ for i_p as follows :

case	i_3	i_5	i_7	i_{11}	i_{13}	i_{17}	i_{19}	i_{23}	i_{29}	i_{31}
(i)	0	3	5	1	7	1	18	2	14	10
(ii)	2	2	4	0	6	0	17	1	13	9
(iii)	0	3	5	1	7	15	18	14	16	10
(iv)	2	2	4	0	6	14	17	13	15	9
(v)	1	1	3	8	5	15	11	4	8	23
(vi)	0	0	2	7	4	14	9	3	7	22
(vii)	2	4	1	6	3	13	8	2	6	21
$(viii)$	1	1	3	8	5	15	8	4	1	23
(ix)	0	3	5	10	7	14	13	6	10	25
(x)	2	2	4	9	6	13	12	5	9	24
(xi)	0	0	2	3	4	14	9	3	7	22
(xii)	2	4	1	2	3	13	8	2	6	21
$(xiii)$	0	3	5	10	7	14	10	6	3	25
(xiv)	2	2	4	9	6	13	9	5	2	24

Our arguments will prove similar in each case. From an initial identity of the form $\{p, q, r, s\}$, we will conclude that $8 \mid n + id$ for some i congruent, modulo 8, to $p + 4$, $q + 4$, $r + 4$ or $s + 4$. For each of these possibilities, one of a collection of 4 (or 2) secondary identities of the shape $\{p_1, q_1, q_1, r_1\}$ then implies a nontrivial solution to an equation of the form (21), contradicting Proposition 3.1. For example, in case (i), $\{31, 32, 49, 50\}$ implies the desired conclusion unless

$$\max\{\nu_2(n + id) : i = 31, 32, 49, 50\} = 2.$$

This hypothesis ensures that $8 \mid n + id$ for one of $i = 3, 4, 5, 6$ which, with the identities $\{6, 11, 11, 16\}$, $\{11, 20, 20, 29\}$, $\{4, 13, 13, 22\}$ and $\{29, 30, 30, 31\}$, contradicts Proposition 3.1. For the remaining cases, we choose our identities as follows :

case	initial identity	$8 \mid n + id$
(i)	$\{31, 32, 49, 50\}$	$i = 3, 4, 5, 6$
(iii)	$\{2, 4, 29, 31\}$	$i = 0, 2, 3, 5$
$(v), (viii)$	$\{12, 14, 60, 62\}$	$i = 4, 6$
$(ix), (xiii)$	$\{16, 17, 34, 35\}$	$i = 4, 5, 6, 7$
(xi)	$\{11, 13, 59, 61\}$	$i = 3, 5$

and

case	secondary identities
(i)	$\{6,11,11,16\}, \{11,20,20,29\}, \{4,13,13,22\}, \{29,30,30,31\}$
(iii)	$\{21,24,24,27\}, \{27,42,42,57\}, \{2,11,11,20\}, \{4,13,13,22\}$
$(v), (viii)$	$\{13,28,28,43\}, \{9,22,22,35\}$
$(ix), (xiii)$	$\{1,4,4,7\}, \{16,37,37,58\}, \{17,22,22,27\}, \{2,23,23,44\}$
(xi)	$\{6,19,19,32\}, \{8,13,13,18\}$

In case (ii), (iv), (vi), (vii), (x), (xii) and (xiv), we argue as for (i), (iii), (v), (ix) and (xi), only with $\{p,q,r,s\}$ replaced, in each case, by $\{p-i,q-i,r-i,s-i\}$ for $i=1$ or $i=2$. This completes the proof of Theorem 1.4, for $63 \leq k \leq 74$.

To finish the proof of Theorem 1.4, it remains to handle the case $k = 75$. In this situation, after lengthy calculations (carried out in Maple on a Beowulf cluster at Simon Fraser University), we conclude that there always exist i and j satisfying either (50) or (51). The code utilized in this computation is available from the authors on request.

9. Concluding remarks

Presumably, the cases $2 \leq l \leq 5$ in Theorem 1.2 may be sharpened with a more careful combinatorial analysis, at least if $(k,l) \neq (4,2)$ or $(3,3)$. As far as we can tell, the statement, for large prime values of l, essentially reflects the limitations of our method. An extension of Theorem 1.2 to larger values of k would be a reasonably routine matter if one had available a full set of Galois conjugacy classes of weight 2 cuspidal newforms at larger levels than currently present in [38]. Proving an analog of Theorem 1.4 for larger k is also certainly possible via the techniques described herein; to some degree, at this stage, the problem is primarily a matter of combinatorics.

10. Acknowledgements

The authors are grateful to Professor Á. Pintér and Dr. S. Tengely for their valuable remarks, to Dr. R. Ferguson for his assistance in carrying out the various computations described herein, and to an anonymous referee whose comments helped to simplify our arguments in Section 4.3, while pointing out various other inaccuracies.

References

[1] M.A. Bennett and C. Skinner, Ternary Diophantine equations via Galois representations and modular forms, *Canad. J. Math.*, 56 (2004), no. 1, 23–54.

[2] W. Bosma, J. Cannon, et al., *Magma* computer algebra system, available from the website from `http://magma.maths.usyd.edu.au/`, 2005.

[3] N. Bruin, Chabauty methods and covering techniques applied to generalised Fermat equations, CWI Tract 133, 77 pages, 2002

[4] N. Bruin, Chabauty methods using elliptic curves, *J. Reine Angew. Math.*, 562 (2003), 27–49.

[5] N. Bruin and E. V. Flynn, Towers of 2-covers of hyperelliptic curves, *Trans. Amer. Math. Soc.*, to appear.
[6] N. Bruin, Transcript of computations, available from the website `http://www.cecm.sfu.ca/~bruin/CubesInAP`, 2005.
[7] J.W.S. Cassels, The Mordell-Weil group of curves of genus 2, Arithmetic and geometry, Vol. I 27–60, Progr. Math. 35, Birkhauser, Boston, Mass. 1983.
[8] J.W.S. Cassels and E.V. Flynn, Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2, LMS–LNS 230, Cambridge University Press, Cambridge, 1996.
[9] J. Cremona, *Algorithms for Modular Elliptic Curves*, Cambridge University Press, 1992.
[10] H. Darmon and A. Granville, On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$, *Bull. L.M.S.* 27 (1995), 513–543.
[11] H. Darmon and L. Merel, Winding quotients and some variants of Fermat's Last Theorem *J. Reine Angew. Math.* 490 (1997), 81–100.
[12] P. Dénes, Über die diophantische Gleichung $x^l + y^l = cz^l$, *Acta Math.* 88 (1952), 241–251.
[13] L. E. Dickson, History of the theory of numbers. Vol. II: Diophantine analysis Chelsea Publishing Co., New York 1966.
[14] P. Erdős and J.L. Selfridge, The product of consecutive integers is never a power, *Illinois J. Math.* 19 (1975), 292–301.
[15] 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 (1997), 435–463.
[16] K. Győry, Über die diophantische Gleichung $x^p + y^p = cz^p$, *Publ. Math. Debrecen* 13 (1966), 301–305.
[17] K. Győry, On the diophantine equation $n(n + 1) \dots (n + k - 1) = bx^l$, *Acta Arith.* 83 (1998), 87–92.
[18] K. Győry, Power values of products of consecutive integers and binomial coefficients, *Number Theory and Its Applications*, Kluwer Acad. Publ. 1999, 145–156.
[19] K. Győry, L. Hajdu and N. Saradha, On the Diophantine equation $n(n + d) \dots (n + (k - 1)d) = by^l$, *Canad. Math. Bull.* 47 (2004), no. 3, 373–388.
[20] G. Hanrot, N. Saradha and T.N. Shorey, Almost perfect powers in consecutive integers, *Acta Arith.* 99 (2001), 13–25.
[21] A. Kraus, Majorations effectives pour l'équation de Fermat généralisée, *Canad. J. Math.* 49 (1997), no. 6, 1139–1161.
[22] A. Kraus, On the equation $x^p + y^q = z^r$: a survey, *Ramanujan J.* 3 (1999), no. 3, 315–333.
[23] R. Marszalek, On the product of consecutive terms of an arithmetic progression, *Monatsh. Math.* 100 (1985), 215–222.
[24] G. Martin, Dimensions of the spaces of cuspforms and newforms on $\Gamma_0(N)$ and $\Gamma_1(N)$, *J. Number Theory*, to appear.
[25] L. Merel, Arithmetic of elliptic curves and Diophantine equations, *J. Théor. Nombres Bordeaux* 11 (1999), 173–200.
[26] R. Obláth, Über das Produkt fünf aufeinander folgender Zahlen in einer arithmetischen Reiche, *Publ. Math. Debrecen* 1 (1950), 222–226.
[27] R. Obláth, Eine Bemerkung über Produkte aufeinander folgender Zahlen, *J. Indian Math. Soc.* 15 (1951), 135–139.
[28] K. Ribet, On the equation $a^p + 2^\alpha b^p + c^p = 0$, *Acta Arith.* 79 (1997), 7–16.
[29] J.B. Rosser and L. Schoenfeld, Approximate formulas for some functions of prime numbers, *Illinois J. Math.* 6 (1962), 64–94.
[30] J.W. Sander, Rational points on a class of superelliptic curves, *J. London Math. Soc.* 59 (1999), 422–434.

[31] N. Saradha, On perfect powers in products with terms from arithmetic progressions, *Acta Arith.* 82 (1997), 147–172.
[32] N. Saradha and T.N. Shorey, Almost perfect powers in arithmetic progression, *Acta Arith.* 99 (2001), 363–388.
[33] N. Saradha and T.N. Shorey, Almost squares in arithmetic progression, *Compositio Math.* 138 (2003), no. 1, 73–111.
[34] L. Schoenfeld, Sharper bounds for the Chebyshev functions $\theta(x)$ and $\psi(x)$ II, *Math. Comp.* 30 (1976), 337–360.
[35] T.N. Shorey, Powers in arithmetic progression, in A Panorama in Number Theory (G. Wüstholz, ed.), Cambridge University Press, Cambridge 2002, 325–336.
[36] T.N. Shorey, Powers in arithmetic progression (II), in New Aspects of Analytic Number Theory, Kyoto 2002, 202–214.
[37] T.N. Shorey and R. Tijdeman, Perfect powers in products of terms in an arithmetic progression, *Compositio Math.* 75 (1990), 307–344.
[38] W. Stein, The Modular forms database, Available from the website `http://modular.fas.harvard.edu/Tables/`, 2005.
[39] M. Stoll, On the height constant for curves of genus two, *Acta Arith.* 90 (1999), 183–201.
[40] M. Stoll, Implementing 2-descent for Jacobians of hyperelliptic curves, *Acta Arith.* 98 (2001), 245–277.
[41] M. Stoll, On the height constant for curves of genus two II, *Acta Arith.* 104 (2002), 165–182.
[42] R. Tijdeman, Diophantine equations and diophantine approximations, in Number Theory and Applications, Kluwer Acad. Press, 1989, 215–243.
[43] A. Wiles, Modular elliptic curves and Fermat's Last Theorem, *Ann. Math* 141 (1995), 443–551.

Department of Mathematics, University of British Columbia, Vancouver, B.C., V6T 1Z2 Canada
E-mail address: `bennett@math.ubc.ca`

Department of Mathematics, Simon Fraser University, Burnaby, BC, V5A 1S6 Canada
E-mail address: `nbruin@sfu.ca`

Number Theory Research Group of the Hungarian Academy of Sciences, Institute of Mathematics, University of Debrecen, P.O. Box 12, 4010 Debrecen, Hungary
E-mail address: `gyory@math.klte.hu`

Number Theory Research Group of the Hungarian Academy of Sciences, Institute of Mathematics, University of Debrecen, P.O. Box 12, 4010 Debrecen, Hungary
E-mail address: `hajdul@math.klte.hu`

I.4 [HTT09]: Cubes in products of terms in arithmetic progression

Publ. Math. Debrecen **74** (2009), 215–232.

CUBES IN PRODUCTS OF TERMS IN ARITHMETIC PROGRESSION

L. HAJDU, SZ. TENGELY, R. TIJDEMAN

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.

1. Introduction

In this paper we consider the problem of almost cubes in arithmetic progressions. This problem is closely related to the Diophantine equation

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

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], [28], [29], [31], [32], [33], [34], [35], [36], [37], [38], [40], [41], the references given there, and the other papers mentioned in the introduction.

In this paper we concentrate on results where all solutions of (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 (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 (1) has no solutions with $b = d = 1$.

2000 *Mathematics Subject Classification.* 11D41, 11D25, 11B25.

Key words and phrases. Perfect cubes, arithmetic progressions.

L. Hajdu is supported in part by the Hungarian Academy of Sciences and by the OTKA grants T48791 and K67580. Sz. Tengely is supported in part the Hungarian Academy of Sciences, by the Magyary Zoltán Higher Educational Public Foundation, and by the OTKA grant T48791.

Saradha and Shorey [27] proved that (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 (1) with $3 \leq k < 110$ for $b = 1$. Combining their result with those of Tengely [39] all solutions of (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 (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 (1) has no solutions with $P(y) > k$. For general d, Győry [13] showed that equation (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 (1) with $l = 3$. We solve equation (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.

2. Notation and results

As we are interested in cubes in arithmetic progressions, we take $l = 3$ in (1). That is, we consider the Diophantine equation

$$n(n+d)\dots(n+(k-1)d) = by^3 \tag{2}$$

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

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

with $P(a_i) \leq k$, a_i is cube-free. Note that (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 2.1. *Suppose that (n, d, k, y) is a solution to equation (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 2.1 from the following theorem.

Theorem 2.2. *Suppose that (n, d, k, b, y) is a solution to equation (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:

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

Note that the above statement follows from Theorem 1.1 of Bennett, Bruin, Győry, Hajdu [1] in case $k < 12$ and $P(b) \le P_k$ with $P_3 = 2$, $P_4 = P_5 = 3$, $P_6 = P_7 = P_8 = P_9 = P_{10} = P_{11} = 5$.

3. Lemmas and auxiliary results

We need some results of Selmer [30] on cubic equations.

Lemma 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 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 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 $(1, 1)$. □

4. Proofs

In this section we provide the proofs of our results. As Theorem 2.1 follows from Theorem 2.2 by a simple inductive argument, first we give the proof of the latter result.

Proof of Theorem 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 $k \leq 13$ $P(a_0 a_1 \dots a_{p_k - 1}) \leq p_k$ holds, and for $k > 13$ we have $P(a_0 a_1 \dots a_{p_k}) < p_k + 1$. 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 $5 \mid a_2 a_3$. 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 (2) we get all solutions by Lemma 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 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

$$x_0^3 + x_2^3 = 9x_1^3 \text{ and } x_0^3 - 2x_2^3 = -6x_4^3. \tag{4}$$

Factorizing the first equation of (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 (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 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

$$x_1^3 + 8x_6^3 = 9x_5^3 \text{ and } x_6^3 - 3x_1^3 = -2x_0^3. \tag{5}$$

Factorizing the first equation of (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 (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

$$(x_6 - \beta x_1)(4x_6^2 - 2x_1x_6 + x_1^2) = (-3\beta + 3)z^3$$

for some $z \in O_L$. We divide both sides of this equation by x_1^3 and apply Lemma 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 (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 $0 \leq h < 11$.

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

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

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 $a_{i_1}, \dots, a_{i_t}$ be the coefficients in (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 $v_i \overset{c}{\equiv} r + i \pmod 9$ ($i = 0, 1, \dots, k-1$). For $l = 1, 2, 3$ put

$$C_l = \{i \ :\ (u_i, v_i) \in E_l,\ i = 0, 1, \dots, k-1\}.$$

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 $p < k$, $p \ne 2, 3, 7$. 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

$$U_t = \{i \ :\ a_i = \pm 2^t,\ i \in \{0, 1, \dots, k-1\}\}$$

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 $5 \stackrel{c}{\equiv} 1 \pmod{13}$. If $i, j \in U_t$ for some $t \in \{0, 1, 2, 3\}$, then $i - i_0 \stackrel{c}{\equiv} j - i_0 \pmod{13}$. If $i \in U_{t_1}$, $j \in U_{t_2}$ with $0 \le t_1 < t_2 \le 2$, then $i - i_0 \stackrel{c}{\not\equiv} j - i_0 \pmod{13}$. 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

$$t \stackrel{c}{\equiv} n + id \stackrel{c}{\equiv} (r + i)d \stackrel{c}{\equiv} td \pmod{7}$$

implies that $d \stackrel{c}{\equiv} 1 \pmod{7}$. 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 $p \stackrel{c}{\equiv} 2, 3, 4, 5 \pmod{7}$, 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 $d \stackrel{c}{\equiv} 1 \pmod{7}$ immediately implies $\gamma = 0$. Further, if $7 \mid n$ and $a_2 = \pm 13^\gamma$ with $\gamma \in \{0, 1, 2\}$, then $d \stackrel{c}{\equiv} 1 \pmod{7}$ 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 $d \stackrel{c}{\equiv} 1 \pmod{7}$. 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

$$m_5 \le 3, \ m_{11} \le 2, \ m_{13} \le 2, \ m_{17} \le 1, \ m_{19} \le 1, \ m_{23} \le 1.$$

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 $P(a_4 a_7 a_{10}) \le 2$. 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 3.1 to the identity $n + (n + 10d) = 2(n + 5d)$ we get all the solutions of (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 3.2 at most four numbers among $a_1, a_3, \dots, a_{13}$ can be equal to ± 1. Moreover, $\gcd(n, d) = 1$ implies that $15 \mid a_i$ can be valid for at most one $i \in \{0, 1, \dots, k-1\}$. 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 3.2 a simple calculation yields that the cubic residues of $a_1, a_3, \dots, a_{13}$ 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 $a_1, a_3, \dots, a_{13}$ there are at most two multiples of 5 and one multiple of 7, 11 and 13 each. Lemma 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 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 $P(a_0 a_2 \dots a_{12}) \le 7$ (or $P(a_2 a_4 \dots a_{14}) \le 7$), 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 $a_1, a_3, \dots, a_{17}$ 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 $a_1, a_3, \dots, a_{17}$ 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 $a_1, a_3, \dots, a_{17}$. However, by Lemma 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 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 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 (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 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 $a_1, a_3, \dots, a_{19}$ equal ± 1. However, then there are three such coefficients which belong to an arithmetic progression. Thus by Lemma 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 $a_1, a_3, \dots, a_{19}$ 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 $a_1, a_3, \dots, a_{19}$ 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 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 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 $P(a_6 a_8 \ldots a_{18}) \leq 7$ 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 $a_1, a_3, \ldots, a_{23}$ 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 $a_1, a_3, \ldots, a_{23}$ 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 $a_1, a_3, \ldots, a_{23}$ are $\overset{c}{\equiv} 1 \pmod{13}$. Hence, by Lemma 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 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 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 3.2.

Finally, assume that $3 \mid d$, and $\gcd(7 \cdot 13, d) = 1$. Then among $a_1, a_3, \dots, a_{23}$ 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 3.2 we get that exactly four of the coefficients $a_1, a_3, \dots, a_{23}$ 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 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 $P(a_4 a_9 a_{14}) \le 2$, 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 $a_1, a_3, \dots, a_{29}$ 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 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 $a_1, a_3, \dots, a_{29}$ are equal to ± 1. Hence there are three such coefficients in arithmetic progression, and the statement follows from Lemma 3.1.

Assume next that $13 \mid d$, but $7 \nmid d$. Then among the odd coefficients $a_1, a_3, \dots, a_{29}$ 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 $a_1, a_3, \dots, a_{29}$ 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 $a_1, a_3, \dots, a_{29}$ 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 2.2. □

Proof of Theorem 2.1. Obviously, for $k < 32$ the statement is an immediate consequence of Theorem 2.2. Further, observe that $b = 1$ implies that for any k with $31 < k < 39$, one can find j with $0 \le j \le k - 30$ such that $P(a_j a_{j+1} \dots a_{j+29}) \le 29$. Hence the statement follows from Theorem 2.2. □

Acknowledgement. The authors are grateful to the referee for the useful remarks.

References

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

[2] W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), 235–265.

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

[4] N. Bruin, *Chabauty methods and covering techniques applied to generalized Fermat equations*, CWI Tract, Vol. 133, Stichting Mathematisch Centrum, Centrum voor Wiskunde en Informatica, Amsterdam, 2002.
[5] N. Bruin, *Chabauty methods using elliptic curves*, J. Reine Angew. Math. **562** (2003), 27–49.
[6] H. Darmon, L. Merel, *Winding quotients and some variants of Fermat's Last Theorem*, J. Reine Angew. Math. **490** (1997), 81–100.
[7] L. E. Dickson, *History of the theory of numbers. Vol. II: Diophantine analysis*, Chelsea Publishing Co., New York 1966, xxv+803 pp.
[8] P. Erdős, *Note on products of consecutive integers (II)*, J. London Math. Soc. **14** (1939), 194–198.
[9] P. Erdős, J. L. Selfridge, *The product of consecutive integers is never a power*, Illinois J. Math. **19** (1975), 292–301.
[10] P. Filakovszky, L. Hajdu, *The resolution of the equation* $x(x+d)\dots(x+(k-1)d) = by^2$ *for fixed* d, Acta Arith. **98** (2001), 151–154.
[11] K. Győry, *On the diophantine equation* $\binom{n}{k} = x^l$, Acta Arith. **80** (1997), 289–295.
[12] K. Győry, *On the diophantine equation* $n(n+1)\dots(n+k-1) = bx^l$, Acta Arith. **83** (1998), 87–92.
[13] K. Győry, *Power values of products of consecutive integers and binomial coefficients*, Number Theory and Its Applications (S. Kanemitsu and K. Győry, eds.), Kluwer Acad. Publ. 1999, pp. 145–156.
[14] K. Győry, *Perfect powers in products with consecutive terms from arithmetic progressions*, More Sets, Graphs and Numbers (E. Győri, G. O. H Katona, L. Lovász, eds.), Bolyai Society Mathematical Studies **15** (2006), pp. 143-155.
[15] K. Győry, L. Hajdu, N. Saradha, *On the Diophantine equation* $n(n+d)\dots(n+(k-1)d) = by^l$, Canad. Math. Bull. **47** (2004), 373–388; **48** (2005), 636.
[16] G. Hanrot, N. Saradha, T. N. Shorey, *Almost perfect powers in consecutive integers*, Acta Arith. **99** (2001), 13–25.
[17] N. Hirata-Kohno, S. Laishram, T. N. Shorey, R. Tijdeman, *An extension of a theorem of Euler*, Acta Arith. **129** (2007), 71–102.
[18] S. Laishram, *An estimate for the length of an arithmetic progression the product of whose terms is almost square*, Publ. Math. Debrecen **68** (2006), 451–475.
[19] S. Laishram, T. N. Shorey, *The equation* $n(n+d)\dots(n+(k-1)d) = by^2$ *with* $\omega(d) \le 6$ *or* $d \le 10^{10}$, Acta Arith. **129** (2007), 249–305.
[20] R. Marszalek, *On the product of consecutive terms of an arithmetic progression*, Monatsh. Math. **100** (1985), 215–222.
[21] R. Obláth, *Über das Produkt fünf aufeinander folgender Zahlen in einer arithmetischer Reihe*, Publ. Math. Debrecen **1** (1950), 222–226.
[22] O. Rigge, *Über ein diophantisches Problem*, 9th Congress Math. Scand., Helsingfors 1938, Mercator 1939, pp. 155–160.
[23] J. W. Sander, *Rational points on a class of superelliptic curves*, J. London Math. Soc. **59** (1999), 422–434.
[24] N. Saradha, *On perfect powers in products with terms from arithmetic progressions*, Acta Arith. **82** (1997), 147–172.
[25] N. Saradha, *Squares in products with terms in an arithmetic progression*, Acta Arith. **86** (1998), 27–43.
[26] N. Saradha, T. N. Shorey, *Almost perfect powers in arithmetic progression*, Acta Arith. **99** (2001), 363–388.
[27] N. Saradha, T. N. Shorey, *Almost Squares in Arithmetic Progression*, Compositio Math. **138** (2003), 73–111.

[28] N. Saradha, T. N. Shorey, *Almost Squares and Factorisations in Consecutive Integers*, Compositio Math. **138** (2003), 113-124.
[29] N. Saradha, T. N. Shorey, *Contributions towards a conjecture of Erdős on perfect powers in arithmetic progressions*, Compositio Math. **141** (2005), 541-560.
[30] E. Selmer, *The diophantine equation* $ax^3 + by^3 + cz^3 = 0$, Acta Math. **85** (1951), 205–362.
[31] T. N. Shorey, *Perfect powers in products of arithmetical progressions with fixed initial term*, Indag. Math. N.S. **7** (1996), 521–525.
[32] T. N. Shorey, *Powers in arithmetic progression*, A Panorama in Number Theory (G. Wüstholz, ed.), Cambridge University Press 2002, pp. 325–336.
[33] T. N. Shorey, *Powers in arithmetic progression (II)*, New Aspects of Analytic Number Theory, Kyoto 2002, pp. 202–214.
[34] T. N. Shorey, *Diophantine approximations, Diophantine equations, Transcendence and Applications*, Indian Jour. of Pure and Applied Math. **37** (2006), 9-39.
[35] T. N. Shorey, R. Tijdeman, *Perfect powers in products of terms in an arithmetic progression*, Compositio Math. **75** (1990), 307–344.
[36] T. N. Shorey, R. Tijdeman, *Perfect powers in products of terms in an arithmetic progression II*, Compositio Math. **82** (1992), 119–136.
[37] T. N. Shorey, R. Tijdeman, *Perfect powers in products of terms in an arithmetic progression III*, Acta Arith. **61** (1992), 391–398.
[38] T. N. Shorey, R. Tijdeman, *Some methods of Erdős applied to finite arithmetic progressions integers and related equations*, The Mathematics of Paul Erdős I, Springer 1997, pp. 251–267.
[39] Sz. Tengely, *Note on the paper "An extension of a theorem of Euler" by Hirata-Kohno et. al*, Acta Arith. **134** (2008), 329–335.
[40] R. Tijdeman, *Diophantine equations and diophantine approximations*, Number Theory and Applications, Kluwer Acad. Press 1989, 215–243.
[41] R. Tijdeman, *Exponential diophantine equations 1986-1996*, Number Theory: Diophantine, Computational and Algebraic Aspects (K. Győry, A. Pethő and V. T. Sós, eds.), Walter de Gruyter, Berlin–New York 1998, pp. 523–540.

Lajos Hajdu
Institute of Mathematics
University of Debrecen
and the Number Theory Research Group
of the Hungarian Academy of Sciences
P.O.Box 12
4010 Debrecen
Hungary
E-mail address: hajdul@math.klte.hu

Szabolcs Tengely
Institute of Mathematics
University of Debrecen
and the Number Theory Research Group
of the Hungarian Academy of Sciences
P.O.Box 12
4010 Debrecen
Hungary
E-mail address: tengely@math.klte.hu

Robert Tijdeman
Mathematical Institute
Leiden University
P.O.Box 9512
2300 RA Leiden
The Netherlands
E-mail address: tijdeman@math.leidenuniv.nl

II. Számtani sorozatot alkotó vegyes hatványok

II.1 [H04]: Perfect powers in arithmetic progression.

A note on the inhomogeneous case

Acta Arith. **113** (2004), 343–349.

PERFECT POWERS IN ARITHMETIC PROGRESSION. A NOTE ON THE INHOMOGENEOUS CASE

L. Hajdu[1]

Dedicated to Professor R. Tijdeman on the occasion of his sixtieth birthday

Abstract. We show that the *abc* conjecture implies that the number of terms of any arithmetic progression consisting of almost perfect "inhomogeneous" powers is bounded, moreover, if the exponents of the powers are all ≥ 4, then the number of such progressions is finite. We derive a similar statement unconditionally, provided that the exponents of the terms in the progression are bounded from above.

1. Introduction

Arithmetic progressions consisting of almost perfect powers are widely investigated in the "homogeneous" case. That is, one is interested in arithmetic progressions of the shape

$$a_0x_0^l, \ldots, a_{k-1}x_{k-1}^l \quad \text{with} \quad a_i, x_i \in \mathbb{Z} \ \ (0 \leq i \leq k-1),$$

with some fixed integer $l \geq 2$, such that the coefficients a_i are "restricted" in some sense. It was already known by Fermat and proved by Euler (see [D] pp. 440 and 635) that four distinct squares cannot form an arithmetic progression. The contributions of Darmon and Merel [DM] on the Fermat equation imply that there are no three l-th powers with $l \geq 3$ in arithmetic progression, up to the trivial cases. In this paper we take up the problem when the arithmetic progression consists of almost perfect "inhomogeneous" powers. Let $S = \{p_1, \ldots, p_s\}$ be any set of positive primes with $p_1 < \ldots < p_s$, and write $\mathbb{Z}_S$ for the set of those non-zero integers whose prime divisors belong to S. Put

$$H = \{\eta x^l \mid \eta \in \mathbb{Z}_S, \ x, l \in \mathbb{Z} \text{ with } x \neq 0 \text{ and } l \geq 2\},$$

and note that $\pm 1 \in H$, but $0 \notin H$. To guarantee that the representation of every element $h \in H$ is unique, we further assume that for $h = \eta x^l$ we have that η is l-th power free, $x > 0$, and $l = 2$ if $h \in \mathbb{Z}_S$. In particular, if $x = 1$ then η is square-free. The main purpose of this paper is to show that the *abc* conjecture implies that the number of terms of any "coprime" arithmetic progression in H is bounded by a

2000 *Mathematics Subject Classification:* 11D41.

[1]Research supported in part by the Netherlands Organization for Scientific Research (NWO), by grants T42985 and F34981 of the Hungarian National Foundation for Scientific Research, and by the FKFP grant 3272-13/066/2001.

constant $c(s,P)$ depending only on $s=|S|$ and $P=p_s$. Moreover, the number of such progressions having at least three terms, where the exponents of the powers are ≥ 4, is finite. We derive a similar statement unconditionally, provided that the exponents of the terms in the progression are bounded from above. Our main tools, besides the *abc* conjecture, will be a theorem of Euler on equation (1) below with $l=2$, the above mentioned result of Darmon and Merel on Fermat-type ternary equations, and a famous theorem of van der Waerden from Ramsey theory, about arithmetic progressions.

Finally, we mention that our problem is related to the equation

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

in non-zero integers n,d,b,y, $k\geq 2$, $l\geq 2$ with $\gcd(n,d)=1$, $P(b)\leq k$, where for any integer u with $|u|>1$ we write $P(u)$ for the greatest prime factor of u and we put $P(\pm 1)=1$. It is easy to show that using (1) one can write

$$n+id=a_ix_i^l \quad \text{with} \quad P(a_i)\leq k-1 \quad (0\leq i\leq k-1). \tag{2}$$

Equation (1) and its various specializations have a very extensive literature. For related results we just refer to the survey papers and recent articles [BGyH], [Gy], [GyHS], [SS], [S1], [S2], [S3], [T1], [T2], and the references given there. We only mention two particular theorems about (1), which are relevant from our viewpoint. Shorey (see [S1]) proved that the *abc* conjecture implies that with $l\geq 4$, k is bounded by an absolute constant in (1). Extending this result, Győry, Hajdu and Saradha [GyHS] deduced from the *abc* conjecture that with $l\geq 4$ and $k\geq 3$, equation (1) has only finitely many solutions. Thus our theorems yield a kind of extension of the above mentioned results of Shorey [S1] and Győry, Hajdu and Saradha [GyHS], to the inhomogeneous case. However, it is important to note that as in (2) $P(a_i)\leq k-1$, and we fix the prime divisors of the l-th power free part of $h\in H$ in advance, the results obtained here do not imply the corresponding theorems in [S1] and [GyHS].

2. Main results

In what follows, $c_0,\dots,c_{15}$ will denote constants depending only on s and P. Though $s\leq P$, our arguments will be more clear if we indicate the dependence also upon s. By a non-constant arithmetic progression we will simply mean a progression with non-zero common difference.

Theorem 1. *Suppose that the abc conjecture is valid. Let $h_0,\dots,h_{k-1}$ be any non-constant arithmetic progression in H, with $h_i=\eta_i x_i^{l_i}$ $(0\leq i\leq k-1)$, such that $gcd(h_0,h_1)\leq c_0$ for some c_0. Then we have $\max(k,l)<c_1$, where $l=\max\limits_{0\leq i\leq k-1} l_i$. Moreover, the number of such progressions with $k\geq 3$ and $l_i\geq 4$, is bounded by some c_2.*

Remark 1. Looking at the proof of Theorem 1 closely, one can easily see that the second part of the statement can be extended as follows. Consider progressions $h_0,\dots,h_{k-1}$ as above, such that $k\geq 3$ and for every $i\in\{0,\dots,k-1\}$ there exist $j,t\in\{0,\dots,k-1\}\setminus\{i\}$ with $j\neq t$ and $1/l_i+1/l_j+1/l_t<1$. Then the *abc* conjecture implies that the number of such progressions is bounded by some c_2.

Remark 2. The condition $\gcd(h_0, h_1) \leq c_0$ in Theorem 1 is necessary. Indeed, there exist non-constant arithmetic progressions in H consisting of non-zero perfect powers, having arbitrarily many terms. To see this, observe that each pair of distinct positive perfect powers can be considered as a non-constant arithmetic progression of two terms. Suppose that for some $i \geq 2$, $h_0, \ldots, h_{i-1}$ is such a progression of positive perfect powers, say $h_j = x_j^{l_j}$ with $x_j \geq 1$ and $l_j \geq 2$ $(0 \leq j \leq i-1)$. Let $t = 2h_{i-1} - h_{i-2}$ and $l_i' = \prod_{j=0}^{i-1} l_j$, and write

$$h_j' = t^{l_i'} h_j \quad \text{for} \quad 0 \leq j \leq i-1, \quad \text{and} \quad h_i' = t^{l_i'+1}.$$

In this way we obtain a non-constant arithmetic progression $h_0', \ldots, h_{i-1}', h_i'$ consisting of positive perfect powers, having exponents $l_0, \ldots, l_{i-1}, l_i = l_i' + 1$. This verifies our claim, which shows that the assumption $\gcd(h_0, h_1) \leq c_0$ cannot be omitted.

If we drop the *abc* conjecture, we need a further assumption to get a finiteness statement for the number of terms in our arithmetic progressions.

Theorem 2. *Let l be a fixed integer with $l \geq 2$. Then for any non-constant arithmetic progression $h_0, \ldots, h_{k-1}$ in H such that $l_i \leq l$ in the representation $h_i = \eta_i x_i^{l_i}$ $(0 \leq i \leq k-1)$, we have $k \leq C_0(s, P, l)$, where $C_0(s, P, l)$ is a constant depending only on s, P and l.*

Remark 3. Note that in Theorem 2 we do not need the assumption $\gcd(h_0, h_1) \leq c_0$. However, the example in Remark 2 shows that the condition $l_i \leq l$ $(0 \leq i \leq k-1)$ is necessary in this case.

Finally, we propose the following

Conjecture. Theorem 1 is true unconditionally, i.e. independently of the *abc* conjecture.

3. Some lemmas

To prove our theorems, we need several lemmas. The first one concerns almost perfect squares in arithmetic progression.

Lemma 1. *The product of four consecutive terms in a non-constant positive arithmetic progression is never a square.*

Proof. This is a classical result of Euler (cf. [M], p. 21). □

Our next lemma is about Fermat-type ternary equations.

Lemma 2. *Let $l \geq 3$ be an integer. Then the equation*

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

has no solution in coprime non-zero integers X, Y, Z with $XYZ \neq \pm 1$.

Proof. This was proved by Darmon and Merel [DM]. □

The next lemma is from Ramsey theory, concerning arithmetic progressions.

Lemma 3. *For every positive integers u and v there exists a positive integer w such that for any coloring of the set $\{1,\dots,w\}$ using u colors, we get a non-constant monochromatic arithmetic progression, having at least v terms.*

Proof. This nice result is due to van der Waerden (cf. [vdW]). □

The next statement takes care of Theorem 1 unconditionally, in case of homogeneous powers.

Lemma 4. *Let l be a fixed integer with $l \geq 2$. Suppose that $h_0,\dots,h_{k-1}$ is an arithmetic progression in H, such that $h_i = \eta_i x_i^l$, for all $i = 0,\dots,k-1$. Then $k < C_1(s,P,l)$, where $C_1(s,P,l)$ is a constant depending only on s, P and l.*

Proof. Color the terms of the arithmetic progression $h_0,\dots,h_{k-1}$ in such a way that h_i and h_j have the same color if and only if $\eta_i = \eta_j$ $(0 \leq i,j \leq k-1)$. As η_i and η_j are l-th power free, at most $2l^s$ colors are necessary. (We need the factor 2 because of the signs.)

Assume first that $l = 2$. We apply Lemma 3 with $(u,v) = (2^{s+1},4)$ to conclude that if $k \geq w$ with some $w = w(s)$, then there exist indices $0 \leq i_1 < i_2 < i_3 < i_4 \leq k-1$ such that $h_{i_1}, h_{i_2}, h_{i_3}, h_{i_4}$ is a non-constant arithmetic progression of non-zero integers, with $\eta_{i_1} = \eta_{i_2} = \eta_{i_3} = \eta_{i_4}$. Then we have

$$h_{i_1}h_{i_2}h_{i_3}h_{i_4} = (\eta_{i_1}^2 x_{i_1}x_{i_2}x_{i_3}x_{i_4})^2.$$

However, by Lemma 1, this is impossible. (Note that it does not make a difference whether η_{i_1} is positive or negative.) This gives a contradiction, whence $k < w$, and the lemma follows when $l = 2$.

Suppose now that $l \geq 3$. We apply again Lemma 3, this time with $(u,v) = (2l^s,3)$ to derive that if $k \geq w$ with some $w = w(s,l)$, then there exist indices $0 \leq i_1 < i_2 < i_3 \leq k-1$ such that $h_{i_1}, h_{i_2}, h_{i_3}$ is an arithmetic progression, with $\eta_{i_1} = \eta_{i_2} = \eta_{i_3}$. Hence we obtain

$$x_{i_1}^l + x_{i_3}^l = 2x_{i_2}^l. \tag{3}$$

By Lemma 2, as $h_{i_j} \neq 0$ $(j = 1,\dots,3)$ and our progression is non-constant, we deduce that (3) is impossible. Thus we get a contradiction, whence $k < w$, and the lemma is proved. □

Remark 4. Note that assuming the *abc* conjecture, this lemma follows from the afore mentioned result of Shorey [S1], in the case when $\gcd(h_0,h_1) = 1$.

Lemma 5. *Suppose that the abc conjecture is valid, and let $c_3 = C_1(s,P,2)$ be the constant given in Lemma 4, corresponding to the exponent $l = 2$. Then there exists a c_4 such that if $h_0,\dots,h_{k-1}$ is any arithmetic progression in H with $h_i = \eta_i x_i^{l_i}$, such that $gcd(h_0,h_1) < c_5$ and $k \geq 2c_3$, then $l_i < c_4$ holds for all $i = 0,\dots,k-1$.*

Proof. Suppose that we have an arithmetic progression $h_0,\dots,h_{k-1}$ as above, and take any $i \in \{0,\dots,k-1\}$ with $l_i \geq 7$. (If no such i exists, then the lemma follows with $c_4 = 7$.) Note that $x_i > 1$. By Lemma 4 we infer that there exists a j with $0 < |i-j| \leq c_3$ such that $l_j \geq 3$. Choose any $t \in \{0,\dots,k-1\}\setminus\{i,j\}$ with $|i-t| \leq 2$. Then with some coprime non-zero integers $\lambda_i,\lambda_j,\lambda_t$ with $\max(\lambda_i,\lambda_j,\lambda_t) \leq |i-j|+2$ we have $\lambda_i h_i + \lambda_j h_j + \lambda_t h_t = 0$. This gives

$$\lambda_i\eta_i x_i^{l_i} + \lambda_j\eta_j x_j^{l_j} + \lambda_t\eta_t x_t^{l_t} = 0. \tag{4}$$

Let D denote the gcd of the above three terms, and observe that as $\gcd(h_0, h_1) \le c_5$, we have $D < c_6$.

We show that the *abc* conjecture implies that l_i is bounded. Note that when $D = 1$, and the coefficients of $x_i^{l_i}, x_j^{l_j}, x_t^{l_t}$ are fixed, by a similar argument Tijdeman derived from the *abc* conjecture that (4) has only finitely many solutions (see [T1], p. 234). Let $r \in \{i, j, t\}$ be the index for which $|\lambda_r \eta_r x_r^{l_r}|$ is maximal among these three terms. The (effective version of) the *abc* conjecture, with $\varepsilon = 1/42$ gives

$$|\lambda_r \eta_r x_r^{l_r}| < c_7 \left(\prod_{p | x_i x_j x_t} p \right)^{43/42}.$$

As $l_i \ge 7$, $l_j \ge 3$, and $l_t \ge 2$, whence $1/l_i + 1/l_j + 1/l_t < 1 - 1/42$, this yields

$$|\lambda_r \eta_r x_r^{l_r}| \le c_8 x_r^{(1763/1764) l_r}.$$

If $x_r = 1$ (implying that $r = t$, $l_r = 2$, and η_r is square-free), then by

$$x_i^{l_i} < |\lambda_i \eta_i x_i^{l_i}| \le |\lambda_r \eta_r x_r^{l_r}| \tag{5}$$

and $x_i > 1$, we get $l_i < c_9$. Otherwise, $x_r > 1$ gives $l_r < c_{10}$, whence $|\lambda_r \eta_r x_r^{l_r}| < c_{11}$. Thus using again (5) and $x_i > 1$, we obtain $l_i < c_{12}$ also in this case. As i was taken arbitrarily with $l_i \ge 7$, the statement follows with $c_4 = \max(7, c_9, c_{12})$. □

4. Proofs of the theorems

Now we are ready to prove our main results. We start with the proof of Theorem 2, because it is more convenient to do so.

Proof of Theorem 2. Let $C_2(s, P, l)$ be the maximum of the values $C_1(s, P, L)$ defined in Lemma 4, where L ranges through the interval $[2, l]$. Apply Lemma 3 to our progression with $(u, v) = (l-1, C_2(s, P, l))$. (The terms having the same exponents, have the same colors.) Thus Lemma 3 gives some constant $C_0(s, P, l)$, depending only on s, P and l, such that $k \ge C_0(s, P, l)$ would be a contradiction by Lemma 4. Thus $k < C_0(s, P, l)$, and the theorem follows. □

Proof of Theorem 1. We may suppose that $k \ge 2c_3$, where $c_3 \ge 2$ is given in Lemma 5. Then by Lemma 5 we have that $l_i \le c_4$, for all $i = 0, \dots, k-1$. Thus the first part of the theorem follows from Theorem 2, with $c_1 = \max(c_4, C_0(s, P, c_4))$.

To prove the second part, suppose that $l_i \ge 4$ for all $i = 0, \dots, k-1$. We already now that $\max(k, l) < c_1$. Fix k and choose any different $i, j, t \in \{0, \dots, k-1\}$. Just as in the proof of Lemma 5, we get an equation of the form

$$\lambda_i \eta_i x_i^{l_i} + \lambda_j \eta_j x_j^{l_j} + \lambda_t \eta_t x_t^{l_t} = 0$$

with some integers $\lambda_i, \lambda_j, \lambda_t$, such that $\max(|\lambda_i|, |\lambda_j|, |\lambda_t|) < k < c_1$. Moreover, the gcd of the three terms on the left hand side is bounded by some c_{13}. Following the argument of Lemma 5, as x_i, x_j, x_t are all > 1, and $1/l_i + 1/l_j + 1/l_t \le 3/4$, using the *abc* conjecture we derive that $\max(x_i^{l_i}, x_j^{l_j}, x_t^{l_t}) < c_{14}$. As also $\max(|\eta_i|, |\eta_j|, |\eta_t|) < c_{15}$, the theorem follows. □

5. Acknowledgement

The author is grateful to Cs. Sándor for his motivating question, and to the referee for his helpful and useful remarks.

References

[BGyH] M. A. Bennett, K. Győry and L. Hajdu, *Powers from products of consecutive terms in arithmetic progression*, J. reine Angew. Math., submitted.

[DM] H. Darmon and L. Merel, *Winding quotients and some variants of Fermat's Last Theorem*, J. Reine Angew. Math. **490** (1997), 81–100.

[D] L. E. Dickson, *History of the theory of numbers. Vol. II: Diophantine analysis*, Chelsea Publishing Co., New York, 1966, pp. xxv+803.

[Gy] K. Győry, *Power values of products of consecutive integers and binomial coefficients*, Number Theory and Its Applications, Kluwer Acad. Publ., 1999, pp. 145–156.

[GyHS] K. Győry, L. Hajdu and N. Saradha, *On the diophantine equation* $n(n+d)\dots(n+(k-1)d) = by^l$, Canad. Math. J. (to appear).

[M] L. J. Mordell, *Diophantine Equations*, Academic Press, London and New York, 1969.

[SS] N. Saradha and T. N. Shorey, *Contributions towards a conjecture of Erdős on perfect powers in arithmetic progression*, J. reine Angew. Math., submitted.

[S1] T. N. Shorey, *Exponential diophantine equations involving products of consecutive integers and related equations*, Number Theory (R. P. Bambah, V. C. Dumir and R. J. Hans-Gill, eds.), Hindustan Book Agency, 1999, pp. 463–495.

[S2] T. N. Shorey, *Powers in arithmetic progression*, A Panorama in Number Theory (G. Wüstholz, ed.), Cambridge University Press, Cambridge, 2002, pp. 325–336.

[S3] T. N. Shorey, *Powers in arithmetic progression (II)*, New Aspects of Analytic Number Theory, Kyoto, 2002, pp. 202–214.

[T1] R. Tijdeman, *Diophantine equations and diophantine approximations*, Number Theory and Applications (R. A. Mollin, ed.), Kluwer Acad. Press, 1989, pp. 215–243.

[T2] R. Tijdeman, *Exponential diophantine equations 1986–1996*, Number Theory, Walter de Gruyter, 1998, pp. 523–539.

[vdW] B. L. van der Waerden, *Beweis einer Baudetschen Vermutung*, Nieuw Archief voor Wiskunde **19** (1927), 212–216.

L. Hajdu
Number Theory Research Group
of the Hungarian Academy of Sciences, and
Institute of Mathematics
University of Debrecen
P.O. Box 12
4010 Debrecen
Hungary

E-mail address:
hajdul@math.klte.hu

II.2 [BGyHT06]: Arithmetic progressions consisting of unlike powers

Indag. Math. **17** (2006), 539–555.

ARITHMETIC PROGRESSIONS CONSISTING OF UNLIKE POWERS

N. Bruin[1], K. Győry[2], L. Hajdu[3] and Sz. Tengely[4]

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 $(x_0^{l_0}, x_1^{l_1}, \dots, x_{k-1}^{l_{k-1}})$ with $x_i \in \mathbb{Z}$, $\gcd(x_0, x_1) = 1$ and $2 \leq l_i \leq L$ for $i = 0, 1, \dots, k-1$. Furthermore, we show that, for $L = 3$, the progression $(1, 1, \dots, 1)$ is the only such progression up to sign. Our proofs involve some well-known theorems of Faltings [F], Darmon and Granville [DG] as well as Chabauty's method applied to superelliptic curves.

1. Introduction

By a classical result of Euler, which apparently was already known to Fermat (see [D] pp. 440 and 635), four distinct squares cannot form an arithmetic progression. Darmon and Merel [DM] 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. [T], [Sh] and [BBGyH] 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*

$$(h_0, h_1, \dots, h_{k-1})$$

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,

2000 Mathematics Subject Classification: 11D41.

[1]Research supported in part by National Science and Engineering Research Council Canada (NSERC).

[2]Research supported in part by grants T42985 and T38225 of the Hungarian National Foundation for Scientific Research (HNFSR).

[3]Research supported in part by grants T42985 and T48791 of the HNFSR and by the János Bolyai Research Fellowship of the Hungarian Academy of Sciences.

[4]Research supported in part by grant T48791 of the HNFSR.

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 [H] the ABC conjecture implies that if

$$(x_0^{l_0}, x_1^{l_1}, \dots, x_{k-1}^{l_{k-1}})$$

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. [M],[DG],[PT],[T1],[T2] 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 [H], we restrict the size of the exponents l_i and prove the following finiteness result:

Theorem 1. *Let $k \geq 4$ and $L \geq 2$. There are only finitely many k-term integral arithmetic progressions $(h_0, h_1, \dots, h_{k-1})$ 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 $i = 0, 1, \dots, k-1$.*

The proof of this theorem uses that for each of the finitely many possible exponent vectors $(l_0, \dots, l_{k-1})$, the primitive arithmetic progressions of the form $(x_0^{l_0}, \dots, x_{k-1}^{l_{k-1}})$ 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 [F], 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 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 $(h_0, h_1, \dots, h_{k-1})$ satisfying the following conditions:*

(i) *For $i = 0, \dots, k-1$, 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 parametrising algebraic curves and, using Chabauty's method, the rational points on them. This allows us to prove:

Theorem 3. *Let $k \geq 4$, and suppose that $(h_0, h_1, \dots, h_{k-1}) = (x_0^{l_0}, x_1^{l_1}, \dots, x_{k-1}^{l_{k-1}})$ is a primitive integral arithmetic progression with $x_i \in \mathbb{Z}$ and $2 \leq l_i \leq 3$ for $i = 0, 1, \dots, k-1$. Then*

$$(h_0, h_1, \dots, h_{k-1}) = \pm(1, 1, \dots, 1).$$

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 [B]. 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 $g(u,v) = u^4 + 4u^3v + 8u^2v^2 - 8uv^3 + 4v^4$.

2. Auxiliary results

The proof of Theorem 2 depends on the following well-known result by Darmon and Granville [DG].

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. [M], p. 21), which was already known by Fermat (see [D] 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 [M] on p. 126. □

The next lemma provides the parametrization of the solutions of certain ternary Diophantine equations.

Lemma. *All solutions of the equations*

$$\text{i) } 2b^2 - a^2 = c^3, \quad \text{ii) } a^2 + b^2 = 2c^3, \quad \text{iii) } a^2 + 2b^2 = 3c^3, \quad \text{iv) } 3b^2 - a^2 = 2c^3,$$

$$\text{v) } 3b^2 - 2a^2 = c^3, \quad \text{vi) } a^2 + b^2 = 2c^2, \quad \text{vii) } 2a^2 + b^2 = 3c^2, \quad \text{viii) } a^2 + 3b^2 = c^2$$

in integers a, b and c with $gcd(a, b, c) = 1$ are given by the following parametrizations:

i) $a = \pm(x^3 + 6xy^2)$, $b = \pm(3x^2y + 2y^3)$ *or* $a = \pm(x^3 + 6x^2y + 6xy^2 + 4y^3)$, $b = \pm(x^3 + 3x^2y + 6xy^2 + 2y^3)$

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

$$a + \sqrt{2}b = (1 + \sqrt{2})^{\alpha}(\sqrt{2})^{\beta}(x + \sqrt{2}y)^3, \tag{1}$$

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 (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 $\gcd(x, y) = 1$. $\square$

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 $2 \le l_i \le L$ leaves only finitely many possibilities for the exponent vector $\underline{l} = (l_0, \dots, l_{k-1})$. 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 $\underline{\eta} = (\eta_0, \dots, \eta_{k-1})$. Hence, we only need to prove the theorem for $k = 3, 4, 5$, and $\underline{l}$ and $\underline{\eta}$ fixed. Note that if $\gcd(h_0, h_1) \le D$, then certainly $\gcd(x_i, x_j) \le D$. 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 $0 \le i < j \le k-1$.
(b) $(x_0, \dots, x_{k-1}) \in \mathbb{Z}^k$ with $\gcd(x_0, x_1) \le D$.

Hence, we need to solve

$$(j-m)\eta_i x_i^{l_i} + (m-i)\eta_j x_j^{l_j} + (i-j)\eta_m x_m^{l_m} = 0 \text{ for all } 0 \le m, i, j \le k-1.$$

For $m = 0, i = 1$, we obtain that each of our solutions would give rise to a solution to

$$j\eta_1 x_1^{l_1} - \eta_j x_j^{l_j} + (1-j)\eta_0 x_0^{l_0} = 0. \tag{3}$$

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 Merel. 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 (3) 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 [notes], where a full transcript of a session using the computer algebra system MAGMA [magma] 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 $\mathcal{J}_{\mathrm{tors}}(\mathbb{Q})$ (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 [St] 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 [C] 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 [CF], [Fl], [FPS], [P].

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

$$x_1^2 = \frac{x_0^3 + x_2^3}{2}, \quad x_3^2 = \frac{-x_0^3 + 3x_2^3}{2}. \tag{4}$$

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 (4) 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 $\mathcal{J}_{\mathrm{tors}}(\mathbb{Q})$ 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

$$x_1^2 = \frac{2x_0^3 + x_3^3}{3}, \quad x_2^2 = \frac{x_0^3 + 2x_3^3}{3}$$

and using that 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, hance 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

$$x_1^4 + dx_1^2 - (x^3 + 6x^2y + 6xy^2 + 4y^3)^2 = 0 \tag{5}$$

or

$$x_1^4 + dx_1^2 - (x^3 + 6xy^2)^2 = 0 \tag{6}$$

follows, respectively. In the first case, the left hand side of (5) 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 torison 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 (6) 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 [CF]). We use part of the 2-coverings of $\mathcal{C}_4$ following [B]. For details, see [notes]. 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

$$\begin{aligned} D_\delta &: \ (Y_1)^2 = \delta R(X) \\ L_\delta &: \ (Y_2)^2 = \delta Q(X) \end{aligned}$$

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

$$(7)\quad f(x,y) := 3x^6 + 18x^5y + 9x^4y^2 - 148x^3y^3 - 27x^2y^4 + 162xy^5 - 81y^6 = 2(\pm 4x_0)^3$$

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 factorisation $f(x,y) = g(x,y)h(x,y)$ 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

$$(-2\alpha^3+13\alpha^2-28\alpha+44)/9,$$
$$(16\alpha^3+52\alpha^2+14\alpha-1)/9,$$
$$(2\alpha^3+3\alpha^2-14\alpha-6)/3$$

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 [B] 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 [notes].

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. $\square$

References

[BBGyH] M. A. Bennett, N. Bruin, K. Győry and L. Hajdu, *Powers from products of consecutive terms in arithmetic progression*, Bull. London Math. Soc. (to appear).

[B] N. Bruin, *Chabauty methods and covering techniques applied to generalized Fermat equations*, CWI Tract, vol. 133, Stichting Mathematisch Centrum, Centrum voor Wiskunde en Informatica, Amsterdam, 2002.

[CF] J. W. S. Cassels and E. V. Flynn, *Prolegomena to a middlebrow arithmetic of curves of genus* 2, vol. 230, Cambridge University Press, Cambridge, 1996, pp. xiv+219.

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

[DG] 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** (1995), 513–543.

[DM] H. Darmon and L. Merel, *Winding quotients and some variants of Fermat's Last Theorem*, J. Reine Angew. Math. **490** (1997), 81–100.

[D] L. E. Dickson, *History of the theory of numbers. Vol. II: Diophantine analysis*, Chelsea Publishing Co., New York, 1966, pp. xxv+803.

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

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

[FPS] 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** (1997), 435–463.

[H] L. Hajdu, *Perfect powers in arithmetic progression. A note on the inhomogeneous case*, Acta Arith. **113** (2004), 343–349.

[M] L. J. Mordell, *Diophantine Equations*, Academic Press, London and New York, 1969.

[magma] J. Cannon et al., *The Magma computational algebra system* , http://magma.maths.usyd.edu.au.

[notes] *Transcript of computations*, http://www.cecm.sfu.ca/∼nbruin/unlikepowers.

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

[P] B. Poonen, *The classification of rational preperiodic points of quadratic polynomials over* $\mathbb{Q}$*: a refined conjecture*, Math. Z. **228** (1998), 11–29.

[Sh] T. N. Shorey, *Powers in arithmetic progression*, in: A Panorama in Number Theory (G. Wüstholz, ed.), Cambridge Univ. Press, Cambridge, 2002, pp. 325–336.

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

[T1] Sz. Tengely, *On the Diophantine equation* $x^2 + a^2 = 2y^p$, Indag. Math. (N.S.) **15** (2004), 291–304.

[T2] Sz. Tengely, *Effective Methods for Diophantine Equations*, Ph.D. thesis, Leiden Univ., Leiden, The Netherlands, 2004.

[T] R. Tijdeman, *Diophantine equations and diophantine approximations*, in: Number Theory and Applications (R. A. Mollin, ed.), Kluwer Acad. Press, 1989, pp. 215–243.

Nils Bruin

Department of Mathematics
Simon Fraser University
Burnaby, BC
Canada V5A 1S6

Kálmán Győry
Lajos Hajdu

Number Theory Research Group
of the Hungarian Academy of Sciences, and

University of Debrecen
Institute of Mathematics
P.O. Box 12
4010 Debrecen
Hungary

Szabolcs Tengely

University of Debrecen
Institute of Mathematics
P.O. Box 12
4010 Debrecen
Hungary

E-mail address:
nbruin@cecm.sfu.ca
gyory@math.klte.hu
hajdul@math.klte.hu
tengely@math.klte.hu

II.3 [H08]: Powerful arithmetic progressions

Indag. Math. **19** (2008), 547–561.

POWERFUL ARITHMETIC PROGRESSIONS

L. HAJDU[1]

Abstract. We give a complete characterization of so called powerful arithmetic progressions, i.e. of progressions whose kth term is a kth power for all k. We also prove that the length of any primitive arithmetic progression of powers can be bounded both by any term of the progression different from 0 and ± 1, and by its common difference. In particular, such a progression can have only finite length.

1. Introduction

In this paper we consider arithmetic progressions of mixed powers. We start with a question concerning a special but interesting case, then we turn to the general problem.

In 1998 Boklan [1] asked the following question: what is the length of the longest nonconstant arithmetic progression of integers with the property that the kth term (for all $k \geq 1$) is a perfect kth power? Such progressions are called powerful arithmetic progressions.

The problem was solved by Robertson [15], who proved that there are no such progressions of length six. He gave a particular example of a length five progression, too. Note that the same result was obtained by Manoharmayum, Reid, the GCHQ Problems Group, and Boklan and Elkies, as well (see [15] again).

In this paper we give a complete characterization of possible lengths of powerful arithmetic progressions. For this we need a simple notion. A (finite or infinite) arithmetic progression $a_1, a_2, \ldots, a_n, \ldots$ of integers is called *primitive*, if $\gcd(a_1, a_2) = 1$ is valid. Throughout the paper we shall write d for the common difference of such a progression. Note that the progression is primitive if and only if a_1 and d are coprime. We prove that the only primitive powerful arithmetic progression of length five is the trivial one, but there are infinitely many such progressions of length four. We also prove that in the nonprimitive case there are infinitely many pairwise nonproportional powerful arithmetic progressions of length five. In view of the above mentioned result of

2000 *Mathematics Subject Classification.* 11D61, 11B25, 11Y50.

Key words and phrases. Perfect powers, arithmetic progression.

1) Research supported in part by the Hungarian Academy of Sciences, and by the OTKA grants T48791 and T67580.

Robertson, our results (and their proofs) provide a complete characterization of the possible lengths of powerful arithmetic progressions. For some related results we refer to the papers [6], [10] and the references there. For example, in [6], all arithmetic progressions of squares and cubes are completely described. The main tool of our proofs is the elliptic Chabauty method (see e.g. [3], [4] and the references given there).

We also prove some results about more general arithmetic progressions of powers. That is, we consider progressions of the form

$$x_1^{k_1}, x_2^{k_2}, \ldots, x_n^{k_n}, \ldots \tag{1}$$

with $x_i \in \mathbb{Z}$, $k_i \geq 2$ $(i = 1, 2, \ldots)$. Obviously, such arithmetic progressions are closely related to generalized Fermat-type equations of the form

$$AX^p + BY^q = CZ^r,$$

where A, B, C, p, q, r are integers with $ABC \neq 0$, $p, q, r \geq 2$, and X, Y, Z are unknown integers. For general finiteness results about such equations (in the case when the exponents p, q, r are arbitrary, but fixed), see the excellent paper [8] and the references there.

We are interested in bounding the length of (1). Under some conditions, there are certain related results in the literature. The author in [9] proved that if $k_i \leq K$ holds in (1) for all i, then the length of the progression is bounded in terms of K only. Later, under the further assumption of primitivity, the number of such progressions has been bounded, as well (see [6]). In [9] it is also proved that assuming the *abc* conjecture, the condition $k_i \leq K$ can be replaced by primitivity, and the length of the progression is still bounded.

In the present paper we show that the length of a progression (1) can be bounded both by the help of any of its terms different from $0, \pm 1$, and with its common difference. As an immediate consequence we obtain that the length of any nonconstant arithmetic progression of powers is finite. Though the latter theorem can also be obtained as a simple consequence of a classical result of Dirichlet, we were unable to find it in the literature.

2. Results

We start with characterizing powerful arithmetic progressions. Our main result in this direction is the following.

Theorem 2.1. *The only primitive powerful arithmetic progression of length five is the trivial one, given by* $1, 1, 1, 1, 1$.

For the complete characterization of lengths, we also need

Theorem 2.2. *There are infinitely many primitive powerful arithmetic progressions of length four.*

Note that in the proof of Theorem 2.2 we give a complete description of length four primitive powerful arithmetic progressions.

The next result shows why it is necessary to impose the primitivity condition in the above two theorems. Note that having a particular primitive powerful arithmetic progression, after multiplying by appropriate factors one can obtain infinitely many nonprimitive progressions. Hence to get some meaningful statement we need to avoid this triviality.

Theorem 2.3. *There are infinitely many pairwise nonproportional powerful arithmetic progressions of length five.*

The result of Robertson and others mentioned in the introduction yields that there are no length six nonconstant powerful arithmetic progressions. So the above theorems provide a complete characterization of the lengths of powerful arithmetic progressions.

We also prove some results about general arithmetic progressions of powers. First we show that the length of such a progression can be bounded by its terms different from $0, \pm 1$.

Theorem 2.4. *Let x and k be integers, with $|x| \geq 2$ and $k \geq 2$. Then there exists a constant $C(x,k)$, depending only on x and k, such that the length of any arithmetic progression of powers containing x^k is at most $C(x,k)$.*

The next result shows that the assumption $x \neq 0$ is necessary in the previous theorem. We mention that the cases $x = \pm 1$ remain open; see also the problem posed in Remark 2.3.

Proposition 2.1. *There exist arithmetic progressions of powers of arbitrary (finite) length containing 0 as a term.*

Now we prove that the length of an arithmetic progression of powers can also be bounded by its common difference.

Theorem 2.5. *Let d denote the common difference of a nonconstant arithmetic progression (1) of powers and write n for the length of the progression. Then we have both estimates:*

i) $n \leq \max(3.125 \log(d) - 1, 73)$,

ii) $n \leq \max(2(\omega(d)+1)(\log(\omega(d)+1) + \log\log(\omega(d)+1)) - 1, 21)$,

where $\omega(d)$ denotes the number of prime divisors of d.

Remark 2.1. Note that in view of the proof, for small values of d, both bounds i) and ii) for the length of the progression can be improved. As the most interesting example, in case of $d = 1$ the first two terms of the progression give rise to the famous Catalan-equation

$$X^u - Y^v = 1$$

in unknown integers X, Y, u, v with $u, v \geq 2$. As is well-known, the only solution to this equation with $XY \neq 0$ is given by $(X, Y, u, v) =$

$(3, 2, 2, 3)$ (see [13]). Hence in this case, taking into account the trivial progression $-1, 0, 1$, the length of (1) is at most three.

Remark 2.2. In [17], Shorey and Tijdeman investigated the equation

$$x(x+d)\dots(x+(n-1)d) = by^k, \tag{2}$$

where x, d, n, b, y, k are unknown positive integers with $\gcd(x, d) = 1$, $k \geq 2$ and $P(b) \leq n$ where $P(b)$ denotes the greatest prime divisor of b (with the convention $P(1) = 1$). They proved for the solutions of (2) that $n < C(\omega(d))$ must be valid for some effective constant $C(\omega(d))$ depending only on $\omega(d)$. By a simple standard argument, one can show that equation (2) is equivalent to having an arithmetic progression of the form

$$a_1x_1^k, a_2x_2^k, \dots, a_nx_n^k$$

with some positive integers a_i with $P(a_i) \leq n$. Thus interestingly (though with different settings) we have similar bounds for the lengths of arithmetic progressions of powers with "equal" and "different" exponents, in terms of the common difference d.

As a simple and immediate consequence of both Theorem 2.4 and Theorem 2.5, we obtain the following result.

Corollary 2.1. *The length of any nonconstant arithmetic progression of powers is finite.*

Remark 2.3. One can easily construct progressions (1) of arbitrary finite length, see e.g. Proposition 2.1 and Remark 2 of [9]. Hence Corollary 2.1 is best possible in the qualitative sense. However, by the constructions in Proposition 2.1 and in [9], only nonprimitive progressions can be obtained. We propose the following problem: prove that the length of any primitive nonconstant arithmetic progression of powers is bounded by an absolute constant.

3. Proofs

Proof of Theorem 2.1. Suppose that

$$x_1^1,\ x_2^2,\ x_3^3,\ x_4^4,\ x_5^5 \tag{3}$$

is a primitive powerful arithmetic progression of integers. We observe from the primitivity condition that $\gcd(x_2, x_3) = 1$. Further we have

$$3(x_4^2)^2 - x_2^2 = 2x_5^5. \tag{4}$$

Let $K = \mathbb{Q}(\alpha)$ with $\alpha = \sqrt{3}$, and let $\mathcal{O}_K$ denote the ring of integers of K. Factorizing the above equation in $\mathcal{O}_K$ we get

$$(\alpha x_4^2 - x_2)(\alpha x_4^2 + x_2) = 2x_5^5. \tag{5}$$

It is well known that $\varepsilon = \alpha + 2$ is a fundamental unit of K of norm $N_{K/\mathbb{Q}}(\varepsilon) = -1$, the only roots of unity of K are ± 1 and we have $2 = \varepsilon(\alpha - 1)^2$. Further $\{1, \alpha\}$ is an integral basis of K.

By the primitivity condition one can easily check that $\gcd(x_2, x_4) \leq 2$. If $\gcd(x_2, x_4) = 2$, then we get $2d = x_4^4 - x_2^2$. Hence d is even which violates the primitivity condition. So we conclude that $\gcd(x_2, x_4) = 1$. Using this assertion, keeping in mind the well-known fact that $\mathcal{O}_K$ is a Euclidean ring, we obtain from (5) that

$$\alpha x_4^2 + x_2 = \varepsilon^{t_1}(\alpha + 1)^{t_2}(\alpha u + v)^5 \tag{6}$$

holds with some integers u, v, t_1, t_2 with $-2 \leq t_1 \leq 2$ and $0 \leq t_2 \leq 4$. Here we used the fact that -1 is a full fifth power. By $\gcd(x_2, x_4) = 1$, we have $\gcd(u, v) = 1$. We shall use this fact later on without any reference. Further, taking the field norms of both sides of (6), we immediately get that $t_2 = 1$. Finally, taking field conjugates over K and substituting $-x_2$ and $-v$ in places of x_2 and v, respectively, we may assume without loss of generality that $t_1 \in \{0, 1, 2\}$. We investigate these cases in turn.

The case $t_1 = 0$. Using that $t_2 = 1$, by comparing the coefficients of α on both sides of (6), we get

$$v^5 + 5v^4u + 30v^3u^2 + 30v^2u^3 + 45vu^4 + 9u^5 = x_4^2. \tag{7}$$

Let $f_0(v, u)$ denote the left hand side of (7), and define the polynomial g_0 by $g_0(x) = x^5 + 5x^4 + 30x^3 + 30x^2 + 45x + 9$ (i.e. $g_0(x) = f_0(x, 1)$). A simple check, for e.g. by Magma [2], assures that g_0 is irreducible over $\mathbb{Q}$. Let β denote a root of g_0, and put $L = \mathbb{Q}(\beta)$. Write $\mathcal{O}_L$ for the ring of integers of L.

To proceed smoothly, we need some information about L. These data are available by the use of Magma again. The class number of L is one,

$$\vartheta_0 = 1, \quad \vartheta_1 = \beta, \quad \vartheta_2 = (\beta^2 + 1)/2,$$
$$\vartheta_3 = (\beta^3 + 5\beta^2 + 9\beta + 9)/12, \quad \vartheta_4 = (\beta^4 + 8\beta^2 + 15)/24$$

is an integral basis of L, and

$$\eta_1 = -\vartheta_1 + 2\vartheta_3 - 2\vartheta_4, \quad \eta_2 = -\vartheta_0 - \vartheta_1 - 2\vartheta_2 + 2\vartheta_3 + \vartheta_4$$

is a system of fundamental units for L, with $N_{L/\mathbb{Q}}(\eta_1) = N_{L/\mathbb{Q}}(\eta_2) = 1$. Further, the only roots of unity in L are ± 1, and we also have

$$2 = \gamma_1\gamma_2^2, \quad 3 = \gamma_3\vartheta_1^2, \quad 5 = \eta_2\gamma_4^5,$$

where the γ_i $(i = 1, \ldots, 4)$ are some prime elements in $\mathcal{O}_L$, with

$$N_{L/\mathbb{Q}}(\gamma_1) = 2, \quad N_{L/\mathbb{Q}}(\gamma_2) = 4, \quad N_{L/\mathbb{Q}}(\gamma_3) = 3, \quad N_{L/\mathbb{Q}}(\gamma_4) = 5.$$

As the γ_i do not play any role later on, we suppress the concrete values. Note that ϑ_1 is also a prime in $\mathcal{O}_L$, and $N_{L/\mathbb{Q}}(\vartheta_1) = -9$.

Factorizing the left hand side of (7) over $\mathcal{O}_L$ (using Magma again) we get

$$(v - \vartheta_1 u)h_0(v, u) = x_4^2 \tag{8}$$

with

$$h_0(v,u) = v^4 + (5\vartheta_0 + \vartheta_1)v^3u + (29\vartheta_0 + 5\vartheta_1 + 2\vartheta_2)v^2u^2 + \\ + (21\vartheta_0 + 21\vartheta_1 + 12\vartheta_3)vu^3 - (12\vartheta_0 + 15\vartheta_1 + 6\vartheta_2 - 60\vartheta_3 - 24\vartheta_4)u^4.$$

Using that the only prime divisors of the discriminant of g_0 are $2, 3, 5$, we obtain from (8) that both

$$v - \vartheta_1 u = (-1)^{s_1}\ \eta_1^{s_2}\ \eta_2^{s_3}\ \gamma_1^{s_4}\ \gamma_2^{s_5}\ \gamma_3^{s_6}\ \vartheta_1^{s_7}\ \gamma_4^{s_8}\ \gamma_5^{s_9}\ \delta_1^2 \tag{9}$$

and

$$h_0(v,u) = (-1)^{s_1}\ \eta_1^{s_2}\ \eta_2^{s_3}\ \gamma_1^{s_4}\ \gamma_2^{s_5}\ \gamma_3^{s_6}\ \vartheta_1^{s_7}\ \gamma_4^{s_8}\ \gamma_5^{s_9}\ \delta_2^2 \tag{10}$$

must hold, with some $\delta_1, \delta_2 \in \mathcal{O}_L$ and $s_i \in \{0,1\}$ $(i = 1, \dots, 9)$. (As the product of the right hand sides of (9) and (10) should be a full square, one can easily check that the exponents s_i must indeed coincide in (9) and (10).) Taking field norms of both sides of (9), we immediately get that $s_4 = s_5 = s_6 = s_8 = s_9 = 0$ and $s_1 + s_7 \neq 1$. Hence we are left with eight possibilities.

In case of $s_2 = 1$, all the four corresponding equations can be excluded locally. If $u = 0$, then $v = \pm 1$ and using (7) and (6), we get that the progression (3) is given by $1, 1, 1, 1, 1$. Otherwise, after dividing both sides of equation (10) by u^4 and merging it into δ_2^2, we consider the corresponding equations as hyperelliptic curves over L (using the `HyperellipticCurve` command of Magma). Then we determine those prime ideals of $\mathcal{O}_L$, where the equation might not be solvable locally (by the procedure `BadPrimes`). Finally, we test whether these equations are locally solvable at all these prime ideals or not (using the procedure `IsLocallySolvable`). In all four cases mentioned above, we could find a prime ideal where the curves has no points locally. Hence these cases can be excluded.

Suppose next that, together with $s_2 = 0$, we have $s_1 = s_3 = s_7 = 1$. Then writing $\delta_1 = z_0\vartheta_0 + z_1\vartheta_1 + z_2\vartheta_2 + z_3\vartheta_3 + z_4\vartheta_4$ in (9) and expanding both sides of the equation, we obtain from matching the coefficients of $\vartheta_0, \vartheta_1, \vartheta_4$ that the integers

$$z_0^2 + z_1^2 + z_3^2 + v, \quad u, \quad z_0^2 + z_1^2 + z_3^2$$

must all be even. Hence we conclude that both v and u are even. However, by (7), this implies that x_4 is even which contradicts the primitivity of the arithmetic progression, in a similar manner as before.

Assume next that (beside $s_2 = 0$) we have $s_1 = s_7 = 0$, $s_3 = 1$. Then by the same method used in the previous paragraph, following the same notation (but now matching the coefficients of $\vartheta_0, \vartheta_1, \vartheta_3, \vartheta_4$) we get that the integers

$$z_0^2 + z_1^2 + z_3^2 + z_4^2 + v, \quad z_0^2 + z_1^2 + z_3^2 + z_4^2 + u, \quad z_4^2, \quad z_0^2 + z_1^2 + z_3^2$$

are all even. Hence we easily obtain that both v and u are even, thus by (7), x_4 is even once again. So this case is also excluded by contradiction.

Consider now the case $s_1 = s_3 = s_7 = 0$ (and $s_2 = 0$). Then (10) defines a projective genus 1 curve $C_1^{(0)}$ over L (considering v, u, δ_2 to be unknowns from L). By the help of the point $P = (0 : 1 : 0)$ the curve $C_1^{(0)}$ can be transformed into an elliptic curve. More precisely, by a method of Cassels (see [7]) using P, one can find a homogeneous elliptic curve C' in the usual form

$$C' : \quad y^2z + r_1xyz + r_3yz^2 = x^3 + r_2x^2z + r_4xz^2 + r_6z^3$$

with coefficients $r_1, r_2, r_3, r_4, r_6 \in L$ such that $C_1^{(0)}$ and C' are birationally equivalent. After dehomogenizing C' we get a plane elliptic curve over L. In our case the resulting dehomogenized elliptic curve has a minimal model

$$E_1^{(0)} : \; Y^2 = X^3 - (\vartheta_1 + \vartheta_2 + \vartheta_3 + \vartheta_4)X^2 + (73\vartheta_0 + 95\vartheta_1 + \\ + 26\vartheta_2 - 287\vartheta_3 - 125\vartheta_4)X + 125\vartheta_0 + 158\vartheta_1 + 48\vartheta_2 - 466\vartheta_3 - 204\vartheta_4.$$

Note that all the curves, together with the transformations among them can be handled by Magma. For more explanation about the techniques we use we refer to [5]. Now, as v and u are known to be rational coordinates of $C_1^{(0)}$, one can apply the elliptic Chabauty method to solve (10) completely. Here we only indicate the main steps of the solution, without explaining the background theory. For the theory of the method we refer to [3] and [4] and the references given there. To see how the method works in practice, in particular by the help of Magma, [5] is an excellent source. For applying elliptic Chabauty in similar context, beside the above references see also [6], [10], [11], [12], [19]. So, to have the method work, the rank of $E_1^{(0)}(L)$ should be strictly less than the degree of L (which is five). In the present case it turns out that the rank of $E_1^{(0)}(L)$ is three, so elliptic Chabauty is applicable. Further, the procedure `PseudoMordellWeilGroup` of Magma is able to find a subgroup $G_1^{(0)}$ of $E_1^{(0)}(L)$ of finite odd index. Then, using the procedure `Chabauty` with the prime 11, we get that all solutions to (10) with v, u coprime rational integers are

$$(v, u, \delta_2) = (\pm 1, 0, \pm 1), (-1, 4, \pm(51\vartheta_0 + 50\vartheta_1 + 18\vartheta_2 - 168\vartheta_3 - 68\vartheta_4)).$$

The first solution by (7) yields that $x_4 = \pm 1$. Further, (6) implies that $x_2 = \pm 1$, so the arithmetic progression (3) is given by $1, 1, 1, 1, 1$. In the second case (7) gives an immediate contradiction.

Finally, assume that $s_1 = s_7 = 1$, $s_3 = 0$ (and also $s_2 = 0$). Then similarly as in the previous paragraph, (10) defines a projective genus 1 curve $C_2^{(0)}$ over L. Using the point $(0 : 3/\vartheta_1 : 1)$, $C_2^{(0)}$ can be transformed into an elliptic curve, which has a minimal model

$$E_2^{(0)} : \; Y^2 = X^3 + (\vartheta_1 - \vartheta_3 + \vartheta_4)X^2 - (1261\vartheta_0 + 1657\vartheta_1 + \\ + 2245\vartheta_2 - 2691\vartheta_3 - 701\vartheta_4)X - 110\vartheta_0 - 4684\vartheta_1 - 487\vartheta_2 + 8571\vartheta_3 - 9096\vartheta_4.$$

The rank of $E_2^{(0)}(L)$ is one, so elliptic Chabauty can be applied for $E_2^{(0)}$. Note that here the procedure `PseudoMordellWeilGroup` with the default settings fails to find a subgroup $G_2^{(0)}$ of $E_2^{(0)}(L)$ of finite odd index. However, using the procedure `SelmerGroup` and the nontorsion point

$$\left(\frac{28\vartheta_0+44\vartheta_1+54\vartheta_2-68\vartheta_3-5\vartheta_4}{5}, \frac{266\vartheta_0+200\vartheta_1+461\vartheta_2-296\vartheta_3-450\vartheta_4}{5}\right)$$

of $E_2^{(0)}(L)$, by a slightly more involved procedure (explained in detail in [5], pp. 18 and 19), we can find such a subgroup $G_2^{(0)}$. Then again, using the procedure `Chabauty` now with the prime 7, we get all solutions to (10) with v, u rational. Note that now by the procedure `IsPSaturated` we also need to check that the index $[E_2^{(0)}(L) : G_2^{(0)}]$ is not divisible by 5. After all, we get that

$$(v, u, \delta_2) = (0, \pm 1, \pm(4\vartheta_0+5\vartheta_1+2\vartheta_2-20\vartheta_3-8\vartheta_4))$$

are the only solutions to (10) with coprime integers v, u. Then (7) implies $x_4 = \pm 3$ and (6) yields that $x_2 = \pm 27$. Though this with $x_5 = -3$ extends to a solution of (4), however, as one can easily check, does not yield any (even nonprimitive) arithmetic progression of the form (3).

The case $t_1 = 1$. Noting that $t_2 = 1$, comparing again the coefficients of α on both sides of (6) in this case, we obtain

$$3v^5+25v^4u+90v^3u^2+150v^2u^3+135vu^4+45u^5 = x_4^2. \tag{11}$$

Let $f_1(v, u)$ denote the left hand side of (11) and define the polynomial g_1 as $g_1(x) = 3x^5+25x^4+30x^3+30x^2+45x+9$ (that is $g_1(x) = f_1(x, 1)$). Using Magma we get that g_1 is irreducible over $\mathbb{Q}$. Let L denote the same number field as in case of $t_1 = 0$ and keep all the related notation as well. (Note that g_0 and g_1 define the same number field L.) Factorizing the left hand side of (11), we get

$$\begin{aligned}((-27\vartheta_0-32\vartheta_1-10\vartheta_2+96\vartheta_3+40\vartheta_4)v+\\ +(26\vartheta_0+25\vartheta_1+8\vartheta_2-72\vartheta_3-30\vartheta_4)u)h_1(v, u) = x_4^2\end{aligned} \tag{12}$$

where

$$\begin{aligned}h_1(v, u) = (-\vartheta_0+2\vartheta_2)v^4-(5\vartheta_0-3\vartheta_1-14\vartheta_2+\\ +2\vartheta_4)v^3u-(3\vartheta_0-13\vartheta_1-40\vartheta_2+8\vartheta_3+14\vartheta_4)v^2u^2-(9\vartheta_0-3\vartheta_1-30\vartheta_2-12\vartheta_3+\\ +18\vartheta_4)vu^3-6\vartheta_0-3\vartheta_1+6\vartheta_2+12\vartheta_3-6\vartheta_4.\end{aligned}$$

As the only prime divisors of the discriminant of g_1 are $2, 3, 5$, from (12), we get that both

$$(13)\quad (-27\vartheta_0 - 32\vartheta_1 - 10\vartheta_2 + 96\vartheta_3 + 40\vartheta_4)v + (26\vartheta_0 + 25\vartheta_1 + \\ + 8\vartheta_2 - 72\vartheta_3 - 30\vartheta_4)u = (-1)^{k_1}\ \eta_1^{k_2}\ \eta_2^{k_3}\ \gamma_1^{k_4}\ \gamma_2^{k_5}\ \gamma_3^{k_6}\ \vartheta_1^{k_7}\ \gamma_4^{k_8}\ \gamma_5^{k_9}\ \xi_1^2$$

and

$$(14)\qquad h_1(v,u) = (-1)^{k_1}\ \eta_1^{k_2}\ \eta_2^{k_3}\ \gamma_1^{k_4}\ \gamma_2^{k_5}\ \gamma_3^{k_6}\ \vartheta_1^{k_7}\ \gamma_4^{k_8}\ \gamma_5^{k_9}\ \xi_2^2$$

hold, with some $\xi_1, \xi_2 \in \mathcal{O}_L$ and $k_i \in \{0, 1\}$. (Similarly as in case of $t_1 = 0$, the k_i must coincide in (13) and (14).) Taking field norms of both sides of (13) yields $k_4 = k_5 = k_6 = k_8 = k_9 = 0$ and $k_1 + k_7 \neq 1$. Hence we are left with eight possibilities again.

In case of $k_2 = 1$, all the four corresponding equations (14) can be excluded locally. As it can be done in the same way as for $t_1 = 0$, we suppress the details.

If $k_3 = 1$ (together with $k_2 = 0$), then, in both possible cases, we can apply the same method as with $t_1 = 0$. Looking at the coefficients of the ϑ_i in (13), modulo 2 we obtain that both v and u should be even which gives a contradiction in a similar manner as previously. We suppress the details once again.

Consider now the case $k_1 = k_3 = k_7 = 0$ (and $k_2 = 0$). Then similarly as with $t_1 = 0$, (14) defines a projective genus 1 curve $C_1^{(1)}$ over L. By the help of the point $(0 : 1 : 0)$ (after dividing each coefficients by the leading coefficient ϑ_1^2 of $h_1(v, u)$, and also merging it into ξ_2^2), $C_1^{(1)}$ can be transformed into an elliptic curve which has a minimal model

$$E_1^{(1)}:\ Y^2 = X^3 - (\vartheta_1 + \vartheta_2 + \vartheta_3)X^2 + (26\vartheta_0 + 50\vartheta_1 + \\ + 47\vartheta_2 - 84\vartheta_3 + 18\vartheta_4)X + 148\vartheta_0 + 140\vartheta_1 + 260\vartheta_2 - 216\vartheta_3 - 192\vartheta_4.$$

Using elliptic Chabauty as previously, by the procedure `Chabauty` of Magma with the prime 7, we obtain that all solutions to (14) with coprime integers v, u are

$$(v, u, \xi_2) = (\pm 1, 0, \pm\vartheta_1).$$

This by (11) yields a contradiction.

Finally let $k_1 = k_7 = 1$, $k_3 = 0$ (together with $k_2 = 0$). Then as before, (14) defines a projective genus 1 curve $C_2^{(1)}$ over L. Using the point $(0 : 7\vartheta_0 + 7\vartheta_1 + 2\vartheta_2 - 19\vartheta_3 - 8\vartheta_4 : 1)$, $C_2^{(1)}$ can be transformed into an elliptic curve having a minimal model

$$E_2^{(1)}:\ Y^2 = X^3 - (\vartheta_0 - \vartheta_1 + \vartheta_2 - \vartheta_3 - \vartheta_4)X^2 + (12\vartheta_0 + 17\vartheta_1 + \\ + 24\vartheta_2 - 29\vartheta_3 - 7\vartheta_4)X - 11\vartheta_0 - 26\vartheta_1 - 21\vartheta_2 + 44\vartheta_3 - 16\vartheta_4.$$

By the help of the procedure `Chabauty` with the prime 11, we obtain that

$$(v,u,\xi_2) = (0,\pm 1,\pm(2\vartheta_0 - 5\vartheta_3 - 2\vartheta_4)),$$
$$(12,17,\pm(728\vartheta_0 - 642\vartheta_1 + 402\vartheta 2 - 317\vartheta_3 + 298\vartheta_4))$$

are the only solutions to (14) with coprime integers v,u. In case of the first possibility, (11) immediately implies a contradiction. In the second case, (11) and (7) give $x_4 = \pm 3\cdot 6323$ and $x_2 = \pm 3^3\cdot 23094391$, respectively. These values with $x_5 = -3\cdot 241$ yield a solution to (4). However, as one can readily check, they do not give rise to any (even nonprimitive) arithmetic progression (3).

The case $t_1 = 2$. In this case, from equation (6), we obtain

$$(v+u)f_2(v,u) = x_4^2 \tag{15}$$

with $f_2(v,u) = 11v^4 + 84v^3u + 246v^2u^2 + 324vu^3 + 171u^4$. Put $g_2(x) = f_2(x,1)$. As the discriminant of $(v+u)f_2(v,u)$ is divisible by the primes $2,3,5$ only, from (15), we get

$$f_2(v,u) = (-1)^{m_1}\ 2^{m_2}\ 3^{m_3}\ 5^{m_4}\ w^2 \tag{16}$$

with some integer w and $m_i \in \{0,1\}$ $(i = 1,2,3,4)$. If $m_2 = 1$, then by (15) x_4 is even, which leads to a contradiction in a similar manner as many times before. Hence we may assume that $m_2 = 0$ in (16). In the remaining eight cases, after dividing both sides by u^4 (which by (15) cannot be zero), (16) gives rise to hyperelliptic equations of the form

$$(-1)^{m_1}3^{m_3}5^{m_4}g_2(x) = y^2, \tag{17}$$

where $g_2(x) = f_2(x,1)$. In the cases where $m_3 = 1$ and also in case of $m_1 = 1$, $m_3 = m_4 = 0$, the procedure `IsLocallySolvable` of Magma gives a contradiction modulo one of $2,3,5$. In the cases $m_1 = m_3 = m_4 = 0$ and $m_1 = m_4 = 1$, $m_3 = 0$, by (16), one can easily check that $3 \mid v$ must be valid. Then, in view of (15), we obtain $3 \mid x_4$ and by (6) also that $3 \mid x_2$ which contradicts the primitivity of the progression (3). Finally, if $m_1 = m_3 = 0$, $m_4 = 1$ then checking (16) modulo 4, we easily obtain that w must be even. However, then x_4 is also even by (15), which leads to a contradiction in the usual fashion. □

Proof of Theorem 2.2. To prove the theorem, it is obviously sufficient to show that there are infinitely many primitive arithmetic progressions of integers of the form

$$x_2^2,\quad x_3^3,\quad x_4^4. \tag{18}$$

We give a full characterization of progressions of the form (18). For this purpose, in fact we need to completely describe the solution set of the equation

$$x_2^2 + x_4^4 = 2x_3^3. \tag{19}$$

As is well-known, the solutions of equation (19) can be parametrized. More precisely, x_2, x_3, x_4 are coprime solutions to (19) if and only if

$$x_2 = u^3-3u^2v-3uv^2+v^3,\ x_3 = u^2+v^2,\ x_4^2 = u^3+3u^2v-3uv^2-v^3 \tag{20}$$

hold with some coprime integers u, v, $u \not\equiv v \pmod 2$ (see e.g. [14]). Trivially, we need to focus only on the last item of (20). Having it satisfied, the values of x_2 and x_3 are automatically chosen.

Obviously, we can find integers t, z such that $v = tz^2$ uniquely if we assume t to be square-free. As $z = 0$ leads to the constant progression $1, 1, 1$ in (18), we may also suppose that $z \neq 0$. Then the last item of (20) gives

$$E_t :\ Y^2 = X^3 + 3tX^2 - 3t^2X - t^3 \tag{21}$$

where

$$X = v/z^2 \quad \text{and} \quad Y = x_4/z^3. \tag{22}$$

We may consider (21) as a parametric family of elliptic curves E_t, taking t to be a square-free integral parameter and X, Y to be unknown rationals. As is well-known, any rational point on this curve has the property that the square of the denominator of Y is the same as the cube of the denominator of X (see e.g. [18]). That is, the transformation in (22) can be reversed.

Hence, taking any square-free t and choosing any rational point (X, Y) of E_t, we can write $X = U_1/V^2$ and $Y = U_2/V^3$ with integers U_1, U_2, V such that $\gcd(U_1U_2, V) = 1$. If further $\gcd(U_1, t) = 1$ and $U_1 \not\equiv tV^2 \pmod 2$, then putting $u = U_1$ and $v = tV^2$ we get a parametrization by (20) leading to a primitive arithmetic progression of the form (18). Already the choice $t = 1$ is sufficient to find infinitely many such solutions. Indeed, by Magma, we get that the rank of E_1 is one and the point $P = (-1, 2)$ generates the free part of the Mordell-Weil group of E_1. In particular, there are infinitely many rational points on E_1 leading to (different) arithmetic progressions of the shape (18). As one can easily see, this is the case for all points nP where n is a power of 2. To see an example, consider the point

$$4P = (10961/1936,\ -1372655/85184)$$

on E_1. Then putting $u = 10961$ and $v = 1936$ in (20), we get the primitive arithmetic progression

$$503107236801^2,\ 123891617^3,\ 1372655^4.$$

Observe that by the above procedure all progressions (18) can be determined. □

Proof of Theorem 2.3. By Theorem 2.2 we know that there are infinitely many primitive arithmetic progression of integers of the form

$$x_1^1,\ x_2^2,\ x_3^3,\ x_4^4. \tag{23}$$

Choose any progression of the shape (23) and put $s = x_4^4 + d$, where d denotes the common difference of the progression. Observe that by writing

$$y_1 = x_1 s^{24},\ y_2 = x_2 s^{12},\ y_3 = x_3 s^8,\ y_4 = x_4 s^6,\ y_5 = s^5,$$

the progression

$$y_1^1,\ y_2^2,\ y_3^3,\ y_4^4,\ y_5^5$$

is of the desired shape, and further the progressions obtained in this way are pairwise nonproportional. Hence the theorem follows. □

To prove Theorem 2.4 we need the following lemma.

Lemma 3.1. *Suppose that for a nonconstant arithmetic progression of powers of the form* (1) *we have $k_i \leq K$ for all i. Then the length of the progression is bounded by a constant depending only on K.*

Proof. The statement is a simple consequence of Theorem 2 of [9]. □

Proof of Theorem 2.4. Suppose that x^k is a member of an arithmetic progression of the form (1) where x and k are integers with $|x| \geq 2$, $k \geq 2$. Let p be a prime divisor of x and put $\alpha = \mathrm{ord}_p(x)$. Further, write d for the common difference of the progression, and set $\beta = \mathrm{ord}_p(d)$. Let γ be an arbitrary integer with $\gamma \geq \max(0, k\alpha + 1 - \beta)$. Observe that, for any $t \in \mathbb{Z}$, we have $\mathrm{ord}_p(y_t) = k\alpha$ where $y_t = x^k + tp^\gamma d$. Hence if $y_t = x_t^{k_t}$ holds for some t, then $k_t \leq k\alpha$ must be valid. As the numbers y_t form an arithmetic progression (with common difference $p^\gamma d$), by Lemma 3.1 we obtain that the length of this progression is bounded in terms of $k\alpha$. Hence the length of the original progression must be bounded by a constant $C(k, p, \alpha)$ depending only on k, p, α. As $p \leq x$ and $\alpha \leq \log(x)/\log(2)$, the statement follows. □

Proof of Proposition 2.1. Let p_i denote the ith prime. Take an arbitrary positive integer n. Then all integers m with $1 \leq m < p_{n+1}$ can be uniquely written in the form $m = p_1^{\alpha_{1m}} \dots p_n^{\alpha_{nm}}$ with nonnegative integers α_{im} $(i = 1, \dots, n)$. Put

$$H = \{(\alpha_{1m}, \dots, \alpha_{nm}) \ :\ 1 \leq m < p_{n+1}\}.$$

Further, for each $(h_1, \dots, h_n) \in H$ pick up an odd prime $q_{(h_1,\dots,h_n)}$. Then for every $i = 1, \dots, n$ choose a positive β_i such that

$$\beta_i \equiv -h_i \pmod{q_{(h_1,\dots,h_n)}} \quad \text{for all } (h_1, \dots, h_n) \in H. \tag{24}$$

By the Chinese remainder theorem we know that such β_i exists for all i. Let $d = p_1^{\beta_1} \dots p_n^{\beta_n}$, and observe that for every t from the interval $[-p_{n+1} + 1, p_{n+1} - 1]$, by (24), td is a $q_{(h_1,\dots,h_n)}$th power for the appropriate $(h_1, \dots, h_n) \in H$. Hence these numbers td form an arithmetic progression of powers of length $2p_{n+1} - 1$, and the statement follows.

We illustrate the construction with a simple example. Take $n = 2$. Then we have

$$H = \{(0,0), (1,0), (0,1), (2,0)\},$$

corresponding to the exponents of $p_1 = 2$ and $p_2 = 3$ in the numbers $1, 2, 3, 4$. Let

$$q_{(0,0)} = 3,\ q_{(1,0)} = 5,\ q_{(0,1)} = 7,\ q_{(2,0)} = 11.$$

Then (24) yields $\beta_1 = 504$ and $\beta_2 = 825$. Hence setting $d = 2^{504}3^{825}$, the numbers td $(-4 \le t \le 4)$ form a progression of the shape (1) of length $2 \cdot p_3 - 1 = 9$. □

Proof of Theorem 2.5. Let p be any prime which does not divide d. Then among any $2p$ consecutive terms of the progression there are two, say y_0 and $y_p = y_0 + pd$, which are divisible by p. Further, either $\mathrm{ord}_p(y_0) = 1$ or $\mathrm{ord}_p(y_p) = 1$ must be valid. However, as these terms are perfect powers, this is impossible. Hence $n \le 2p - 1$.

To derive the bound i), write $\vartheta^*(p)$ for the logarithm of the product of all primes $< p$, with the convention $\vartheta^*(2) = 0$. Then the Corollary of Theorem 4 of [16] implies that

$$\vartheta^*(p) > p(1 - 1/\log(p)) - \log(p)$$

provided that $p \ge 41$. Hence a simple calculation yields that for $p \ge 41$ we have

$$\vartheta^*(p)/p > 0.64.$$

As clearly $\log(d) \ge \vartheta^*(p)$ if $p \ge 41$, we have

$$2p - 1 < 3.125 \log(d) - 1$$

in this case. Otherwise, trivially $2p - 1 \le 73$ holds, and the bound i) follows.

To get the estimate ii), write p_i for the ith prime. The Corollary of Theorem 3 of [16] gives that for $i \ge 6$

$$p_i < i(\log(i) + \log\log(i))$$

holds. Noting that $p \le p_{\omega(d)+1}$, the above inequality immediately yields ii), and the theorem follows. □

Proof of Corollary 2.1. Obviously, the statement is a trivial and immediate consequence both of Theorem 2.4 and of Theorem 2.5. However we show here that the result easily follows also from Dirichlet's famous theorem about primes in arithmetic progressions. Let

$$a_1, a_2, \ldots, a_n, \ldots \tag{25}$$

be a nonconstant arithmetic progression of integers. Suppose that $a_i = x_i^{k_i}$ holds with $k_i \ge 2$ for all $i = 1, 2, \ldots$. Let $D = \gcd(a_1, a_2)$. Then we can write $a_i = Db_i$ for all $i = 1, 2, \ldots$. Observe that then

$$b_1, b_2, \ldots, b_n, \ldots$$

is also an arithmetic progression, and we have $\gcd(b_1, b_2) = 1$, as well. Thus if the length of this progression is infinite, by Dirichlet's theorem we obtain that it contains infinitely many primes. Let p be any prime in the progression with $p > D$. Then $b_i = p$ is valid for some i, hence we should have $x_i^{k_i} = Dp$. However p divides the right hand side exactly on the first power which contradicts the assumption $k_i \geq 2$. Hence any progression of the shape (25) must have finite length and the statement follows. □

4. Acknowledgment

The author is grateful to the referee for his useful remarks.

References

[1] K. D. Boklan, *Problem 10702*, Amer. Math. Monthly **105** (1998), p. 956.
[2] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), 235–265.
[3] N. Bruin, *Chabauty methods and covering techniques applied to generalized Fermat equations*, CWI Tract, Vol. 133, Stichting Mathematisch Centrum, Centrum voor Wiskunde en Informatica, Amsterdam, 2002.
[4] N. Bruin, *Chabauty methods using elliptic curves*, J. Reine Angew. Math. **562** (2003), 27–49.
[5] N. Bruin, *Diophantine equations of signature* $(n, n, 2)$, In: Discovering mathematics with Magma, Algorithms Comput. Math. **19** (2006), 63–91.
[6] N. Bruin, K. Győry, L. Hajdu, Sz. Tengely, *Arithmetic progressions consisting of unlike powers*, Indag. Math. **17** (2006), 539–555.
[7] J. W. S. Cassels, *Lectures on elliptic curves*, London Mathematical Society Student Texts, vol. 24, Cambridge University Press, Cambridge, 1991.
[8] H. Darmon, A. Granville, *On the equations* $z^m = F(x, y)$ *and* $Ax^p + By^q = Cz^r$, Bull. London Math. Soc. **27** (1995), 513–543.
[9] L. Hajdu, *Perfect powers in arithmetic progression. A note on the inhomogeneous case*, Acta Arith. **113** (2004), 343–349.
[10] L. Hajdu, Sz. Tengely, *Arithmetic progressions of squares, cubes and n-th powers*, Functiones et Approximatio (to appear).
[11] L. Hajdu, Sz. Tengely, R. Tijdeman, *Cubes in products of terms in arithmetic progression*, Publ. Math. Debrecen **74** (2009), 215–232.
[12] S. Laishram, T. N. Shorey, Sz. Tengely, *Squares in products in arithmetic progression with at most one term omitted and common difference a prime power*, Acta Arith. **135** (2008), 143–158.
[13] P. Mihăilescu, *Primary cyclotomic units and a proof of Catalan's conjecture*, J. Reine Angew. Math. **572** (2004), 167–195.
[14] I. Pink, Sz. Tengely, *Full powers in arithmetic progressions*, Publ. Math. Debrecen **57** (2000), 535–545.
[15] J. P. Robertson, *The Maximum Length of a Powerful Arithmetic Progression: 10702*, Amer. Math. Monthly **107** (2000), p. 951.
[16] J. B. Rosser, L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. **6** (1962), 64-94.
[17] T. N. Shorey, R. Tijdeman, *Perfect powers in products of terms in arithmetical progression*, Compositio Math. **75** (1990), 307–344.
[18] J. H. Silverman, J. Tate *Rational points on elliptic curves*, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1992.

[19] Sz. Tengely, *Note on the paper "An extension of a theorem of Euler" by Hirata-Kohno et al.*, Acta Arith. **134** (2008), 329–335.

University of Debrecen, Institute of Mathematics
and the Number Theory Research Group
of the Hungarian Academy of Sciences
Debrecen
P.O. Box 12.
H-4010
Hungary
E-mail address: hajdul@math.klte.hu

III. Számtani sorozatot alkotó vegyes hatványok

III.1 [H07]: Arithmetic progressions

in linear combinations of S-units

Period. Math. Hungar. **54** (2007), 175–181.

ARITHMETIC PROGRESSIONS IN LINEAR COMBINATIONS OF S-UNITS

L. Hajdu

Abstract. M. Pohst asked the following question: is it true that every prime can be written in the form $2^u \pm 3^v$ with some non-negative integers u, v? We put the problem into a general framework, and prove that the length of any arithmetic progression in t-term linear combinations of elements from a multiplicative group of rank r (e.g. of S-units) is bounded in terms of r, t, n, where n is the number of the coefficient t-tuples of the linear combinations. Combining this result with a recent theorem of Green and Tao on arithmetic progressions of primes, we give a negative answer to the problem of M. Pohst.

1. Introduction and results

Linear equations involving elements from a multiplicative group (such as e.g. S-unit equations) play a vital role and have wide and deep applications in several parts of diophantine number theory. For theoretical results and applications of such and related equations we refer to the papers [2–5,8–9], and the references given there. Combining the underlying theory of such equations and a classical result of van der Waerden [10] about arithmetic progressions, we show that the length of any arithmetic progression consisting of t-term linear combinations of elements from a finitely generated multiplicative group of rank r is bounded in terms of r, t, n, where n is the number of the coefficient t-tuples of the linear combinations.

To formulate our results we need some notation. We follow the paper [5], with slight modifications. Let K be an algebraically closed field of characteristic zero. Write K^* for the multiplicative group of the non-zero elements of K, and let Γ be a multiplicative subgroup of K^* having finite rank r. Let t be a positive integer, and let $\mathcal{A}$ be a finite subset of K^t having n elements. Put

$$H_t(\Gamma, \mathcal{A}) = \left\{ \sum_{i=1}^{t} a_i x_i : (a_1, \dots, a_t) \in \mathcal{A},\ (x_1, \dots, x_t) \in \Gamma^t \right\}.$$

The main result of this paper is the following.

2000 *Mathematics Subject Classification:* 11D57 (11B25). *Key words and phrases:* linear equations in variables from a multiplicative group, S-unit equations, arithmetic progressions, primes. Research supported in part by the János Bolyai Research Fellowship of the Hungarian Academy of Sciences and by the OTKA grants T042985 and T048791.

Theorem 1. *There exists a constant $C(r,t,n)$ depending only on r, t and n such that the length of any non-constant arithmetic progression in $H_t(\Gamma,\mathcal{A})$ is at most $C(r,t,n)$.*

Note that in the upper bound $C(r,t,n)$ none of r,t,n could be omitted. This will be demonstrated by a simple example in Remark 1 after the proof of Theorem 1. Further, at the same place we show that the number of arithmetic progressions in $H_t(\Gamma,\mathcal{A})$ can be infinite, in case of any possible length.

Now as an application, we formulate a result concerning primes represented by sums of integers which are rational S-units. This is motivated by the next problem. M. Pohst asked the following question (oral communication): is it true that every prime can be written in the form $2^u \pm 3^v$, with some non-negative integers u,v? As we will see, by a recent, celebrated result of Green and Tao [7] on arithmetic progressions consisting of primes, this question can be reduced to S-unit equations in a natural way. By the help of Theorem 1 we will provide a negative answer to this question, under much more general circumstances. Note that the theorem would be true under even more general conditions, as well. However, we think that it is not natural to use here more general settings.

To formulate this result, let $S=\{p_1,\dots,p_r\}$ be a (nonempty) set of (positive) primes in $\mathbb{Z}$. As usual, let $\mathbb{Z}_S$ denote the set of those integers, which do not have any prime divisors outside S. In particular, we have $\pm 1\in\mathbb{Z}_S$. Let t be a positive integer and let A be a finite non-empty subset of $\mathbb{Z}^t$. Put

$$H_t(\mathbb{Z}_S,A)=\left\{\sum_{i=1}^{t}a_is_i : (a_1,\dots,a_t)\in A,\ (s_1,\dots,s_t)\in\mathbb{Z}_S^t\right\}.$$

Theorem 2. *For any S, t and A there are infinitely many primes outside the set $H_t(\mathbb{Z}_S,A)$.*

Taking $S=\{2,3\}$, $t=2$ and $A=\{(1,1)\}$, the above theorem yields a negative answer to the problem of M. Pohst. Note that the smallest prime not of the shape $2^u\pm 3^v$ is 53; this fact is demonstrated in Remark 2 after the proof of Theorem 2. We also mention that it is widely believed that there are infinitely many Mersenne-primes, i.e. primes of the shape 2^u-1 ($u\in\mathbb{N}$). As these primes (would) all belong to $H_2(S,A)$ with $S=\{2\}$, $t=2$ and $A=\{(1,1)\}$, we probably cannot claim that $H_t(S,A)$ contains only finitely many primes in general. Hence the theorem seems to be best possible in the qualitative sense.

2. Proofs of the theorems

To prove our theorems, we need several tools. The first one is a deep and general finiteness result for the number of solutions of linear equations involving elements of Γ, due to Evertse, Schlickewei and Schmidt [5].

Keeping the notation from the previous section, consider the equation

$$a_1x_1+\ldots+a_tx_t=1 \tag{1}$$

in $\underline{x}=(x_1,\dots,x_t)\in\Gamma^t$, where $\underline{a}=(a_1,\dots,a_t)\in(K^*)^t$. A solution $\underline{x}$ is called non-degenerate, if no subsum of the left hand side of (1) vanishes, that is $\sum_{i\in I}a_ix_i\neq 0$ for any nonempty subset I of $\{1,\dots,t\}$. The next statement is a simple and immediate consequence of Theorem 1.1 from [5].

Theorem A. *There exists a constant $c_1(r,t)$ depending only on r and t (independent of $\underline{a}$) such that equation (1) has at most $c_1(r,t)$ non-degenerate solutions $\underline{x} \in \Gamma^t$.*

We will also need the following simple and well-known corollary of the above theorem.

Corollary 1. *There exists a constant $c_2(r,t)$ depending only on r and t with the following property. If $(x_1,\dots,x_t) \in \Gamma^t$ is a solution to (1) then $x_i = \alpha_{P(i)} x_i^*$ $(i = 1,\dots,t)$ with some $\alpha_{P(i)}, x_i^* \in \Gamma$, where $(x_1^*,\dots,x_t^*)$ belongs to a set of cardinality at most $c_2(r,t)$. Further, here $P_1,\dots,P_s,P_{s+1}$ is a partition of $\{1,\dots,t\}$, $P(i)$ denotes the class P_l for which $i \in P_l$, and $\alpha_{P_{s+1}} = 1$.*

Proof. Partitioning the sum at the left hand side of (1) into vanishing subsums (the indices in the subsums compose the classes $P_1,\dots,P_s$, respectively) and a subsum yielding 1 (the indices in this subsum compose P_{s+1}) such that none of these subsums has a vanishing subsum, the statement follows from Theorem A by a simple inductive argument. □

The next well-known result from Ramsey theory is due to van der Waerden (cf. [10]). This theorem will be very helpful in taking care of the vanishing subsums in the occurring linear equations of the shape (1).

Theorem B. *For every positive integers k and h there exists a positive integer $W = W(k,h)$ such that for any coloring of the set $\{1,\dots,W\}$ using k colors, we get a non-constant monochromatic arithmetic progression, having at least h terms.*

Finally, in the proof of Theorem 2 we also make use of the following recent deep and celebrated theorem of Green and Tao [7] about arithmetic progressions of primes.

Theorem C. *There are arbitrarily long arithmetic progressions of primes.*

Now we are ready to prove our results.

Proof of Theorem 1. We proceed by induction on t. Let $t = 1$ and take an arbitrary non-empty subset $\mathcal{A}$ of K having n elements. Let $q_1,\dots,q_L$ be a non-constant arithmetic progression in $H_1(\Gamma,\mathcal{A})$; write $q_j = a^{(j)}x^{(j)}$ $(a^{(j)} \in \mathcal{A},\ x^{(j)} \in \Gamma,\ j = 1,\dots,L)$. Without loss of generality we may assume that $0 \notin \mathcal{A}$; otherwise we can give bounds for the lengths of the positive and negative parts of the progression independently, and then simply combine them. Let $d := q_2 - q_1 \neq 0$ denote the common difference of the progression. Subtracting the consecutive terms, we get the equalities

$$(a^{(j+1)}/d)x^{(j+1)} - (a^{(j)}/d)x^{(j)} = 1 \quad (j = 1,\dots,L-1).$$

If $L - 1 > n^2 c_1(r,2)$ then by $|\mathcal{A}| = n$ and the box principle we get that for some $j \in \{1,\dots,L-1\}$ the equation

$$(a^{(j+1)}/d)x_1 - (a^{(j)}/d)x_2 = 1$$

has more than $c_1(r,2)$ solutions in $(x_1,x_2) \in \Gamma^2$. However, by Theorem A this is a contradiction. Hence $L \le C(r,1,n) := n^2 c_1(r,2) + 1$, and the theorem follows for $t = 1$.

Let now t be an arbitrary integer with $t \geq 2$, and assume that the statement is true for $t-1$. That is, the length of any arithmetic progression in $H_{t-1}(\Gamma, \mathcal{B})$ with any non-empty $\mathcal{B} \subseteq K^{t-1}$, $|\mathcal{B}| = m$ is at most $C(r, t-1, m)$ for some constant $C(r, t-1, m)$ depending only on $r, t-1, m$. Further, let $\mathcal{A}$ be a non-empty subset of K^t having n elements, and let $q_1, \dots, q_L$ be a non-constant arithmetic progression in $H_t(\Gamma, \mathcal{A})$. Assume first that $n = 1$. Let $\mathcal{A} = \{(a_1, \dots, a_t)\}$, and put

$$q_j = \sum_{i=1}^{t} a_i x_i^{(j)} \quad (j = 1, \dots, L)$$

where $(x_1^{(j)}, \dots, x_t^{(j)}) \in \Gamma^t$. We have

$$\sum_{i=1}^{t} (a_i/d) x_i^{(j+1)} - \sum_{i=1}^{t} (a_i/d) x_i^{(j)} = 1 \quad (j = 1, \dots, L-1)$$

where $d := q_2 - q_1 \neq 0$ is the common difference of the progression. Note that if $a_1 \dots a_t = 0$ then by the induction step we immediately have $L \leq C(r, t-1, 1)$ and the theorem follows in this case. Otherwise, Corollary 1 implies that for each $j \in \{1, \dots, L-1\}$, $x_i^{(j)}$ is of the form $x_i^{(j)} = \alpha_{P(i)} x_i^*$ with certain $(x_1^*, \dots, x_t^*)$ coming from a finite subset of Γ^t of cardinality bounded by some $c_2(r, t)$ and certain $\alpha_{P(i)} \in \Gamma$ $(i = 1, \dots, t)$. Here $P_1, \dots, P_s, P_{s+1}$ is some partition of the set $\{1, \dots, t\}$, and $P(i)$ denotes the class P_l $(1 \leq l \leq s+1)$ for which $i \in P_l$. Further, P_{s+1} is possibly empty, but otherwise $\alpha_{P_{s+1}} = 1$. Obviously, we have $1 \leq s+1 \leq t$, further $1 \leq s \leq t$ if P_{s+1} is empty. Now we paint the terms q_j $(j = 1, \dots, L-1)$ of the arithmetic progression. We code the colors in the following way. Those q_j will get the same color, where in the above representation the very same partition of the indices $\{1, \dots, t\}$ occurs, moreover, the "parameter t-tuples" $(x_1^*, \dots, x_t^*)$ also coincide. That is, q_{j_1} and q_{j_2} will get the same color if and only if we have

$$(x_1^{(j_1)}, \dots, x_t^{(j_1)}) = (\alpha_{P(1)} x_1^*, \dots, \alpha_{P(t)} x_t^*)$$

and

$$(x_1^{(j_2)}, \dots, x_t^{(j_2)}) = (\alpha'_{P(1)} x_1^*, \dots, \alpha'_{P(t)} x_t^*)$$

with the same partition $P_1, \dots, P_s, P_{s+1}$, the same $(x_1^*, \dots, x_t^*) \in \Gamma^t$, and some $\alpha_{P(1)}, \dots, \alpha_{P(t)}, \alpha'_{P(1)}, \dots, \alpha'_{P(t)} \in \Gamma$. Observe that by Corollary 1 and elementary combinatorics, the number of colors is bounded by some constant $c_3(r, t)$ depending only on r and t. Take $k = c_3(r, t)$ and $h = C(r, t-1, 1) + 1$. Suppose that $L - 1 \geq W(k, h)$. Then by Theorem B we find that there exists a monochromatic arithmetic progression in $H_t(\Gamma, \mathcal{A})$ corresponding to the above coloring, of length $C(r, t-1, 1) + 1$. If this subprogression corresponds to a case where P_{s+1} is non-empty, then observe that in each corresponding q_j the very same constant $\sum_{P(i)=P_{s+1}} a_i x_i^*$ occurs. Cancelling this constant from each term of the subprogression, we get an arithmetic progression in $H_{t-1}(\Gamma, \mathcal{A}')$ (with the appropriate one-elemented $\mathcal{A}'$) of length $C(r, t-1, 1) + 1$, which is a contradiction. Suppose now that P_{s+1} is empty. Observe that in this case $s < t$ must be valid. Hence there exists a class, say P_1

with at least two members. However, then writing $b_l = \sum_{P(i)=P_l} a_i x_i^*$ $(l = 1, \dots, s)$ the representation

$$q_j = \sum_{l=1}^{s} b_l \alpha_{P_l}$$

belongs to $H_{t-1}(\Gamma, \{\underline{b}\})$, with $\underline{b} = (b_1, \dots, b_s, 0 \dots, 0) \in K^{t-1}$. Hence we get an arithmetic progression in the latter set, of length $C(r, t-1, 1) + 1$, which is a contradiction again. As there are now more cases to distinguish, we get that $L \leq C(r, t, 1) := W(k, h)$ must be valid. Hence the theorem follows in this case.

Finally, consider the general case, i.e. with a non-empty $\mathcal{A} \subseteq K^t$, $|\mathcal{A}| = n$, and let $q_1, \dots, q_L$ be a non-constant arithmetic progression in $H_t(\Gamma, \mathcal{A})$. Paint q_j $(j = 1, \dots, L)$ with a color corresponding to that $\underline{a} \in \mathcal{A}$ which belongs to the representation of q_j. Let $k = n$ and $h = C(r, t, 1) + 1$. Applying Theorem B we get that if $L \geq W(k, h)$, then there exists a monochromatic subprogression of the original arithmetic progression of length at least $C(r, t, 1) + 1$. As in this subprogression the terms correspond to the same $\underline{a} \in \mathcal{A}$, this is a contradiction. Hence $L \leq C(r, t, n) := W(k, h) - 1$, and the theorem follows. □

Remark 1. As we mentioned in the introduction, in the upper bound $C(r, t, n)$ none of r, t, n could be omitted. To see this, for simplicity take $K = \mathbb{Q}$. First let t be arbitrary but fixed, take $\Gamma = \{-1, 1\}$ and let $\mathcal{A} = \{(1, \dots, 1)\}$. As the arithmetic progression $-t, -t+2, \dots, t-2, t$ belongs to $H_t(\Gamma, \mathcal{A})$, the dependence on t is necessary. Let now $t = 1$, and take an arbitrary positive integer k. Choosing either $\Gamma = \{1\}$ and $\mathcal{A} = \{1, \dots, k\}$ or $\Gamma = U_S$ with $S = \{p : p \text{ is prime and } p \mid k!\}$ (for the notation see the proof of Theorem 2 below) and $\mathcal{A} = \{1\}$, in both cases we get that the arithmetic progression $1, \dots, k$ belongs to $H_t(\Gamma, \mathcal{A})$. This shows that the dependence on both r and n is necessary, as well.

Further, in general it is not possible to give a bound for the *number* of progressions in $H_t(\Gamma, \mathcal{A})$. Indeed, take $K = \mathbb{Q}$, $S = \{2\}$ and let $\Gamma = U_S$. Setting $\mathcal{A} = \{0, 1\}$ we see that $0, 2^u, 2^{u+1}$ is an arithmetic progression in $H_1(\Gamma, \mathcal{A})$ for any $u \in \mathbb{N}$. To get a "non-trivial" example, observe that $1, 2^u + 1, 2^{u+1} + 1$ is an arithmetic progression consisting of pairwise relatively prime terms in $H_2(\Gamma, \mathcal{A})$, for any $u \in \mathbb{N}$. In general, take arbitrary K, Γ, t and $\mathcal{A}$, and suppose that $q_1, \dots, q_L$ is an arithmetic progression in $H_t(\Gamma, \mathcal{A})$. Then $q_1 + x, \dots, q_L + x$ is an arithmetic progression in $H_{t+1}(\Gamma, \mathcal{A}')$ with any $x \in \Gamma$, where $\mathcal{A}'$ is chosen accordingly. This shows that $H_t(\Gamma, \mathcal{A})$ can contain infinitely many arithmetic progressions in general.

Proof of Theorem 2. Let t and S be fixed, and let A be a non-empty subset of $\mathbb{Z}^t$ with $|A| = n$. As is well-known, taking $K = \mathbb{Q}$ and

$$U_S = \{p/q : p, q \in \mathbb{Z} \setminus \{0\},\ \gcd(p, q) = 1,\ pq \in \mathbb{Z}_S\},$$

U_S is a finitely generated multiplicative subgroup of $\mathbb{Q}^*$ (with $\mathbb{Z}_S \subseteq U_S$), of rank $r = |S|$. Further, Theorem C obviously implies that there are infinitely many pairwise disjoint arithmetic progressions of primes of length $C(r, t, n) + 1$ (where $C(r, t, n)$ is specified in Theorem 1). As by Theorem 1 each such progression contains a prime outside $H_t(U_S, A)$, the statement follows. □

Remark 2. The smallest prime yielding a negative answer to the problem of M. Pohst is 53. This can be seen as follows. On the one hand, it is easy to check that all

the smaller primes can be represented in the desired form, with "small" u, v. (The "largest" decomposition is given by $2^7 - 3^4 = 47$.) On the other hand, if 53 is of the shape $2^u \pm 3^v$, then we have $2^\alpha y^2 = 3^\beta x^3 + 53$ with $\alpha \in \{0, 1\}$ and $\beta \in \{0, 1, 2\}$ where $\pm x$ and y are powers of 3 and 2, respectively. However, a simple computation with Magma (see [1]) gives that these elliptic equations have no solutions of the required shape, and our claim follows. Note that as these equations can be easily transformed into Mordell equations, their solutions are already known from [6].

3. Acknowledgement

The author is grateful to A. Pethő for letting him know about the problem of M. Pohst, and for his encouragement.

References

[1] J. Cannon et al., *The Magma computational algebra system*, http://magma.maths.usyd.edu.au.
[2] J.-H. Evertse, K. Győry, *On unit equations and decomposable form equations*, J. Reine Angew. Math. **358** (1985), 6–19.
[3] J.-H. Evertse, K. Győry, C. Stewart, R. Tijdeman, *S-unit equations and their applications*, New Advances in Transcendence Theory (A. Baker, ed.), Cambridge University Press, Cambridge, 1988, pp. 110–174.
[4] J.-H. Evertse, H. P. Schlickewei, *The absolute subspace theorem and linear equations with unknowns from a multiplicative group*, Number theory in progress, Vol. 1 (Zakopane-Kościelisko, 1997), de Gruyter, Berlin, 1999, pp. 121–142.
[5] J.-H. Evertse, H. P. Schlickewei, W. M. Schmidt, *Linear equations in variables which lie in a multiplicative group*, Annals Math. **155** (2002), 807–836.
[6] J. Gebel, A. Pető, H. G. Zimmer, *On Mordell's equation*, Compositio Math. **110** (1998), 335-367.
[7] B. Green, T. Tao, *The primes contain arbitrarily long arithmetic progressions*, arXiv:math.NT/0404188 **v5** (9 Feb 2006), 56 pp.
[8] K. Győry, *Some recent applications of S-unit equations*, Astérisque **209** (1992), 17–38.
[9] K. Győry, *Solving Diophantine equations by Baker's theory*, A panorama of number theory or the view from Baker's garden (Zürich, 1999), Cambridge Univ. Press, Cambridge, 2002, pp. 38–72.
[10] B. L. van der Waerden, *Beweis einer Baudetschen Vermutung*, Nieuw Archief voor Wiskunde **19** (1927), 212–216.

L. Hajdu
Number Theory Research Group
of the Hungarian Academy of Sciences, and
Institute of Mathematics
University of Debrecen
P.O. Box 12
4010 Debrecen
Hungary
E-mail address:
hajdul@math.klte.hu

III.2 [BHP]: Arithmetic progressions in the solution sets of norm form equations

Rocky Mountain J. Math. (közlésre elfogadva).

ARITHMETIC PROGRESSIONS IN THE SOLUTION SETS OF NORM FORM EQUATIONS

ATTILA BÉRCZES, LAJOS HAJDU, AND ATTILA PETHŐ

1. Introduction

Let K be an algebraic number field of degree k, and let $\alpha_1, \ldots, \alpha_n$ be linearly independent elements of K over $\mathbb{Q}$. Denote by $D \in \mathbb{Z}$ the common denominator of $\alpha_1, \ldots, \alpha_n$ and put $\beta_i = D\alpha_i$ $(i = 1, \ldots, n)$. Note that $\beta_1, \ldots, \beta_n$ are algebraic integers of K. Let m be a non-zero integer and consider the norm form equation

$$N_{K/\mathbb{Q}}(x_1\alpha_1 + \ldots + x_n\alpha_n) = m \tag{1.1}$$

in integers $x_1, \ldots, x_n$. Let H denote the solution set of (1.1) and $|H|$ the size of H. Note that if the $\mathbb{Z}$-module generated by $\alpha_1, \ldots, \alpha_n$ contains a submodule, which is a full module in a subfield of $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ different from the imaginary quadratic fields and $\mathbb{Q}$, then this equation can have infinitely many solutions (see e.g. Schmidt [19]). Various arithmetical properties of the elements of H were studied in [11] and [8]. In the present paper we are concerned with arithmetical progressions in H. Arranging the elements of H in an $|H| \times n$ array $\mathcal{H}$, one may ask at least two natural questions about arithmetical progressions appearing in H. The "horizontal" one: do there exist infinitely many rows of $\mathcal{H}$, which form arithmetic progressions; and the "vertical" one: do there exist arbitrary long arithmetic progressions in some column of $\mathcal{H}$? Note that the first question is meaningful only if $n > 2$.

The "horizontal" problem was treated by Bérczes and Pethő [4] by proving that if $\alpha_i = \alpha^{i-1}$ $(i = 1, \ldots, n)$ then in general $\mathcal{H}$ contains only finitely many effectively computable "horizontal" AP's and they were able to localize the possible exceptional cases. Later Bérczes and Pethő [5], Bérczes Pethő and Ziegler [6] and Bazsó [2] computed all horizontal AP's in the solution sets of norm form equations corresponding to the fields generated by the polynomials $x^n - a, 2 \leq a \leq 100$, $x^3 - (a-1)x^2 - (a+2)x - 1, a \in \mathbb{Z}$ and $x^n + a, 2 \leq a \leq 100$, respectively.

2000 Mathematics Subject Classification: 11D57, 11D45, 11B25.

Keywords and Phrases: norm form equations, arithmetic progressions.

The research was supported in part by grants T48791 and T67580 of the Hungarian National Foundation for Scientific Research, the János Bolyai Research Fellowship of the Hungarian Academy of Sciences, and by the National Office for Research and Technology.

For quadratic norm form equations, which are called Pell equations if K is a real quadratic field, only the "vertical" problem is interesting. In this direction Pethő and Ziegler [18] proved among others that the length of the "vertical" AP's in $\mathcal{H}$ is bounded by a constant, which depends on the coefficients of the (quadratic) form and on m. On the other hand, they proved that every three term AP occurs in the second column of infinitely many $\mathcal{H}$. Dujella, Pethő and Tadić [7] was able to extend this result to four term AP's.

The main goal of the present paper is to generalize the result of Pethő and Ziegler [18] to arbitrary norm form equations. In the sequel *AP in H* always means a "vertical" arithmetical progression belonging to $\mathcal{H}$. A sequence in H, with the property that all the corresponding coordinate sequences form "vertical" AP's, will be called an *algebraic AP in H*.

2. Results

Now we summarize our main results.

Theorem 2.1. *Let $(x_1^{(j)}, \dots, x_n^{(j)})$ $(j = 1, \dots, t)$ be a sequence of distinct elements in H such that $x_i^{(j)}$ is an arithmetic progression for some $i \in \{1, \dots, n\}$. Then we have $t \leq c_1$, where $c_1 = c_1(k, m, D)$ is an explicitly computable constant.*

Theorem 2.2. *The set H contains at most c_3 arithmetic progressions of the form $\underline{x} + k\underline{d}$ $(k = -1, 0, 1)$. Here $c_3 = c_3(k, m, D)$ is an explicitly computable constant, $\underline{x} = (x_1, \dots, x_n)$, d is a non-zero integer, and $\underline{d}$ is the n-tuple with all entries equal to d.*

By Theorem 2.1 the length of any AP in H is bounded. In the particular case $k = 2$, H does not contain any algebraic AP (see Pethő and Ziegler [18]). However, it is not possible to give a bound for the number of AP-s in H for $k \geq 3$. It is demonstrated by the following example. Let $P(x) = x(x-1)\dots(x-k+1)+(-1)^k$ and denote by α one of its roots. It was proved in [14] (Lemma 2.2, see also [1, 13] and [17]), that $P(x)$ is irreducible and the conjugates of α are $\alpha+1, \dots, \alpha+k-1$. Thus these k numbers are units of norm 1 in the algebraic number field $\mathbb{Q}(\alpha)$, moreover they form an AP of length k. If μ is an algebraic integer in $\mathbb{Q}(\alpha)$ of norm m then $\mu\alpha, \mu(\alpha+1), \dots, \mu(\alpha+k-1)$ also have norm m, and form an AP of length k.

The next theorem shows that in general if H contains algebraic AP-s at all, then it contains infinitely many.

Theorem 2.3. *Suppose that $n = k \geq 3$. Let $t \geq 3$ be an integer. If H contains a non-constant t-term algebraic AP, then it contains infinitely many.*

Now we prove that the algebraic AP's from the example before Theorem 2.3 are the longest ones. More precisely, we have the following theorem.

Theorem 2.4. *Let K be an algebraic number field of degree k. Assume that $\alpha_1, \dots, \alpha_t \in K$ have the same field norm and form a non-trivial AP. Then $t \le k$.*

Remark. We note that M. Newman ([16], see also [17]) proved that the length of arithmetic progressions consisting of units of an algebraic number field of degree k is at most k. Theorem 2.4 is a generalization of his result.

To formulate the next result, for a non-zero integer a let $\omega(a)$ denote the number of prime divisors of a, and for a prime p denote by $\mathrm{ord}_p(a)$ the highest exponent u such that p^u divides a.

Theorem 2.5. *Suppose that the Galois group of the normal closure of K is doubly transitive. Then the number of those solutions $(x_1, \dots, x_n)$ of equation (1.1), for which there exists another solution $(y_1, \dots, y_n) \neq (x_1, \dots, x_n)$, such that $\prod_{i=1}^{n}(x_i - y_i) = 0$, is bounded by*

$$\Psi(k, n, mD^k) \exp\left(k(12n)^{6n}\right)$$

where

$$\Psi(k, n, mD^k) := \binom{k}{n-1}^{\omega(mD^k)} \cdot \prod_{\substack{p \mid m \\ p \text{ prime}}} \binom{\mathrm{ord}_p(mD^k) + n - 1}{n-1}.$$

Theorem 2.6. *Let S be a set of s rational primes, and let T be the set of integers without prime divisors outside S. Suppose that the Galois group of the normal closure of K is doubly transitive. Then the number of those solutions $(x_1, \dots, x_n)$ of equation (1.1), for which there exists another solution $(y_1, \dots, y_n) \neq (x_1, \dots, x_n)$, such that $x_i - y_i \in T$ for some $i \in \{1, \dots, n\}$, is bounded by*

$$\Psi(k, n, mD^k) \cdot \exp\left((s+k)(12n)^{6n+3}\right),$$

where Ψ is the function defined in Theorem 2.5.

Remark. By the help of Theorems 2.5 and 2.6 one can easily give a bound for the number of sequences $\mathbf{x}_j = (x_1^{(j)}, \dots, x_n^{(j)}) \in H$ such that one of the coordinates of $\mathbf{x}_j$ forms an arithmetic progression whose difference is zero or is an S-unit, respectively.

3. Auxiliary results

In this section we present some lemmas which will be needed in the proofs of our theorems. For this purpose we need to introduce some notation. Let L be a number field of degree l and denote by U_L the unit group of L. The next statement is an immediate consequence of

a result of Hajdu [12]. Note that a similar result was independently proved by Jarden and Narkiewicz [15]

Lemma 3.1. *Let n be an integer and let A be a finite subset of L^n. There exists a constant $C_1 = C_1(l, n, |A|)$ such that the length of any non-constant arithmetic progression in the set*

$$\left\{ \sum_{i=1}^{n} a_i y_i : (a_1, \dots, a_n) \in A,\ (y_1, \dots, y_n) \in U_L^n \right\}$$

is at most C_1.

For some other arithmetical properties of the set occurring in Lemma 3.1, see [11].

Let K be a number field of degree k, $\alpha_1, \dots, \alpha_n$ linearly independent algebraic integers in K, $m \in \mathbb{Z}$, and $\lambda \in K$. Consider now the equation

$$N_{K/\mathbb{Q}}(\alpha_1 x_1 + \cdots + \alpha_n x_n + \lambda) = m \quad \text{in} \quad x_1, \dots, x_n \in \mathbb{Z}. \tag{3.2}$$

The next lemma is a special case of Corollary 8 of [3].

Lemma 3.2. *Suppose that $\alpha_1, \dots, \alpha_n$ and λ are linearly independent over $\mathbb{Q}$. Then the number of solutions of equation (3.2) does not exceed the bound*

$$\left(2^{17}k\right)^{\left(\frac{2}{3}(n+1)(n+2)(2n+3)-4\right)(\omega(m)+1)}.$$

Let F be an algebraically closed field of characteristic 0. Write F^* for the multiplicative group of nonzero elements of F, and let $(F^*)^n$ be the direct product consisting of n-tuples $\mathbf{x} = (x_1, \dots, x_n)$ with $x_i \in F^*$ for $i = 1, \dots, n$. For $x, y \in (F^*)^n$ write $x * y = (x_1 y_1, \dots, x_n y_n)$. Let Γ be a subgroup of $(F^*)^n$ and suppose that $(a_1, \dots, a_n) \in (F^*)^n$. Consider the so-called generalized unit equation

$$a_1 x_1 + \ldots + a_n x_n = 1 \tag{3.3}$$

in $\mathbf{x} = (x_1, \dots, x_n) \in \Gamma$. A solution $\mathbf{x}$ is called non-degenerate, if no subsum of the left hand side of (3.3) vanishes, that is $\sum_{i \in I} a_i x_i \neq 0$ for any nonempty subset I of $\{1, \dots, n\}$. The next lemma is Theorem 1.1 of Evertse, Schlickewei and Schmidt [10].

Lemma 3.3. *Suppose that Γ has finite rank r. Then the number of non-degenerate solutions $\mathbf{x} \in \Gamma$ of equation (3.3) is bounded by*

$$\exp\left((6n)^{3n}(r+1)\right).$$

Let $\mathcal{M}$ be the $\mathbb{Z}$-module generated by the elements $\alpha_1, \dots, \alpha_n$. Clearly, equation (1.1) can be transformed to the equation

$$N_{K/\mathbb{Q}}(\delta) = m \quad \text{in} \quad \delta \in \mathcal{M}. \tag{3.4}$$

Lemma 3.4. *The set of solutions of (3.4) is contained in some union* $\delta_1\mathcal{O}_K^* \cup \cdots \cup \delta_t\mathcal{O}_K^*$, *where*

$$t \le \Psi(k,n,m) = \binom{k}{n-1}^{\omega(m)} \cdot \prod_{\substack{p\mid m\\ p \text{ prime}}} \binom{\operatorname{ord}_p(m)+n-1}{n-1}$$

and $\delta_1, \ldots, \delta_t$ *are solutions of (3.4).*

Proof. This is a special case of Lemma 4 of [9]. □

4. Proofs

Proof of Theorem 2.1. Recall that H is the solution set of (1.1), D is the common denominator of $\alpha_1, \ldots, \alpha_n$, and $\beta_i = D\alpha_i$ $(i = 1, \ldots, n)$.

Suppose first that we have a non-constant sequence $(x_1^{(j)}, \ldots, x_n^{(j)})$ $(j = 1, \ldots, t)$ in H such that $x_i^{(j)}$ is constant for some $i \in \{1, \ldots, n\}$. Let $\lambda := x_i^{(j)} \cdot \beta_i$. Then equation (1.1) is of the shape (3.2) and by Lemma 3.2 we see that the number of such solutions of (1.1) (i.e. t) is bounded by

$$\left(2^{17}k\right)^{\left(\frac{2}{3}n(n+1)(2n+1)-4\right)(\omega(mD^k)+1)} \le c_1(k,m,D).$$

Assume next that $(x_1^{(j)}, \ldots, x_n^{(j)}) \in H$ for $j = 1, \ldots, t$ such that $x_i^{(j)}$ forms a non-constant arithmetic progression for some $i \in \{1, \ldots, n\}$. Writing $\sigma_1, \ldots, \sigma_k$ for the isomorphisms of K into $\mathbb{C}$, for $u = 1, \ldots, k$ we have

$$x_1\sigma_u(\beta_1) + \ldots + x_n\sigma_u(\beta_n)\sigma_u(\varepsilon)\sigma_u(\mu)$$

where μ is an element of norm mD^k and ε is a unit in the $\mathbb{Z}$-module $\mathbb{Z}[\beta_1, \ldots, \beta_n]$. By Lemma 3.4 μ can be chosen from a set having at most $\Psi(k,n,mD^k)$ elements. Consider a fixed value of μ. Choose the order of the isomorphisms $\sigma_1, \ldots, \sigma_k$ such that the matrix

$$B \begin{pmatrix} \sigma_1(\beta_1) & \ldots & \sigma_1(\beta_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(\beta_1) & \ldots & \sigma_n(\beta_n) \end{pmatrix} \tag{4.5}$$

has non-zero determinant. Hence we have

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = B^{-1} \begin{pmatrix} \sigma_1(\varepsilon)\sigma_1(\mu) \\ \vdots \\ \sigma_n(\varepsilon)\sigma_n(\mu) \end{pmatrix}. \tag{4.6}$$

Writing

$$B^{-1} \begin{pmatrix} \gamma_{11} & \cdots & \gamma_{1n} \\ \vdots & \ddots & \vdots \\ \gamma_{n1} & \cdots & \gamma_{nn} \end{pmatrix} \tag{4.7}$$

we get

$$x_i = a_{i1}y_1 + \ldots + a_{in}y_n$$

for all $i = 1, \dots, n$, where $a_{ih} = \gamma_{ih}\sigma_h(\mu)$ and $y_h = \sigma_h(\varepsilon)$ for $h = 1, \dots, n$. Noting that the y_h $(h = 1, \dots, n)$ are units in the splitting field L of K, and $\deg(L) \leq k!$, using $n \leq k$ the theorem follows from Lemma 3.1. □

Proof of Theorem 2.2. Obviously, in view of Theorem 2.1 it is sufficient to give an upper bound for the number of three-term progressions in H. For this purpose, assume that $(x_1, \dots, x_n)$ is the middle term of a three-term arithmetic progression in H, with common difference $d\underline{1}$. Denote by U_K the unit group of the ring of algebraic integers of the field K. Put

$$\mu_{\pm 1} = (x_1 \pm d)\beta_1 + \ldots + (x_n \pm d)\beta_n \text{ and } \mu_0 = x_1\beta_1 + \ldots + x_n\beta_n.$$

Note that $N_{K/\mathbb{Q}}(\mu_{-1}) = N_{K/\mathbb{Q}}(\mu_0) = N_{K/\mathbb{Q}}(\mu_1) = mD^k$, and further that $\mu_h = \varepsilon_h\mu_h^*$ $(h = -1, 0, 1)$ where $\varepsilon_{-1}, \varepsilon_0, \varepsilon_1 \in U_K$ and $\mu_{-1}^*, \mu_0^*, \mu_1^*$ belong to a finite set whose cardinality is bounded in terms of k, m, D. Thus we have

$$\mu_{-1}^*\varepsilon_{-1} - 2\mu_0^*\varepsilon_0 + \mu_1^*\varepsilon_1 = 0.$$

Hence Lemma 3.3 implies that

$$(\varepsilon_{-1}, \varepsilon_0, \varepsilon_1) = \varepsilon(\varepsilon_{-1}^*, \varepsilon_0^*, \varepsilon_1^*)$$

with some $\varepsilon \in U_K$, where $(\varepsilon_{-1}^*, \varepsilon_0^*, \varepsilon_1^*)$ belongs to a finite subset of U_K^3, of cardinality bounded by some constant depending only on k, m, D. Thus we conclude that

$$\mu_h = \varepsilon\lambda_h \quad (h = -1, 0, 1)$$

holds, where $\varepsilon \in U_K$ and $\lambda_{-1}, \lambda_0, \lambda_1$ belong to a finite set of cardinality depending only on k, m, D again. Observe that $d = \varepsilon(\lambda_1 - \lambda_0)$ holds, and further that this d can be rational for at most one choice of $\varepsilon \in U_K$ (up to a factor -1), for any fixed $(\lambda_{-1}, \lambda_0, \lambda_1)$. Hence the theorem follows. □

Proof of Theorem 2.3. Suppose that $(x_1^{(j)}, \dots, x_n^{(j)})$ $(j = 1, \dots, t)$ is a non-constant algebraic AP in H. Let ε be an arbitrary unit in $\mathbb{Z}[\beta_1, \dots, \beta_n]$ of norm 1, and define $(y_1^{(j)}, \dots, y_n^{(j)})$ by

$$y_1^{(j)}\beta_1 + \ldots + y_n^{(j)}\beta_n = \varepsilon(x_1^{(j)}\beta_1 + \ldots + x_n^{(j)}\beta_n) \text{ for } j = 1, \dots, t.$$

Obviously, then $(y_1^{(j)}, \dots, y_n^{(j)})$ $(j = 1, \dots, t)$ is a non-constant algebraic AP in H. As there are infinitely many units in $\mathbb{Z}[\beta_1, \dots, \beta_n]$ of norm 1, the theorem follows. □

Proof of Theorem 2.4. Denote by m the common norm of $\alpha_1, \dots, \alpha_t$. As these numbers form an AP, we have $\alpha_i = \alpha_1 + (i-1)(\alpha_2 - \alpha_1), i = 1, \dots, t$. This implies $\frac{\alpha_i}{\beta} = \frac{\alpha_1}{\beta} + i - 1$ with $\beta = \alpha_2 - \alpha_1$. Put M for the norm of β and $P(x) = x^u + p_{u-1}x^{u-1} + \cdots + p_0, p_j \in \mathbb{Q}$ for the minimal polynomial of $\frac{\alpha_1}{\beta}$. It is well known that the defining polynomial of $\frac{\alpha_1}{\beta}$ is a power of its minimal polynomial, i.e. $u|k$ and $p_0^{k/u} = (-1)^k m/M$.

If $k = u$ then we even have $p_0 = (-1)^k m/M$ otherwise, because both p_0 and m/M are rational numbers, there are at most two possibilities for p_0, which differ from each other only in their sign.

Consider the polynomials $P_i(x) = P(x-(i-1)), i = 1, \ldots, t$. They are with $P(x)$ irreducible and we have

$$P_i\left(\frac{\alpha_i}{\beta}\right) = P\left(\frac{\alpha_i}{\beta} - (i-1)\right) P\left(\frac{\alpha_1}{\beta}\right) = 0,$$

i.e. $\frac{\alpha_i}{\beta}$ is a root of $P_i(x)$, which together with the irreducibility of $P_i(x)$ implies that it is the minimal polynomial of $\frac{\alpha_i}{\beta}$. Thus its constant term is equal to p_0 if $k = u$ and may differ from p_0 only in its sign, otherwise. Hence $P(-i+1), i = 1, \ldots, t$ is constant if $k = u$ or can assume only at most two different values. If $k = u$ this implies $P(x) = x(x-1)\ldots(x-t+1) + p_0$ and we have $t \le k$ as stated. If $u < k$ then there exists a subset $I \subseteq \{1, \ldots, t\}$ of size $|I| \ge t/2$ such that $P(-i+1)$ takes the same value for all $i \in I$. By the theory of interpolation the degree of P must be at least $|I|$, i.e. $u \ge |I| \ge t/2$. On the other hand, $u < k$ and $u|k$ imply $u \le k/2$. ¿From the last two inequalities we get $t \le k$ in this case, too. □

Proof of Theorem 2.5. We shall bound the number of those solutions of equation (1.1), for which there exists a solution $(y_1, \ldots, y_n) \ne (x_1, \ldots, x_n)$ with $x_i = y_i$ for some $i \in \{1, \ldots, n\}$. Now equation (1.1) means that

$$\beta_1 x_1 + \beta_2 x_2 + \cdots + \beta_n x_n = \mu_1 \varepsilon_1 \tag{4.8}$$

and

$$\beta_1 y_1 + \beta_2 y_2 + \cdots + \beta_n y_n = \mu_2 \varepsilon_2 \tag{4.9}$$

where μ_1, μ_2 are elements of norm mD^k and $\varepsilon_1, \varepsilon_2$ are units in the $\mathbb{Z}$-module generated by $\beta_1, \ldots, \beta_n$. By Lemma 3.4 both μ_1 and μ_2 can be chosen from a set having at most $\Psi(k, n, mD^k)$ elements. Consider fixed values of μ_1 and μ_2. Denote again by $\sigma_1, \ldots, \sigma_k$ the isomorphic embeddings of K into $\mathbb{C}$, choosing their order such that the matrix B in (4.5) has nonzero determinant. Using (4.7), equation (4.8) leads to equation (4.6). This means that

$$x_i = \sum_{j=1}^{n} \gamma_{ij} \sigma_j(\mu_1) \sigma_j(\varepsilon_1). \tag{4.10}$$

Similarly, using equation (4.9) we can show that

$$y_i = \sum_{j=1}^{n} \gamma_{ij} \sigma_j(\mu_2) \sigma_j(\varepsilon_2). \tag{4.11}$$

One can easily check that $\gamma_{ij} \ne 0$ for at least two indices $j \in \{1, \ldots, n\}$. Thus without loss of generality we may assume that $\gamma_{i1}, \ldots, \gamma_{iN}$ are

non-zero and $\gamma_{i,N+1} = \cdots = \gamma_{in} = 0$, for some $2 \leq N \leq n$. Now subtracting equations (4.10) and (4.11) we get

$$\sum_{j=1}^{N} (\gamma_{ij}\sigma_j(\mu_1)\sigma_j(\varepsilon_1) - \gamma_{ij}\sigma_j(\mu_2)\sigma_j(\varepsilon_2)) = 0. \tag{4.12}$$

This is a homogeneous unit equation consisting of $2N$ terms. We shall bound the number of solutions of this equation. First we count the non-degenerate solutions of (4.12). Dividing the equation by the last term we obtain

$$\sum_{j=1}^{N-1} \left(\frac{\gamma_{ij}\sigma_j(\mu_1)}{\gamma_{in}\sigma_N(\mu_2)} \frac{\sigma_j(\varepsilon_1)}{\sigma_N(\varepsilon_2)} - \frac{\gamma_{ij}\sigma_j(\mu_2)}{\gamma_{iN}\sigma_N(\mu_2)} \frac{\sigma_j(\varepsilon_2)}{\sigma_N(\varepsilon_2)} \right) + \frac{\sigma_N(\mu_1)}{\sigma_N(\mu_2)} \frac{\sigma_N(\varepsilon_1)}{\sigma_N(\varepsilon_2)} = 1, \tag{4.13}$$

which is an inhomogeneous unit equation having $2N-1$ terms. We easily see that all solutions to this equation are contained in the subgroup

$$\Gamma = \left\{ \left(\frac{\sigma_1(\varepsilon_1)}{\sigma_N(\varepsilon_2)}, \frac{\sigma_1(\varepsilon_2)}{\sigma_N(\varepsilon_2)}, \frac{\sigma_2(\varepsilon_1)}{\sigma_N(\varepsilon_2)}, \frac{\sigma_2(\varepsilon_2)}{\sigma_N(\varepsilon_2)}, \ldots, \frac{\sigma_N(\varepsilon_1)}{\sigma_N(\varepsilon_2)} \right) \mid \varepsilon_1, \varepsilon_2 \in \mathcal{O}_K^* \right\}$$

of $(\mathbb{C}^*)^{2N-1}$. Clearly, this group has rank at most $2r_K$, where r_K is the unit rank of the field K. Indeed, if $\eta_1, \ldots, \eta_{r_K}$ denotes a fundamental system of units in K then, the subgroup Γ_0 of $(\mathbb{C}^*)^{2N-1}$, generated by the vectors

$$\mathbf{a}_j = (\sigma_1(\eta_j), 1, \sigma_2(\eta_j), 1, \ldots, 1, \sigma_N(\eta_j)) \quad (j = 1, \ldots, r_K),$$

and

$$\mathbf{b}_i = \left(\frac{1}{\sigma_N(\eta_j)}, \frac{\sigma_1(\eta_j)}{\sigma_N(\eta_j)}, \frac{1}{\sigma_N(\eta_j)}, \frac{\sigma_2(\eta_j)}{\sigma_N(\eta_j)}, \ldots, \frac{\sigma_{N-1}(\eta_j)}{\sigma_N(\eta_j)}, \frac{1}{\sigma_N(\eta_j)} \right) \ (j = 1, \ldots, r_K)$$

has rank at most $2r_K$. Further, the factor group Γ/Γ_0 is a torsion group. This means that the solutions of equation (4.13) belong to a subgroup of rank at most of $2k-2$ of $(\mathbb{C}^*)^{2N-1}$. Thus, $\frac{\sigma_1(\varepsilon_1)}{\sigma_N(\varepsilon_2)}$ is contained in a set of at most

$$\exp\left((12N-6)^{6N-3}(2k-1)\right)$$

elements. Fix now such a value. Then using that the Galois group of K is doubly transitive, we see that $\frac{\sigma_l(\varepsilon_1)}{\sigma_j(\varepsilon_2)}$ is also fixed for each $j, l \in \{1, \ldots, k\}$. By multiplying the ratios $\frac{\sigma_1(\varepsilon_1)}{\sigma_j(\varepsilon_2)}$ for $j \in \{1, \ldots, k\}$ and using that $\prod_{j=1}^{k} \sigma_j(\varepsilon_2) = \pm 1$ we get that ε_1 may assume at most $2k$ values. Similarly, ε_2 may assume at most $2k$ values. These altogether show that the number of non-degenerate solutions of equation (4.12) is bounded by

$$\exp\left((12N-6)^{6N-2}(4k-2)\right). \tag{4.14}$$

Now we have to estimate the number of degenerate solutions of (4.12), too. If $\gamma_{ij}\sigma_j(\mu_1)\sigma_j(\varepsilon_1) - \gamma_{ij}\sigma_j(\mu_2)\sigma_j(\varepsilon_2) = 0$ for all $j \in \{1, \ldots, N\}$

then we get that $\sigma_l(\mu_1)\sigma_l(\varepsilon_1)\sigma_l(\mu_2)\sigma_l(\varepsilon_2)$ for some $l \in \{1,\dots,N\}$ and thus $\mu_1\varepsilon_1 = \mu_2\varepsilon_2$. Now subtracting equations (4.8) and (4.9) and using that $\beta_1,\dots,\beta_n$ are linearly independent, we get that $x_j = y_j$ for all $j \in \{1,\dots,n\}$, which is a contradiction. Thus we must have one of the following two cases:

(i) Equation (4.12) has a minimal vanishing sub-sum (i.e. a sub-sum with no further vanishing sub-sums) which contains both $\sigma_j(\varepsilon_1)$ and $\sigma_l(\varepsilon_2)$ for some $j \neq l$, $j,l \in \{1,\dots,N\}$. Similarly to the case of the non-degenerate solutions we can prove that the number of solutions of (4.12) is bounded by the expression in (4.14).

(ii) Equation (4.12) has both a minimal vanishing sub-sum which contains $\sigma_j(\varepsilon_1)$ and $\sigma_l(\varepsilon_1)$ for some $j \neq l$, $j,l \in \{1,\dots,N\}$, and a minimal vanishing sub-sum which contains $\sigma_u(\varepsilon_2)$ and $\sigma_v(\varepsilon_2)$ for some $u \neq v$, $u,v \in \{1,\dots,N\}$. Further, these vanishing sub-sums contain at most N terms. Thus we infer again a much better bound than the bound (4.14) on the number of solutions in this case.

Finally, we have 2^{2N-1} possibilities for choosing the considered sub-sums, so altogether the number of solutions $(\varepsilon_1,\varepsilon_2)$ of equation (4.12) is bounded by

$$\exp\left((12N-6)^{6N-1}(4k-2)\right). \tag{4.15}$$

Thus (using that $N \leq n$) the number of those solutions of equation (1.1), for which there exists a solution $(y_1,\dots,y_n) \neq (x_1,\dots,x_n)$ with $x_i = y_i$, is bounded by

$$\Psi(k,n,mD^k)\exp\left((12n-6)^{6n-1}(4k-2)\right).$$

Thus the number of those solutions $(x_1,\dots,x_n)$ of equation (1.1), for which there exists another solution $(y_1,\dots,y_n) \neq (x_1,\dots,x_n)$, such that $\prod_{i=1}^n (x_i - y_i) = 0$ is bounded by

$$n\Psi(k,n,mD^k)\exp\left((12n-6)^{6n-1}(4k-2)\right) \leq \Psi(k,n,mD^k)\exp\left(k(12n)^{6n}\right).$$

□

Proof of Theorem 2.6. We start the proof of the present theorem exactly in the same way as the proof of Theorem 2.5. The first difference is that instead of equation (4.12) we get

$$\sum_{j=1}^{N} \left(\gamma_{ij}\sigma_j(\mu_1)\sigma_j(\varepsilon_1) - \gamma_{ij}\sigma_j(\mu_2)\sigma_j(\varepsilon_2)\right) = d \in T. \tag{4.16}$$

Now divide this equation by d to get an inhomogeneous S-unit equation having $2N$ terms. Using Lemma 3.3 we can bound (similarly to the proof of Theorem 2.5) the possibilities for either the values of $\frac{\sigma_u(\varepsilon_1)}{d}$, or

the values of $\frac{\sigma_u(\varepsilon_2)}{d}$ for some u, depending on the vanishing subsums in the unit equation. This bound is given by

$$\exp\left((12N)^{6N}(s+2k-1)\right). \tag{4.17}$$

Since $d \in \mathbb{Z}$ and $\sigma_u(\varepsilon_1)$ is a unit, thus if $\frac{\sigma_u(\varepsilon_1)}{d}$ is fixed, then d may assume at most two values and by fixing one of those, $\sigma_u(\varepsilon_1)$ becomes also fixed. Then we can fix ε_2, too. A similar argument works also when first we are able to fix $\frac{\sigma_u(\varepsilon_2)}{d}$. Thus for the number of solutions of equation (1.1), for which there exists another solution $(y_1, \dots, y_n) \neq (x_1, \dots, x_n)$, such that $x_i - y_i \in T$ for some $i \in \{1, \dots, n\}$, is bounded by

$$\Psi(k, n, mD^k) \exp\left((s+k)(12n)^{6n+3}\right).$$

□

Acknowledgement. The research was supported in part by the National Office for Research and Technology. The authors are grateful to the referee for his useful and helpful remarks.

References

[1] N.C. Ankeny, R. Brauer and S. Chowla, *A note on the class-numbers of algebraic number fields*, Amer J. Math. **78** (1956), 51–61.

[2] A. Bazsó, *Further Computational Experiences on Norm Form Equations with Solutions Forming Arithmetic Progressions*, Publ. Math. Debrecen, **71** (2007), 489–497.

[3] A. Bérczes and K. Győry, *On the number of solutions of decomposable polynomial equations*, Acta Arith. **101** (2002), 171–187.

[4] A. Bérczes and A. Pethő, *On norm form equations with solutions forming arithmetic progressions*, Publ. Math. Debrecen, **65** (2004), 281-290.

[5] A. Bérczes and A. Pethő, *Computational experiences on norm form equations with solutions forming arithmetic progressions*, Glasnik Math., **41** (2006), 1–8.

[6] A. Bérczes, A. Pethő and V. Ziegler, *Parameterized Norm Form Equations with Arithmetic progressions*, J. Symbolic Comput. **41** (2006), 790–810.

[7] A. Dujella, A. Pethő and P. Tadić, *On arithmetic progressions on Pellian equations*, Acta Math. Hungar., to appear.

[8] G. Everest and K. Győry, *On some arithmetical properties of solutions of decomposable form equations*, Math. Proc. Cambridge Philos. Soc. **139** (2005), 27–40.

[9] J.-H. Evertse and K. Győry, *The number of families of solutions of decomposable form equations*, Acta Arith. **80** (1997), 367–394.

[10] J.-H. Evertse, H. P. Schlickewei and W. M. Schmidt, *Linear equations in variables which lie in a multiplicative group*, Ann. of Math. (2), **155** (2002), 807–836.

[11] K. Győry, M. Mignotte and T. N. Shorey, *On some arithmetical properties of weighted sums of S-units*, Math. Pannon. **1** (1990), 25–43.

[12] L. Hajdu, *Arithmetic Progressions in Linear Combinations of S-units*, Periodica Math. Hungar. **54** (2007), 175-181.

[13] F. Halter-Koch, *Unabhängige Einheitensysteme für eine allgemeine Klasse algebraischer Zahlkörper*, Abh. Math. Sem. Univ. Hamburg **43** (1975), 85–91.
[14] F. Halter-Koch, G. Lettl, A. Pethő and R. Tichy, *Thue equations associated with Ankeny-Brauer-Chowla number fields*, J. London Math. Soc. **60** (1999), 1–20.
[15] M. Jarden and W. Narkiewicz, *On sums of units*, Monatsh. Math. **150** (2007), 327–332.
[16] M. Newman, *Units in arithmetic progression in an algebraic number field,* Proc. Amer. Math. Soc., **43** (1974), 266–268.
[17] M. Newman, *Consecutive units*, Proc. Amer. Math. Soc., **108** (1990), 303–306.
[18] A. Pethő and V. Ziegler, *Arithmetic progressions on Pell equations*, J. Number Theory, to appear.
[19] W.M. Schmidt, *Norm form equations*, Ann. of Math., **96** (1972), 526–551.

A. Bérczes
Institute of Mathematics, University of Debrecen
Number Theory Research Group, Hungarian Academy of Sciences and
University of Debrecen
H-4010 Debrecen, P.O. Box 12, Hungary
E-mail address: berczesa@math.klte.hu

L. Hajdu
Institute of Mathematics, University of Debrecen
Number Theory Research Group, Hungarian Academy of Sciences and
University of Debrecen
H-4010 Debrecen, P.O. Box 12, Hungary
E-mail address: hajdul@math.klte.hu

A. Pethő
Faculty of Informatics, University of Debrecen
Number Theory Research Group, Hungarian Academy of Sciences and
University of Debrecen
H-4010 Debrecen, P.O. Box 12, Hungary
E-mail address: pethoe@inf.unideb.hu