ON A PROBLEM OF HAJDU AND TENGELY

SAMIR SIKSEK AND MICHAEL STOLL

ABSTRACT. We answer a question asked by Hajdu and Tengely: The only arithmetic progression in coprime integers of the form (a^2, b^2, c^2, d^5) is $(1, 1, 1, 1)$.

For the proof, we first reduce the problem to that of determining the sets of rational points on three specific hyperelliptic curves of genus 4. A 2-cover descent computation shows that there are no rational points on two of these curves. We find generators for a subgroup of finite index of the Mordell-Weil group of the last curve. Applying Chabauty's method and the Mordell-Weil sieve, we prove that the only rational points on this curve are the obvious ones.

1. INTRODUCTION

Euler ([7, pages 440 and 635]) proved Fermat's claim that four distinct squares cannot form an arithmetic progression. There has recently been much interest in powers in arithmetic progressions. For example, Darmon and Merel [6] proved that the only solutions in coprime integers to the Diophantine equations $x^n + y^n = 2z^n$ with $n \geq 3$ satisfy $xyz = 0$ or ± 1. This shows that there are no non-trivial three term arithmetic progressions consisting of n-th powers with $n \geq 3$. The result of Darmon and Merel is far from elementary; it needs all the tools used in Wiles' proof of Fermat's Last Theorem and more.

An arithmetic progression $(x_1, x_2, \ldots, x_k)$ of integers is said to be *primitive* if the terms are coprime, i.e., if $\gcd(x_1, x_2) = 1$. Let S be a finite subset of integers ≥ 2. Hajdu [9] showed that if

$$(a_1^{\ell_1}, \ldots, a_k^{\ell_k}) \tag{1.1}$$

is a non-constant primitive arithmetic progression with $\ell_i \in S$, then k is bounded by some (inexplicit) constant $C(S)$. Bruin, Győry, Hajdu and Tengely [2] showed that for any $k \geq 4$ and any S, there are only finitely many primitive arithmetic progressions of the form (1.1), with $\ell_i \in S$. Moreover, for $S = \{2, 3\}$ and $k \geq 4$, they showed that $a_i = \pm 1$ for $i = 1, \ldots, k$.

A recent paper of Hajdu and Tengely [10] studies primitive arithmetic progressions (1.1) with exponents belonging to $S = \{2, n\}$ and $\{3, n\}$. In particular, they

Date: 23 September, 2009.

2000 *Mathematics Subject Classification.* Primary 11D41, Secondary 11G30, 14G05, 14G25.

show that any primitive non-constant arithmetic progression (1.1) with exponents $\ell_i \in \{2,5\}$ has $k \le 4$. Moreover, for $k = 4$ they show that

$$(\ell_1, \ell_2, \ell_3, \ell_4) = (2,2,2,5) \quad \text{or} \quad (5,2,2,2). \tag{1.2}$$

Note that if $(a_i^{\ell_i} : i = 1, \ldots, k)$ is an arithmetic progression, then so is the reverse progression $(a_i^{\ell_i} : i = k, k-1, \ldots, 1)$. Thus there is really only one case left open by Hajdu and Tengely, with exponents $(\ell_1, \ell_2, \ell_3, \ell_4) = (2,2,2,5)$. This is also mentioned as Problem 11 in a list of 22 open problems recently compiled by Evertse and Tijdeman [8]. In this paper we deal with this case.

Theorem 1. *The only arithmetic progression in coprime integers of the form*

$$(a^2, b^2, c^2, d^5)$$

is $(1,1,1,1)$.

This together with the above-mentioned results of Hajdu and Tengely completes the proof of the following theorem.

Theorem 2. *There are no non-constant primitive arithmetic progressions of the form* (1.1) *with* $\ell_i \in \{2,5\}$ *and* $k \ge 4$.

Note that the primitivity condition is crucial, since otherwise solutions abound. Let for example (a^2, b^2, c^2, d) be any arithmetic progression whose first three terms are squares — there are infinitely many of these; one can take $a = r^2 - 2rs - s^2$, $b = r^2 + s^2$, $c = r^2 + 2rs - s^2$ — then $\big((ad^2)^2, (bd^2)^2, (cd^2)^2, d^5\big)$ is an arithmetic progression whose first three terms are squares and whose last term is a fifth power.

For the proof of Theorem 1, we first reduce the problem to that of determining the sets of rational points on three specific hyperelliptic curves of genus 4. A 2-cover descent computation (following Bruin and Stoll [3]) shows that there are no rational points on two of these curves. We find generators for a subgroup of finite index of the Mordell-Weil group of the last curve. Applying Chabauty's method and the Mordell-Weil sieve, we prove that the only rational points on this curve are the obvious ones. All our computations are performed using the computer package MAGMA [1].

2. Construction of the curves

Let (a^2, b^2, c^2, d^5) be an arithmetic progression in coprime integers. Since a square is $\equiv 0$ or $1 \bmod 4$, it follows that all terms are $\equiv 1 \bmod 4$, in particular, a, b, c and d are all odd.

Considering the last three terms, we have the relation

$$(-d)^5 = b^2 - 2c^2 = (b + c\sqrt{2})(b - c\sqrt{2})\,.$$

Since b and c are odd, the two factors on the right are coprime in $R = \mathbb{Z}[\sqrt{2}]$. Since $R^\times/(R^\times)^5$ is generated by $1+\sqrt{2}$, it follows that

$$b + c\sqrt{2} = (1+\sqrt{2})^j (u + v\sqrt{2})^5 = g_j(u,v) + h_j(u,v)\sqrt{2} \tag{2.1}$$

with $-2 \le j \le 2$ and $u, v \in \mathbb{Z}$ coprime (with u odd and $v \equiv j+1 \bmod 2$). The polynomials g_j and h_j are homogeneous of degree 5.

Now the first three terms of the progression give the relation

$$a^2 = 2b^2 - c^2 = 2g_j(u,v)^2 - h_j(u,v)^2 .$$

Writing $y = a/v^5$ and $x = u/v$, this gives the equation of a hyperelliptic curve of genus 4,

$$C_j : y^2 = f_j(x)$$

where $f_j(x) = 2g_j(x,1)^2 - h_j(x,1)$. Every arithmetic progression of the required form therefore induces a rational point on one of the curves C_j.

We observe that taking conjugates in (2.1) leads to

$$(-1)^j b + (-1)^{j+1} c\sqrt{2} = (1+\sqrt{2})^{-j} (u + (-v)\sqrt{2})^5 ,$$

which implies that $f_{-j}(x) = f_j(-x)$ and therefore that C_{-j} and C_j are isomorphic and their rational points correspond to the same arithmetic progressions. We can therefore restrict attention to C_0, C_1 and C_2. Their equations are as follows.

$$\begin{aligned}
C_0 : y^2 = f_0(x) &= 2x^{10} + 55x^8 + 680x^6 + 1160x^4 + 640x^2 - 16 \\
C_1 : y^2 = f_1(x) &= x^{10} + 30x^9 + 215x^8 + 720x^7 + 1840x^6 + 3024x^5 \\
&\qquad + 3880x^4 + 2880x^3 + 1520x^2 + 480x + 112 \\
C_2 : y^2 = f_2(x) &= 14x^{10} + 180x^9 + 1135x^8 + 4320x^7 + 10760x^6 + 18144x^5 \\
&\qquad + 21320x^4 + 17280x^3 + 9280x^2 + 2880x + 368
\end{aligned}$$

The trivial solution $a = b = c = d = 1$ corresponds to $j = 1$, $(u, v) = (1, 0)$ in the above and therefore gives rise to the point ∞_+ on C_1 (this is the point at infinity where y/x^5 takes the value $+1$). Changing the signs of a, b or c leads to $\infty_- \in C_1(\mathbb{Q})$ or to the two points at infinity on the isomorphic curve C_{-1}.

3. Rational points

In this section, we determine the set of rational points on the three curves C_0, C_1 and C_2. We first consider C_0 and C_2. We apply the 2-cover-descent procedure described in [3] to the two curves and find that in each case, there are no 2-covers that have points everywhere locally. For C_0, only 2-adic information is needed in addition to the global computation, for C_2, we need 2-adic and 7-adic information. Note that the number fields generated by roots of f_0 or f_2 are sufficiently small in terms of degree and discriminant that the necessary class and unit group computations can be done unconditionally. This proves the following.

Proposition 3. *There are no rational points on the curves C_0 and C_2.*

We cannot hope to deal with C_1 in the same easy manner, since C_1 has two rational points at infinity coming from the trivial solutions. We can still perform a 2-cover-descent computation, though, and find that there is only one 2-covering of C_1 with points everywhere locally, which is the cover that lifts the points at infinity. We remark that by the way it is given, the polynomial f_1 factors over $\mathbb{Q}(\sqrt{2})$ into two conjugate factors of degree 5. This implies that the 'fake 2-Selmer set' computed by the 2-cover descent is the true 2-Selmer set, so that there is really only one 2-covering that corresponds to the only element of the set computed by the procedure. We state the result as a lemma. We fix $P_0 = \infty_- \in C_1$ as a basepoint and write J_1 for the Jacobian variety of C_1. Then

$$\iota : C_1 \longrightarrow J_1\,, \quad P \longmapsto [P - P_0]$$

is an embedding defined over $\mathbb{Q}$.

Lemma 4. *Let $P \in C_1(\mathbb{Q})$. Then the divisor class $[P - P_0]$ is in $2J_1(\mathbb{Q})$.*

Proof. Let D be the unique 2-covering of C_1 (up to isomorphism) which has points everywhere locally. Then D is (isomorphic to) the pull-back of $\iota(C_1) \subset J_1$ under the duplication map on J_1. Both P_0 and P lift to rational points on $D \subset J_1$, say Q_0 and Q. It follows that $[P - P_0] = 2Q - 2Q_0 = 2(Q - Q_0) \in 2J_1(\mathbb{Q})$. □

To make use of this information, we need to know $J_1(\mathbb{Q})$, or at least a subgroup of finite index. We find the following two independent points, which are given in Mumford representation as follows.

$$Q_1 = \left(x^4 + 4x^2 + \tfrac{4}{5}, \quad -16x^3 - \tfrac{96}{5}x\right)$$
$$Q_2 = \left(x^4 + \tfrac{24}{5}x^3 + \tfrac{36}{5}x^2 + \tfrac{48}{5}x + \tfrac{36}{5}, \quad -\tfrac{1712}{75}x^3 - \tfrac{976}{25}x^2 - \tfrac{1728}{25}x - \tfrac{2336}{25}\right)$$

Recall that the notation $(a(x), b(x))$ means the divisor class $[D - 2W]$ where D is given by $a(x) = 0, y = b(x)$, and $W = \infty_+ + \infty_-$. We note that $2Q_1 = [\infty_+ - \infty_-]$, which makes Lemma 4 explicit for the known points on C_1.

Lemma 5. *The Mordell-Weil group $J_1(\mathbb{Q})$ is torsion-free, and Q_1, Q_2 are linearly independent. In particular, the rank of $J_1(\mathbb{Q})$ is at least 2.*

Proof. The only primes of bad reduction for C_1 are 2, 3 and 5. It is known that the torsion subgroup of $J_1(\mathbb{Q})$ injects into $J_1(\mathbb{F}_p)$ when p is an odd prime of good reduction. Since $\#J_1(\mathbb{F}_7)$ and $\#J_1(\mathbb{F}_{41})$ are coprime, there can be no nontrivial torsion in $J_1(\mathbb{Q})$.

We check that the image of $\langle Q_1, Q_2 \rangle$ in $J_1(\mathbb{F}_7)$ is not cyclic. This shows that Q_1 and Q_2 must be independent. □

The next step is to show that the Mordell-Weil rank is indeed 2. For this, we compute the 2-Selmer group of J_1 as described in [13]. We give some details of the computation, since it is outside the scope of the functionality that is currently provided by MAGMA (or any other software package).

We first remind ourselves that f_1 factors over $\mathbb{Q}(\sqrt{2})$. This implies that the 'Cassels kernel' is trivial. Therefore the 'fake Selmer group' that we compute is in fact the actual 2-Selmer group of J_1.

We have to compute the image of $J_1(\mathbb{Q}_p)$ under the descent ('$x - T$') map for the primes p of bad reduction. We check that there is no 2-torsion in $J_1(\mathbb{Q}_3)$ and $J_1(\mathbb{Q}_5)$. This implies that the local image there is trivial. Since the (local) Cassels kernel is also trivial, this means that these two primes need not be considered as bad primes for the descent computation. The real locus $C_1(\mathbb{R})$ is connected, which means that there is no information coming from the local image at infinity.

The hardest part is the computation of the local image at $p = 2$. The 2-torsion subgroup $J_1(\mathbb{Q}_2)[2]$ has order 2; this implies that the quotient $J_1(\mathbb{Q}_2)/2J_1(\mathbb{Q}_2)$ has dimension 5 as an $\mathbb{F}_2$-vector space. This quotient is generated by the images of Q_1 and Q_2 and of three further points of the form $[D_i - \frac{\deg D_i}{2} W]$, where D_i is the sum of points on C_1 whose x-coordinates are the roots of

$$\begin{aligned} D_1 : &\quad \left(x - \tfrac{1}{2}\right)\left(x - \tfrac{1}{4}\right), \\ D_2 : &\quad x^2 - 2x + 6, \\ D_3 : &\quad x^4 + 4x^3 + 12x^2 + 36, \end{aligned}$$

respectively.

If K is a number field and S is a set of rational primes, we denote by $K(S, 2)$ the subgroup of $K^\times/(K^\times)^2$ of elements $\alpha(K^\times)^2$ such that $K(\sqrt{\alpha})/K$ is unramified outside the primes of K lying above primes in S. We let L be the number field generated by a root of f_1 and compute the group

$$H = \ker\Big(N_{L/\mathbb{Q}} : \frac{L(\{2\}, 2)}{\mathbb{Q}(\{2\}, 2)} \longrightarrow \mathbb{Q}(\{2\}, 2)\Big)$$

and the homomorphism

$$\mu_2 : H \longrightarrow H_2 = \frac{L_2^\times}{\mathbb{Q}_2^\times (L_2^\times)^2}$$

where $L_2 = L \otimes_{\mathbb{Q}} \mathbb{Q}_2$. Let I_2 be the image of $J_1(\mathbb{Q}_2)$ in H_2. Then the 2-Selmer group is $\mathrm{Sel}^{(2)}(\mathbb{Q}, J_1) = \mu_2^{-1}(I_2)$, and we find that its $\mathbb{F}_2$-dimension is 2. We therefore have the following.

Lemma 6. *The rank of $J_1(\mathbb{Q})$ is 2, and $\langle Q_1, Q_2\rangle \subset J_1(\mathbb{Q})$ is a subgroup of finite odd index.*

Proof. The Selmer group computation shows that the rank is ≤ 2, and Lemma 5 shows that the rank is ≥ 2. For the second statement, we check that the given subgroup surjects onto the 2-Selmer group. $\square$

Now we want to use the Chabauty-Coleman method [4, 5, 12] to show that ∞_+ and ∞_- are the only rational points on C_1. To keep the computations reasonably simple, we want to work at $p = 7$ (the smallest prime of good reduction).

For p a prime of good reduction, write ρ_p for the two 'reduction mod p' maps $J_1(\mathbb{Q}) \to J_1(\mathbb{F}_p)$ and $C_1(\mathbb{Q}) \to C_1(\mathbb{F}_p)$.

Lemma 7. *Let $P \in \mathbb{C}_1(\mathbb{Q})$. Then $\rho_7(P) = \rho_7(\infty_+)$ or $\rho_7(P) = \rho_7(\infty_-)$.*

Proof. Let $G = \langle Q_1, Q_2\rangle$ be the subgroup of $J_1(\mathbb{Q})$ generated by the two points Q_1 and Q_2. We find that $\rho_7(G)$ has index 2 in $J_1(\mathbb{F}_7)$. By Lemma 6, we know that $(J_1(\mathbb{Q}) : G)$ is odd, so we can deduce that $\rho_7(G) = \rho_7(J_1(\mathbb{Q}))$. The group $J_1(\mathbb{F}_7)$ surjects onto $(\mathbb{Z}/5\mathbb{Z})^2$, which implies that the index of G in $J_1(\mathbb{Q})$ is not divisible by 5.

We determine the set of points $P \in C_1(\mathbb{F}_7)$ such that $\iota(P) \in \rho_7(2J_1(\mathbb{Q})) = 2\rho_7(G)$. We find the set

$$X_7 = \{\rho_7(\infty_+), \rho_7(\infty_-), (-2, 2), (-2, -2)\}\,.$$

Note that for any $P \in J_1(\mathbb{Q})$, we must have $\rho_7(P) \in X_7$ by Lemma 4.

Now we look at $p = 13$. The image of G in $J_1(\mathbb{F}_{13})$ has index 5. Since we already know that $(J_1(\mathbb{Q}) : G)$ is not a multiple of 5, this implies that $\rho_{13}(G) = \rho_{13}(J_1(\mathbb{Q}))$. As above for $p = 7$, we compute the set $X_{13} \subset C_1(\mathbb{F}_{13})$ of points mapping into $\rho_{13}(2J_1(\mathbb{Q}))$. We find

$$X_{13} = \{\rho_{13}(\infty_+), \rho_{13}(\infty_-)\}\,.$$

Now suppose that there is $P \in C_1(\mathbb{Q})$ with $\rho_7(P) \in \{(-2, 2), (-2, -2)\}$. Then $\iota(P)$ is in one of two specific cosets in $J_1(\mathbb{Q})/\ker \rho_7 \cong G/\ker \rho_7|_G$. On the other hand, we have $\rho_{13}(P) = \rho_{13}(\infty_\pm)$, so that $\iota(P)$ is in one of two specific cosets in $J_1(\mathbb{Q})/\ker \rho_{13} \cong G/\ker \rho_{13}|_G$. It can be checked that the union of the first two cosets does not meet the union of the second two cosets. This implies that such a point P cannot exist. Therefore, the only remaining possibilities are that $\rho_7(P) = \rho_7(\infty_\pm)$. $\square$

Now we find the space of holomorphic 1-forms on C_1, defined over $\mathbb{Q}_7$, that annihilate the Mordell-Weil group under the integration pairing

$$\Omega^1_{C_1}(\mathbb{Q}_7) \times J_1(\mathbb{Q}_7) \longrightarrow \mathbb{Q}_7\,, \quad (\iota^*\omega, Q) \longmapsto \int_0^Q \omega\,.$$

(Recall that $\iota^* : \Omega^1_{J_1} \to \Omega^1_{C_1}$ gives a canonical identification of the two spaces of differentials.) We follow the procedure described in [11]. We first find two independent points in the intersection of $J_1(\mathbb{Q})$ and the kernel of reduction mod 7. In our case, we take $R_1 = 20Q_1$ and $R_2 = 5Q_1 + 60Q_2$. We represent these points in the form $R_j = [D_j - 4\infty_-]$ with effective divisors D_1, D_2 of degree 4. The points in the support of D_1 and D_2 all reduce to ∞_- modulo the prime above 7 in their fields of definition (which are degree 4 number fields totally ramified at 7). Expressing a basis of $\Omega^1_{C_1}(\mathbb{Q}_7)$ as power series in the uniformiser $t = 1/x$ times dt, we compute the integrals numerically. A little bit of linear algebra shows that the reductions mod 7 of the (suitably scaled) differentials that kill $J_1(\mathbb{Q})$ fill the subspace of $\Omega^1_{C_1}(\mathbb{F}_7)$ spanned by

$$\omega_1 = (1 + 3x - 2x^2)\frac{dx}{2y} \quad \text{and} \quad \omega_2 = (1 - x^2 + x^3)\frac{dx}{2y}\,.$$

Since ω_2 does not vanish at the points $\rho_7(\infty_\pm)$, this implies that there can be at most one rational point P on C_1 with $\rho_7(P) = \rho_7(\infty_+)$ and at most one point P with $\rho_7(P) = \rho_7(\infty_-)$ (see for example [12, Prop. 6.3]).

Proposition 8. *The only rational points on C_1 are ∞_+ and ∞_-.*

Proof. Let $P \in C_1(\mathbb{Q})$. By Lemma 7, $\rho_7(P) = \rho_7(\infty_\pm)$. By the argument above, for each sign $s \in \{+, -\}$, we have $\#\{P \in C_1(\mathbb{Q}) : \rho_7(P) = \rho_7(\infty_s)\} \le 1$. These two facts together imply that $\#C_1(\mathbb{Q}) \le 2$. Since we know the two rational points ∞_+ and ∞_- on C_1, there cannot be any further rational points. □

We can now prove Theorem 1.

Proof of Theorem 1. The considerations in Section 2 imply that if (a^2, b^2, c^2, d^5) is an arithmetic progression in coprime integers, then there are coprime u and v such that $(u/v, a/v^5)$ is a rational point on one of the curves C_j with $-2 \le j \le 2$. By Proposition 3, there are no rational points on C_0 and C_2 and therefore also not on the curve C_{-2}, which is isomorphic to C_2. By Proposition 8, the only rational points on C_1 (and C_{-1}) are the points at infinity. This translates into $a = \pm 1$, $u = \pm 1$, $v = 0$, and we have $j = \pm 1$. We deduce $a^2 = 1$, $b^2 = g_1(\pm 1, 0)^2 = 1$, whence also $c^2 = d^5 = 1$. □

References

[1] W. Bosma, J. Cannon and C. Playoust: *The Magma Algebra System I: The User Language*, J. Symb. Comp. **24** (1997), 235–265. (See also `http://www.maths.usyd.edu.au/`)

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

[3] N. Bruin and M. Stoll: *2-cover descent on hyperelliptic curves*, Math. Comp. **78** (2009), 2347–2370.

[4] C. Chabauty: *Sur les points rationnels des courbes algébriques de genre supérieur à l'unité* (French), C. R. Acad. Sci. Paris **212** (1941), 882–885.
[5] R.F. Coleman: *Effective Chabauty*, Duke Math. J. **52** (1985), 765–770.
[6] H. Darmon and 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.
[8] J.-H. Evertse and R. Tijdeman: *Some open problems about Diophantine equations* from a workshop in Leiden in May 2007, see `http://www.math.leidenuniv.nl/~evertse/07-workshop-problems.pdf`
[9] L. Hajdu, *Perfect powers in arithmetic progression. A note on the inhomogeneous case.* Acta Arith. **113** (2004), no. 4, 343–349.
[10] L. Hajdu and Sz. Tengely, *Arithmetic progressions of squares, cubes and n-th powers*, to appear in Functiones et Approximatio Commentarii Mathematici.
[11] M. Stoll, *Rational 6-cycles under iteration of quadratic polynomials*, London Math. Soc. J. Comput. Math. **11** (2008), 367–380.
[12] M. Stoll: *Independence of rational points on twists of a given curve*, Compositio Math. **142** (2006), 1201–1214.
[13] M. Stoll: *Implementing 2-descent for Jacobians of hyperelliptic curves*, Acta Arith. **98** (2001), 245–277.

Institute of Mathematics, University of Warwick, Coventry CV4 7AL, United Kingdom

E-mail address: `s.siksek@warwick.ac.uk`

Mathematisches Institut, Universität Bayreuth, 95440 Bayreuth, Germany.

E-mail address: `Michael.Stoll@uni-bayreuth.de`