Rev. Mat. Iberoam. **29** (2013), no. 4, 1211–1238
DOI 10.4171/RMI/754

Five squares in arithmetic progression over quadratic fields

Enrique González-Jiménez and Xavier Xarles

Abstract. We provide several criteria to show over which quadratic number fields $\mathbb{Q}(\sqrt{D})$ there is a nonconstant arithmetic progression of five squares. This is carried out by translating the problem to the determination of when some genus five curves C_D defined over $\mathbb{Q}$ have rational points, and then by using a Mordell–Weil sieve argument. Using an elliptic curve Chabauty-like method, we prove that, up to equivalence, the only nonconstant arithmetic progression of five squares over $\mathbb{Q}(\sqrt{409})$ is 7^2, 13^2, 17^2, 409, 23^2. Furthermore, we provide an algorithm for constructing all the nonconstant arithmetic progressions of five squares over all quadratic fields. Finally, we state several problems and conjectures related to this problem.

1. Introduction

A well-known result of Fermat, proved by Euler in 1780, states that there does not exist an arithmetic progression of four squares over $\mathbb{Q}$. Recently, the second author showed that there do not exist six squares in arithmetic progression over a quadratic field (see [29]). As a by-product of his proof, one reaches the conclusion that five squares in arithmetic progression over quadratic fields exist, but are all obtained from arithmetic progressions defined over $\mathbb{Q}$. The aim of this paper is to study over which quadratic fields there are such five-square sequences, in a manner similar to how the first author and J. Steuding studied the four-square sequences in [17].

However, there is a big difference between the four-square and the five-square problems: if a field contains four squares in arithmetic progression, then it probably contains infinitely many (inequivalent modulo squares), but a number field contains only a finite number of five squares in arithmetic progression. The reason for this is that the moduli space parametrizing these objects is a curve of genus 5 (see

Mathematics Subject Classification (2010): Primary 11G30, 11B25, 11D45; Secondary 14H25.
Keywords: Arithmetic progressions, squares, quadratic fields, elliptic curve Chabauty method, Mordell–Weil sieve.

Section 3), and can therefore only contain a finite number of points over a fixed number field by Faltings' Theorem.

On the other hand, one can easily prove (Remark 8.2, Section 8), that there are infinitely many arithmetic progressions such that their first five terms are squares over a quadratic field. The conclusion is that there are infinitely many quadratic fields with five squares in arithmetic progression.

In this paper, we will attempt to persuade the reader that, even though there are infinitely many such fields, they are few. For example, we will show that there are only two number fields $\mathbb{Q}(\sqrt{D})$, for D a square-free integer, with $D < 10^{13}$ having five squares in arithmetic progression: those with $D = 409$ and $D = 4688329$ (see Corollary 8.1). In order to obtain this result, we will develop a method, related to the Mordell–Weil sieve, to prove that certain curves have no rational points.

The outline of the paper is as follows: in Section 2, we provide another proof of a result in [29], essential for our paper. This result states that any arithmetic progression such that its first five terms are squares over a quadratic field is defined over $\mathbb{Q}$. Using this result, we will show in Section 3 that a number field $\mathbb{Q}(\sqrt{D})$ contains five different squares in arithmetic progression if and only if some curve C_D defined over $\mathbb{Q}$ has $\mathbb{Q}$-rational points. Next, we study a little bit of the geometry of these curves C_D. In the following sections, we provide several criteria to show when $C_D(\mathbb{Q})$ is empty: in Section 4, when it has no points at $\mathbb{R}$ or at $\mathbb{Q}_p$; in Section 5, when it has an elliptic quotient of rank 0; and in Section 6, when it does not pass some kind of Mordell–Weil sieve. Section 7 is devoted to computing all the rational points for C_{409}. This is carried out by modifying the elliptic curve Chabauty method, developed by Bruin in [5] and [4]. The result obtained is that there are only 16 rational points, all coming from the arithmetic progression $7^2, 13^2, 17^2, 409, 23^2$. Finally, in the last section, we give some tables related to the computations, some values of D where we do have rational points in C_D, and we state several problems and conjectures.

Acknowledgements. We would like to thank Gonzalo Tornaria for aiding us with some computations concerning the Corollary 8.1. The authors thank the referees for helpful comments and suggestions.

2. The 5 squares condition

Recall that $n+1$ elements of a progression $a_0, \dots, a_n$ in a field K are in arithmetic progression if there are a and $r \in K$ such that $a_i = a + i \cdot r$ for any $i = 0, \dots, n$. This is equivalent, of course, to having $a_i - a_{i-1} = r$ for any $i = 1, \dots, n$. Observe that, in order to study squares in arithmetic progression, we can and will identify the arithmetic progressions $\{a_i\}$ and $\{a_i'\}$ such that there is an $\alpha \in K^*$ with $a_i' = \alpha^2 a_i$ for any i. Hence, if $a_0 \neq 0$, we can divide all a_i by a_0, and the corresponding common difference is then $q = a_1/a_0 - 1$.

Let $K/\mathbb{Q}$ be a quadratic extension. The aim of this section is to show that any nonconstant arithmetic progression whose first five terms are squares over K is defined over $\mathbb{Q}$ modulo the previous identification. Another proof of this result can be found in [29].

First, let us consider the case of four squares in arithmetic progression over K.

Proposition 2.1. *Let $K/\mathbb{Q}$ be a quadratic extension, and let $x_i \in K$ for $i = 0, \dots, 3$ be four elements, not all zero, such that $x_i^2 - x_{i-1}^2 = x_j^2 - x_{j-1}^2 \in K$ for all $i, j = 1, 2, 3$. Then $x_0 \neq 0$; and if $q := (x_1/x_0)^2 - 1$, then $q = 0$ or*

$$\frac{(3q+2)^2}{q^2} \in \mathbb{Q}.$$

Proof. Observe that the conditions on x_0, x_1, x_2, x_3 are equivalent to the equations

$$x_0^2 - 2x_1^2 + x_2^2 = 0\,, \quad x_1^2 - 2x_2^2 + x_3^2 = 0,$$

which determine a curve C in $\mathbb{P}^3$. Observe also that q is invariant after multiplying all the x_i by a constant, so we can work with the corresponding point $[x_0 : x_1 : x_2 : x_3] \in \mathbb{P}^3$. Using the previous equations, one shows easily that x_0 cannot be zero.

Before continuing, we explain the strategy of the proof. Since there are no four squares in arithmetic progression over $\mathbb{Q}$, the genus one curve C satisfies $C(\mathbb{Q}) = \{[1 : \pm 1 : \pm 1 : \pm 1]\}$. Suppose we have a nonconstant map $\psi : C \to E'$ defined over $\mathbb{Q}$, where E' is an elliptic curve defined over $\mathbb{Q}$, such that $\psi(P) = 0$ for all $P \in C(\mathbb{Q})$. Denote by σ the only automorphism of order two of K, so $Gal(K/\mathbb{Q}) = \{\sigma, id\}$. Then, for any point $P \in C(K)$, $\psi(P) \oplus \psi(\sigma(P))$ must be 0, so $\psi(\sigma(P)) = \sigma(\psi(P)) = \ominus\psi(P)$. We will choose such an elliptic curve E' such that the Weierstrass equation satisfies that the x-coordinate of $\psi(P)$ is equal to $(3q+2)^2/q^2$. Since the x-coordinate is invariant by the $\ominus$-involution, we will obtain the result.

Multiplying the equations $x_i^2 = x_0^2 + iq$, for $i = 1, 2, 3$ we obtain

$$(x_1x_2x_3)^2 = (x_0^2 + q)(x_0^2 + 2q)(x_0^2 + 3q).$$

So, replacing q by $(x-2)x_0^2/6$, and $x_1x_2x_3/x_0^2$ by $y/6$, we get the elliptic curve E given by the equation

$$y^2 = x^3 + 5x^2 + 4x,$$

with a map given by $f(x_0, x_1, x_2, x_3) = (2x_3^2/x_0^2, 6x_1x_2x_3/x_0^3)$. This map is in fact an unramified degree four covering, corresponding to one of the descendants in the standard 2-descent. It sends the 8 trivial points to the points $(2, \pm 6)$, which are torsion and of order 4. We need a map that sends some trivial point to the zero, so we just take $\tau(P) := P \oplus (2, -6)$. The map $\tau : E \to E$ (not a morphism of elliptic curves) has the equations

$$\tau(x,y) = \Big(\frac{2(x^2 + 14x + 6y + 4)}{(x-2)^2}, -\frac{6(6xy + x^3 + 16x^2 + 32x + 12y + 8)}{(x-2)^3}\Big).$$

The trivial points then go to the 0 point and the point $(0, 0)$.

Now consider the standard 2-isogeny $\mu : E \to E'$, where E' has the equation $y^2 = x^3 - 10x^2 + 9x$, given by

$$\mu(x,y) = \Big(\frac{y^2}{x^2}, \frac{y(4-x^2)}{x^2}\Big)$$

(see for instance [24], Example III.4.5.). The composition $\mu \circ \tau \circ f$ is exactly the map ψ we want. By applying the formulae above we obtain that the x-coordinate of $\mu(\tau(f(x_0, x_1, x_2, x_3)))$ is exactly equal to $(3q+2)^2/q^2$. □

We apply this proposition to obtain the result on five squares in arithmetic progression.

Corollary 2.2. *Let $K/\mathbb{Q}$ be a quadratic extension, and let $x_i \in K$ for $i = 0, \dots, 4$ be five elements, not all zero, such that $x_i^2 - x_{i-1}^2 = x_j^2 - x_{j-1}^2 \in K$ for all $i, j = 1, 2, 3, 4$. Then $x_0 \neq 0$; and if $q := (x_1/x_0)^2 - 1$, then $q \in \mathbb{Q}$. In particular,*

$$x_i^2/x_0^2 = 1 + iq \in \mathbb{Q}, \quad i = 1, \dots, 4.$$

Proof. Suppose $q \neq 0$. By Proposition 2.1, we have that $t_q := (3q+2)^2/q^2 \in \mathbb{Q}$ and that the same is true for $q' := (x_2/x_1)^2 - 1$. As $q' = q/(q+1)$, the condition for q' is equivalent to $t'_q := (5q+2)^2/q^2 \in \mathbb{Q}$. However, $t'_q - t_q = 16 + 8/q$, so $q \in \mathbb{Q}$. □

3. A diophantine problem over $\mathbb{Q}$

Let D be a square-free integer. We will say that the sets S_1 and S_2 of $\mathbb{Q}(\sqrt{D})$ are square equivalent if there exists $\alpha \in \mathbb{Q}(\sqrt{D})$, $\alpha \neq 0$, such that $S_2 = \alpha^2 S_1$. Notice that the previous equivalence is natural when the sets are formed by squares. Then, Corollary 2.2 shows that any arithmetic progression of 5 squares over $\mathbb{Q}(\sqrt{D})$ is square equivalent to an arithmetic progression defined over $\mathbb{Q}$.

Lemma 3.1. *Let D be a square-free integer. Then an arithmetic progression of five squares over $\mathbb{Q}(\sqrt{D})$ is square equivalent to one of the form $x_i^2 = d_i X_i^2$, where $d_i = 1$ or D, $X_i \in \mathbb{Z}$, and the greatest common divisor of $x_0^2, \dots, x_4^2$ is square-free. We say that the 5-term arithmetic progression is of type $I = \{i \colon d_i = D\} \subset \{0, \dots, 4\}$.*

Proof. Let $z_0, \dots, z_4 \in \mathbb{Q}(\sqrt{D})$ be such that $z_0^2, \dots, z_4^2$ form an arithmetic progression. By Corollary 2.2, it is square equivalent to $y_i^2 = 1 + i\,r/s$, $i = 0, \dots, 4$ for some $r, s \in \mathbb{Z}$. In particular, it is square equivalent to $s^2 y_i^2 = s^2 + isr$ with $s^2, sr \in \mathbb{Z}$. Now let d be the greatest integer such that d^2 divides the greatest common divisor of $s^2 y_0^2, \dots, s^2 y_4^2$. Then the arithmetic progression z_i^2 is square equivalent to $x_i^2 = (s/d)^2 y_i^2$, where the greatest common divisor of $x_0^2, \dots, x_4^2$ is square-free and since $x_i^2 \in \mathbb{Z}$ and $x_i \in \mathbb{Q}(\sqrt{D})$ we have that $x_i^2 = d_i X_i^2$ where $d_i = 1$ or D and $X_i \in \mathbb{Z}$. □

Notice that $7^2, 13^2, 17^2, 409, 23^2$ is an arithmetic progression of length 5 over $\mathbb{Q}(\sqrt{409})$ of type $\{3\}$, since $d_3 = 409$.

We define another equivalence relation on the set of 5-term arithmetic progressions over $\mathbb{Q}(\sqrt{D})$ as follows: we say that two arithmetic progressions $x_0^2, \dots, x_4^2$ and $y_0^2, \dots, y_4^2$ over $\mathbb{Q}(\sqrt{D})$ are equivalent if there exists $r \in \mathbb{Q}$ and $\alpha = r^2$ or $\alpha = D\,r^2$ such that $y_i^2 = \alpha x_i^2$ or $y_{4-i}^2 = x_i^2$ for $i = 0, \dots, 4$.

Lemma 3.2. *Up to equivalence, a nonconstant arithmetic progression of five squares over a quadratic field is of type* $\{3\}$.

Proof. Notice that up to the equivalence defined above, there are only a few types of nonconstant arithmetic progressions of 5 squares over quadratic fields: namely $\{i\}$ for $i = 2, 3, 4$ and $\{i, j\}$ for $i = 0, 1$ and $j = 1, \dots, 4$ with $i < j$.

Now, assume that we have a 5-term arithmetic progression $x_n^2 = a + nq$, $n = 0, \dots, 4$, over $\mathbb{Q}(\sqrt{D})$ of type $\{i, j\}$. Then, by Lemma 3.1, $x_i^2 = DX_i^2$, $x_j^2 = DX_j^2$ and $x_k^2 = X_k^2$ if $k \neq i, j$, where $X_n \in \mathbb{Z}$, $n = 0, \dots, 4$. Let $p > 3$ be a prime dividing D. Since $(j-i)q = x_j^2 - x_i^2 = D(X_j^2 - X_i^2)$, we have $p|q$, and therefore $p|a$. Thus p divides x_n^2 for all $n = 0, \dots, 4$.

Let us see that, in fact, $p^2|x_n^2$ for all $n = 0, \dots, 4$, to obtain a contradiction (recall that the x_n are not in $\mathbb{Z}$, so this is not automatic). Observe that for any $k \in \{0, \dots, 4\}$ with $k \neq i, j$, we have that $x_k^2 = X_k^2$ with $X_k \in \mathbb{Z}$. Hence p divides X_k and so p^2 divides x_k^2. But now, considering $k, l \in \{0, \dots, 4\}$ such that $k, l \neq i, j$ and $l > k$, we obtain that $(l-k)r = x_l^2 - x_k^2$, and hence $p^2|q$, and therefore $p^2|a$. We have proved that the type $\{i, j\}$ is not possible over $\mathbb{Q}(\sqrt{D})$ for $|D| > 6$ and $|D| = 5$. The cases $D = -6, -3, -2, -1, 2$ and 3 are not possible since there are no nonconstant arithmetic progressions of four squares over $\mathbb{Q}(\sqrt{D})$ (cf. [17]). The remaining case $D = 6$ is not possible, although by a different argument, since there are infinitely many nonconstant arithmetic progressions of four squares over $\mathbb{Q}(\sqrt{6})$ (cf. [17]). We are going to prove that the types $\{i, j\}$ for $i = 0, 1$ and $j = 1, \dots, 4$ with $i < j$ are not possible over $\mathbb{Q}(\sqrt{6})$. Define the following three conics in $\mathbb{P}^2(\mathbb{Q})$:

$$\begin{aligned} C_{1,i} &: 6X_i^2 - 12X_{i+1}^2 + X_{i+2}^2 = 0, \\ C_{2,i} &: 6X_i^2 - 2X_{i+1}^2 + 6X_{i+2}^2 = 0, \\ C_{3,i} &: X_i^2 - 2X_{i+1}^2 + 6X_{i+2}^2 = 0. \end{aligned}$$

Then it is straightforward to prove, using Hilbert symbols, that $C_{j,i}(\mathbb{Q}) = \emptyset$ for $j = 1, 2, 3$. Now, consider a 5-term arithmetic progression $x_0^2, x_1^2, x_2^2, x_3^2, x_4^2$. Then x_0, x_1, x_2, x_3, x_4 are solutions of the system of equations

$$x_0^2 - 2x_1^2 + x_2^2 = 0, \quad x_1^2 - 2x_2^2 + x_3^2 = 0, \quad x_2^2 - 2x_3^2 + x_4^2 = 0.$$

In particular, if this 5-term arithmetic progression is over $\mathbb{Q}(\sqrt{6})$ of type, say, $\{0, 1\}$ then $x_0^2 = 6X_0^2$, $x_1^2 = 6X_1^2$ and $x_k^2 = X_k^2$ for $k = 2, 3, 4$ and $X_0, X_1, X_2, X_3, X_4 \in \mathbb{Q}$. Then the first equation of the previous system becomes $6X_0^2 - 12X_1^2 + X_2^2 = 0$. That is, $[X_0 : X_1 : X_2] \in C_{1,0}(\mathbb{Q})$. But since $C_{1,0}(\mathbb{Q}) = \emptyset$ we conclude that there is no nonconstant 5-term arithmetic progression over $\mathbb{Q}(\sqrt{6})$ of type $\{0, 1\}$. For the remaining types we follow the same argument but replacing the conic $C_{1,0}$ by the conics indicated in the following table:

$\{0,1\}$	$\{0,2\}$	$\{0,3\}$	$\{0,4\}$	$\{1,2\}$	$\{1,3\}$	$\{1,4\}$
$C_{1,0}$	$C_{2,0}$	$C_{3,1}$	$C_{3,2}$	$C_{1,1}$	$C_{2,1}$	$C_{3,2}$

The type $\{4\}$ (or equivalently $\{0\}$) is not possible since there are no nonconstant arithmetic progressions of four squares over the rationals.

To finish, let us see that the type $\{2\}$ is not possible. In this case we have that $[x_0 : x_1 : x_3 : x_4] \in \mathbb{P}^3(\mathbb{Q})$ is a point on the intersection of the two quadric surfaces

$$C_{\{2\}} \,:\, \begin{cases} X_1^2 + 2X_4^2 - 3X_3^2 = 0 \\ X_3^2 + 2X_0^2 - 3X_1^2 = 0. \end{cases}$$

in $\mathbb{P}^3$. Note that the eight points $[1 : \pm 1 : \pm 1 : \pm 1]$ belong to $C_{\{2\}}$. In the generic case the intersection of two quadric surfaces in $\mathbb{P}^3$ gives an elliptic curve and, indeed, this will turn out to be true in our case. A Weierstrass model for this curve is given by $E : y^2 = x(x+1)(x+9)$ (this is denoted by `48a3` in Cremona's tables [11], [12]). Using a computer algebra package like `MAGMA` or `SAGE` ([3] and [25] respectively), we check that $E(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$. Therefore $C_{\{2\}} = \{[1 : \pm 1 : \pm 1 : \pm 1]\}$, which implies $x_n^2 = x_0^2$ for $n = 0, 1, 3, 4$. Deriving from this that $Dx_2^2 = x_0^2$ is then straightforward, but this is impossible. □

Let D be a square-free integer. We will denote by C_D the curve over $\mathbb{Q}$ that classifies the arithmetic progressions of type $\{3\}$. As a consequence of the previous result, we get the following geometric characterization.

Corollary 3.3. *Let D be a square-free integer. The, up to equivalence, nonconstant arithmetic progressions of 5 squares over $\mathbb{Q}(\sqrt{D})$ are in bijection with the set $C_D(\mathbb{Q})$.*

The curve C_D has remarkable properties that we are going to show in the sequel. First of all, the curve C_D is a nonsingular curve over $\mathbb{Q}$ of genus 5 that can be given by the following equations in $\mathbb{P}^4$:

$$C_D \,:\, \begin{cases} F_{012} := X_0^2 - 2X_1^2 + X_2^2 \quad = 0, \\ F_{123} := X_1^2 - 2X_2^2 + DX_3^2 = 0, \\ F_{234} := X_2^2 - 2DX_3^2 + X_4^2 = 0, \end{cases} \tag{3.1}$$

where we use the convention that for distinct $i, j, k \in \{0, \ldots, 4\}$, F_{ijk} denotes the curve that classifies the arithmetic progressions $\{a_n\}_n$ (modulo equivalence) such that $a_i = d_i X_i^2$, $a_j = d_j X_j^2$, $a_k = d_k X_k^2$, where $d_i = 1$ if $i \neq 3$ and $d_3 = D$.

Observe that we could also describe the curve C_D by choosing three equations F_{ijk} with the only condition that each of the numbers $1, \ldots, 4$ appears as the subindex of some F_{ijk}.

We have 5 quotients of genus 1 that are the intersection of the two quadric surfaces in $\mathbb{P}^3$ given by $F_{ijk} = 0$ and $F_{ijl} = 0$, where the $i, j, k, l \in \{0, \ldots, 4\}$ are distinct. Note that these quotients are obtained by removing the variable X_n, where $n \neq i, j, k, l$. We denote by $F_D^{(n)}$ this genus 1 curve.

These genus 1 curves do not always have rational points (except for $F^{(3)} := F_D^{(3)}$). Weierstrass models of the Jacobians of these genus 1 curves can be computed by finding them in the case $D = 1$ (using that $F_1^{(i)}$ always has some easily found rational point), and then twisting by D. Using the labeling of Cremona's tables ([11]

and [12]), one can check that $\mathrm{Jac}(F_D^{(0)})$ (resp. $\mathrm{Jac}(F_D^{(1)})$, $\mathrm{Jac}(F_D^{(2)})$, $\mathrm{Jac}(F_D^{(4)})$) is the D-twist of `24a1` (resp. `192a2`, `48a3`, `24a1`) and $\mathrm{Jac}(F^{(3)})$ is `192a2`. We denote by $E^{(0)}$ (resp. $E^{(1)}$, $E^{(2)}$) the elliptic curve `24a1` (resp. `192a2`, `48a3`) and by $E_D^{(i)}$ the D-twist of $E^{(i)}$, for $i = 0, 1, 2$. Observe also that $E^{(2)} = E_{-1}^{(0)}$, so $E_D^{(2)} = E_{-D}^{(0)}$.

Note that, in particular, we have shown the following result about the decomposition of the Jacobian of C_D in the $\mathbb{Q}$-isogeny class.

Lemma 3.4. *Let D be a square-free integer. Then*

$$\mathrm{Jac}(C_D) \overset{\mathbb{Q}}{\sim} \left(E_D^{(0)}\right)^2 \times E_D^{(2)} \times E_D^{(1)} \times E^{(1)} .$$

4. Local solvability for the curve C_D

The aim of this section is to describe under which conditions with respect to D the curve C_D has points in $\mathbb{R}$ and $\mathbb{Q}_p$ for all prime numbers p.

Proposition 4.1. *Let D be a square-free integer. Then C_D has points in $\mathbb{R}$ and in $\mathbb{Q}_p$ for all primes p if and only if $D > 0$, $D \equiv \pm 1 \pmod 5$ and for all primes p dividing D, $p \equiv 1 \pmod{24}$.*

This result is deduced from the following lemmas.

Lemma 4.2. *Let D be a square-free integer. The curve C_D has points in K, for $K = \mathbb{R}$, $\mathbb{Q}_2$, $\mathbb{Q}_3$ and $\mathbb{Q}_5$ if and only if D is a square in K. Explicitly, $D > 0$, $D \equiv 1 \pmod 8$, $D \equiv 1 \pmod 3$ and $D \equiv \pm 1 \pmod 5$, respectively.*

Proof. First, suppose that D is a square over a field K. Then the curve C_D contains the sixteen points $[1 : \pm 1 : \pm 1 : \pm 1/\sqrt{D} : \pm 1]$. This shows one of the implications. In order to show the other implication we will consider the different fields separately. Suppose that $C_D(K) \neq \emptyset$.

If $K = \mathbb{R}$, the equation $F_{234} = 0$ implies that $2DX_3^2 = X_2^2 + X_4^2$, which has solutions in K only if $D > 0$.

Consider now the case $K = \mathbb{Q}_2$. On one hand, the conic given by the equation $F_{123} = X_1^2 - 2X_2^2 + DX_3^2$ has points in $\mathbb{Q}_2$ if and only if $(2, -D)_2 = 1$, where $(\ ,\ )_2$ denotes the Hilbert symbol. This last condition is equivalent to $D \equiv \pm 1 \pmod 8$ or $D \equiv \pm 2 \pmod{16}$. On the other hand, making the same argument for the equation $F_{234} = X_2^2 - 2DX_3^2 + X_4^2$ we get the condition $(-1, 2D)_2 = 1$, which implies $D \equiv 1 \pmod 4$ or $D \equiv 2 \pmod 8$. So we get D odd and $D \equiv 1 \pmod 8$, or D even and $D \equiv 2 \pmod{16}$. This last case is equivalent, modulo squares, to the case $D = 2$ and it is easy to show that $C_2(\mathbb{Q}_2) = \emptyset$.

If $K = \mathbb{Q}_3$, considering the reduction modulo 3 of the conic given by the equation $F_{023} = 0$, we obtain that $D \not\equiv -1 \pmod 3$. Similarly, we have $D \not\equiv 0 \pmod 3$ using $F_{123} = 0$.

Finally if $K = \mathbb{Q}_5$, one can show by an exhaustive search that there is no point in $C_D(\mathbb{F}_5)$ if $D \equiv \pm 2 \pmod 5$. The case $D \equiv 0 \pmod 5$ is handled by using $F_{123} = 0$ modulo 5. □

In the following we will study the remaining primes $p > 5$ in two separate cases, depending on whether p divides D or not. The first observation is that the case that p does not divide D corresponds to the good reduction case.

Lemma 4.3. *Let $p > 3$ be a prime not dividing D. Then the model of C_D given by the equations F_{012}, F_{123} and F_{234} has good reduction at p.*

Proof. We use the Jacobian criterion. The Jacobian matrix of the system of equations defining C_D is

$$A := \left(\partial F_{i(i+1)(i+2)}(X_i, X_{i+1}, X_{i+2})/\partial X_j\right)_{0\leq i\leq 2, 0\leq j\leq 4}.$$

For any $j_1 < j_2$, denote by A_{j_1,j_2} the square matrix obtained from A by deleting the columns j_1 and j_2. Their determinants are

$$|A_{j_1,j_2}| = k_{j_1,j_2} \cdot \prod_{i\neq j_1,j_2} X_i\,,$$

where

$$\begin{array}{lllll} k_{0,1} = 2^3D, & k_{0,2} = -2^4D, & k_{0,3} = 2^33, & k_{0,4} = 2^5D, & k_{1,2} = 2^3D, \\ k_{1,3} = -2^4, & k_{1,4} = 2^33D, & k_{2,3} = 2^3, & k_{2,4} = -2^4D, & k_{3,4} = 2^3. \end{array}$$

Now, suppose we have a singular point of $C_D(\mathbb{F}_p)$. Then, at this point, the matrix A must have rank less than 3, so all these determinants must be 0. However, if $p > 3$ and p does not divide D, then all products of the three homogeneous coordinates must be zero, so the point must have three coordinates equal to 0, which is impossible if $p > 3$. □

Lemma 4.4. *Let $p > 5$ be a prime such that p does not divide D. Then $C_D(\mathbb{Q}_p) \neq \emptyset$.*

Proof. First, by Hensel's lemma, and since C_D has good reduction at p, we have that any point modulo p lifts to some point in $\mathbb{Q}_p$. So we only need to show that $C_D(\mathbb{F}_p) \neq \emptyset$. Now, because of the Weil bounds, we know that $\sharp C_D(\mathbb{F}_p) > p + 1 - 10\sqrt{p}$. So, if $p > 97$, then $C_D(\mathbb{F}_p) \neq \emptyset$ and we are done. For the primes p satisfying $5 < p < 97$, an exhaustive search proves the result. □

We suspect that there should be some reason, besides the Weil bound, that for all primes $p > 5$ not dividing D, the curve C_D has points modulo p, that should be related to the special form it has or to the moduli problem it classifies.

Lemma 4.5. *Let $p > 3$ be a prime dividing D. Then $C_D(\mathbb{Q}_p) \neq \emptyset$ if and only if $p \equiv 1 \pmod{24}$.*

Proof. We will show that a necessary and sufficient condition for $C_D(\mathbb{Q}_p) \neq \emptyset$ is that 2, 3 and -1 are squares in $\mathbb{F}_p$. This happens exactly when $p \equiv 1 \pmod{24}$. Note that this condition is sufficient since $[\sqrt{3} : \sqrt{2} : 1 : 0 : \sqrt{-1}]$ belongs to C_D.

Suppose that we have a point in $C_D(\mathbb{Q}_p)$ given by a solution of the equations F_{ijk} in projective coordinates $[x_0 : x_1 : x_2 : x_3 : x_4]$, with $x_i \in \mathbb{Z}_p$, and such that not all x_i are divisible by p. The first observation is that only one of the x_i may be divisible by p; since if two of them, say x_i and x_j, are divisible by p, we can use the equations F_{ijk} in order to show that x_k is also divisible, for any k.

Now, reducing F_{123} modulo p, we obtain that 2 must be a square modulo p. Reducing F_{234} modulo p we obtain that -1 must be a square modulo p. And finally, reducing $F_{034} = X_0^2 - 4DX_3^2 + 3X_4^2$ modulo p we obtain that 3 must be a square modulo p. Hence the conditions are necessary. □

5. The rank condition

Let us begin by recalling the well-known 2-descent on elliptic curves, as explained for example in Proposition 1.4 of Chapter X in [24]. Consider an elliptic curve E over a number field K given by an equation of the form

$$y^2 = x(x-e_1)(x-e_2)\ , \quad \text{with } e_1, e_2 \in K.$$

Let S be the set of places of K including all archimedean places, all places dividing 2, and all places at which E has bad reduction. Let $K(S,2)$ be the set of all elements b in K^*/K^{*2} such that $\mathrm{ord}_v(b)$ is even for all $v \notin S$. Given any $(b_1,b_2) \in K(S,2) \times K(S,2)$, define the curve H_{b_1,b_2} as the intersection of two quadrics in $\mathbb{P}^3$ given by the equations

$$H_{b_1,b_2} : \begin{cases} b_1 z_1^2 - b_2 z_2^2 &= e_1 z_0^2, \\ b_1 z_1^2 - b_1 b_2 z_3^2 &= e_2 z_0^2. \end{cases}$$

Then the curves H_{b_1,b_2} do not depend on the representatives, up to isomorphism, and they have genus one with Jacobian E. Moreover, we have a natural degree four map $\phi_{b_1,b_2} : H_{b_1,b_2} \to E$ given by

$$\phi_{b_1,b_2}(z_0,z_1,z_2,z_3) := (b_1(z_1/z_0)^2, b_1 b_2 z_1 z_2 z_3 / z_0^3).$$

Moreover, the 2-Selmer group $S^{(2)}(E/K)$ of E may be identified with the subset

$$S^{(2)}(E/K) = \left\{ (b_1,b_2) \in K(S,2) \times K(S,2) \,|\, H_{b_1,b_2}(K_v) \neq \emptyset \ \forall v \text{ place in } K \right\}.$$

The group $E(K)/2E(K)$ may be described, via the natural injective map $\psi : E(K)/2E(K) \to S^{(2)}(E/K)$ defined by

$$\psi(0) = (1,1) \quad \text{and} \quad \psi((x,y)) = \begin{cases} (x, x-e_1) & \text{if} \quad x \neq 0,\, e_1 \\ (e_2/e_1, -e_1) & \text{if} \quad (x,y) = (0,0) \\ (e_1, (e_1-e_2)/e_1) & \text{if} \quad (x,y) = (e_1, 0) \end{cases}$$

as the subgroup consisting of $(b_1,b_2) \in K(S,2) \times K(S,2)$ such that $H_{b_1,b_2}(K) \neq \emptyset$.

The following lemma is elementary by using the description above, and it is left to the reader.

Lemma 5.1. *Let H be a genus 1 curve over a number field K given by an equation of the form*

$$H : \begin{cases} b_1 z_1^2 - b_2 z_2^2 &= e_1 z_0^2 \\ b_1 z_1^2 - b_1 b_2 z_3^2 &= e_2 z_0^2 \end{cases}$$

for some $b_1, b_2, e_1, e_2 \in K$. Let $D \in K^*$ and consider the curves $H_D^{(1)}$, $H_D^{(2)}$ and $H_D^{(3)}$ given by replacing z_1^2 by Dz_1^2, z_2^2 by Dz_2^2 and z_3^2 by Dz_3^2 respectively in *the equations above. Then $H_D^{(1)}$, $H_D^{(2)}$ and $H_D^{(3)}$ are homogeneous spaces for the elliptic curve E_D, the twist by D of E, given by the Weierstrass equation $y^2 = x(x-De_1)(x-De_2)$.*

Moreover, if S_D denotes the set of places of K including all archimedean places, all places dividing $2D$, and all places at which E has bad reduction, the curves $H_D^{(1)}$, $H_D^{(2)}$ and $H_D^{(3)}$ correspond respectively to the elements (Db_1, b_2), (b_1, Db_2) and (Db_1, Db_2) in $K(S_D, 2) \times K(S_D, 2)$.

Proposition 5.2. *Let $D > 0$ be a square-free integer. A necessary condition for the existence of 5 nontrivial squares in arithmetic progression over $\mathbb{Q}(\sqrt{D})$ is that the elliptic curves $E_D^{(0)}$ and $E_D^{(2)}$ given by the equations $Dy^2 = x(x+1)(x+4)$ and $Dy^2 = x(x+1)(x+9)$ have rank 2 or more over $\mathbb{Q}$, and that the elliptic curve $E_D^{(1)}$ given by the equation $Dy^2 = x(x+2)(x+6)$ has positive rank.*

Proof. Assume we have 5 nontrivial squares in arithmetic progression over $\mathbb{Q}(\sqrt{D})$. By using the results from Section 3, we can assume that such squares have the form x_0^2, x_1^2, x_2^2, Dx_3^2 and x_4^2, with $x_i \in \mathbb{Z}$. The condition of being in arithmetic progression is equivalent to $x_0^2 = a$, $x_1^2 = a + q$, $x_2^2 = a + 2q$, $Dx_3^2 = a + 3q$ and $x_4^2 = a + 4q$ for some $a, q \in \mathbb{Z}$. From these equations we easily obtain that the homogeneous spaces

$$\begin{cases} 2(DX_3)^2 - 3DX_2^2 = -DX_0^2 \\ 2(DX_3)^2 - 6DX_1^2 = -4DX_0^2 \end{cases} \quad \text{and} \quad \begin{cases} 2DX_4^2 - 3(DX_3)^2 = -DX_1^2 \\ 2DX_4^2 - 6DX_2^2 = -4DX_1^2 \end{cases}$$

attached to $E_D^{(0)}$ have rational points, which give $(2, 3D)$ and $(2D, 3) \in S^{(2)}(E_D^{(0)}/\mathbb{Q})$ by using Lemma 5.1. Since we are supposing both curves have points in $\mathbb{Q}$, they correspond to two points P_1 and P_2 in $E_D^{(0)}(\mathbb{Q})$. In order to show these have infinite orders, we only need to show that the symbols $(2, 3D)$ and $(2D, 3)$ are not in

$$\psi(E_D^{(0)}[2]) = \{(1,1), (4,4D) = (1,D), (-D,-1), (-D,-D)\}$$

which is clear since $D > 0$. In order to show that P_1 and P_2 are independent modulo torsion, it is sufficient to show that $(2, 3D)(2D, 3) = (D, D)$ is not in $\psi(E_D^{(0)}[2])$, which is again clear. So $E_D^{(0)}(\mathbb{Q})$ has rank > 1.

The other conditions are used in a similar fashion. We have

$$\begin{cases} 3DX_4^2 - 4(DX_3)^2 = -DX_0^2 \\ 3DX_4^2 - 12DX_1^2 = -9DX_0^2 \end{cases} \quad \text{and} \quad \begin{cases} 3DX_0^2 - 4DX_1^2 = -DX_4^2 \\ 3DX_0^2 - 12D^2X_3^2 = -9DX_4^2 \end{cases}$$

which give $(3D, 1)$ and $(3D, 4D) = (3D, D) \in S^{(2)}(E_D^{(2)}/\mathbb{Q})$, again giving two independent points in $E_D^{(2)}(\mathbb{Q})$.

Finally, we have

$$6DX_4^2 - 2(2DX_3)^2 = -2DX_0^2\ ,\ 6DX_4^2 - 12DX_1^2 = -6DX_0^2$$

which gives $(6D, 2) \in S^{(2)}(E_D^{(1)}/\mathbb{Q})$, giving a non-torsion point in $E_D^{(1)}(\mathbb{Q})$. □

Remark 5.3. Suppose that D satisfies the conditions in Proposition 4.1, so that $C_D(\mathbb{Q}_p) \neq \emptyset$ for all p. Then the root number of $E_D^{(0)}$ and $E_D^{(2)}$ is 1 independent of D in both cases, and the root number of $E_D^{(1)}$ is always -1. This is because the root number of the twist by D of an elliptic curve E of conductor N, if N and $D \equiv 1 \pmod 4$ are coprime, is equal to the Kronecker symbol $(D/-N)$ times the root number of E (see, for example, Section 4.3 of [23], which is deduced from the corollary to Proposition 10 in [21]). In our case, assuming D satisfies the conditions in Proposition 4.1, we obtain that the root number of $E_D^{(i)}$ is equal to the root number of $E^{(i)}$, since $(D/-N) = 1$ for $N = 24, 48, 192$.

Assuming the parity conjecture, this implies that the rank of $E_D^{(0)}$ and $E_D^{(2)}$ is always even, and the rank of $E_D^{(1)}$ is always odd. So the last condition in the proposition is (conjecturally) empty.

5.1. Ternary quadratic forms

It has been shown in Proposition 5.2 that a necessary condition for the existence of a nonconstant arithmetic progression of five squares over a quadratic field $\mathbb{Q}(\sqrt{D})$ is that the elliptic curves $E_D^{(0)}$ and $E_D^{(2)}$ have ranks ≥ 2. In this part, we describe some explicit results concerning the ranks of these curves, thereby obtaining an explicitly computable condition.

Remark 5.4. The elliptic curve $E_D^{(0)}$ (resp. $E_D^{(2)}$) parametrizes nonconstant arithmetic progressions of four squares over $\mathbb{Q}(\sqrt{D})$ (resp. $\mathbb{Q}(\sqrt{-D})$) (cf. [17]). Therefore, a necessary condition for the existence of a nonconstant arithmetic progression of five squares over $\mathbb{Q}(\sqrt{D})$ is the existence of a nonconstant arithmetic progression of four squares over $\mathbb{Q}(\sqrt{D})$ and over $\mathbb{Q}(\sqrt{-D})$.

Using Waldspurger's results and Shimura's correspondence *à la* Tunnell, Yoshida (see [30]) obtained several results on the ranks of $E_D^{(0)}$ and $E_D^{(2)}$. In particular, we apply his results for the $D \equiv 1 \pmod{24}$ case to our problem.

Proposition 5.5. *Let D be a square-free integer. If $Q(x,y,z) \in \mathbb{Z}[x,y,z]$ is a ternary quadratic form, denote by $r(D, Q(x,y,z))$ the number of integer representations of D by Q. If*

$$\begin{aligned} & r(D, x^2+12y^2+15z^2+12yz) \neq r(D, 3x^2+4y^2+13z^2+4yz) \\ \text{or} \quad & r(D, x^2+3y^2+144z^2) \neq r(D, 3x^2+9y^2+16z^2), \end{aligned}$$

then there are no nonconstant arithmetic progressions of five squares over $\mathbb{Q}(\sqrt{D})$.

Proof. First, by Proposition 4.1 we have that $D \equiv 1 \pmod{24}$. Now, Yoshida constructs two cusp forms of weight 3/2 denoted by $\Phi_{3,-3}$ and $\Phi_{1,1}$, such that if we denote by $a_D(\Phi_{3,-3})$ (resp. $a_D(\Phi_{1,1})$) the D-th coefficient of the Fourier q-expansion of $\Phi_{3,-3}$ (resp. $\Phi_{1,1}$), we have

$$\begin{aligned} a_D(\Phi_{3,-3}) = 0 \quad & \text{if and only if} \quad L(E_D^{(0)}, 1) = 0, \\ a_D(\Phi_{1,1}) = 0 \quad & \text{if and only if} \quad L(E_D^{(2)}, 1) = 0. \end{aligned}$$

Then by the definition of these cusp forms we have

$$\begin{aligned} a_D(\Phi_{3,-3}) &= r(D, x^2+12y^2+15z^2+12yz) - r(D, 3x^2+4y^2+13z^2+4yz)\,, \\ a_D(\Phi_{1,1}) &= r(D, x^2+3y^2+144z^2) - r(D, 3x^2+9y^2+16z^2)\,, \end{aligned}$$

which concludes the proof. □

Remark 5.6. For $D = 2521$, the conditions in Propositions 4.1, 5.2 and 5.5 are fulfilled, and in fact all of the relevant genus 1 curves have rational points. But we will show in Corollary 8.1 that $C_{2521}(\mathbb{Q}) = \emptyset$.

6. The Mordell–Weil sieve

In this section we develop a method to test when C_D has no rational points based on the Mordell–Weil sieve (see [22], [15], [20], [27], [7]).

The idea is the following: suppose we have a curve C defined over a number field K together with a map $\phi : C \to A$ to an abelian variety A defined over K. We want to show that $C(K) = \emptyset$, and we know that $\phi(C(K)) \subset H \subset A(K)$, where H is a certain subset of $A(K)$. Let $\wp$ be a prime of K and consider the reduction at $\wp$ of all the objects $\phi_\wp : C_\wp \to A_\wp$, together with the reduction maps $\mathrm{red}_\wp : A(K) \to A(k_\wp)$, where $k_\wp$ is the residue field at $\wp$. Now, we have that $\mathrm{red}_\wp(C(K)) \subset \phi_\wp(C(k_\wp)) \cap \mathrm{red}_\wp(H)$, so

$$\phi(C(K)) \subset H^{(\wp)} := \mathrm{red}_\wp^{-1}\big(\phi_\wp(C(k_\wp)) \cap \mathrm{red}_\wp(H)\big).$$

After considering enough primes, it can occur that

$$\bigcap_{\text{some primes } \wp} H^{(\wp)} = \emptyset,$$

yielding that $C(K) = \emptyset$.

In our case, we consider the curve C_D together with a map $\phi : C_D \to E^{(1)}$, where $E^{(1)}$ is the curve given by the Weierstrass equation $y^2 = x(x+2)(x+6)$. The curve $E^{(1)}$ has Mordell–Weil group $E^{(1)}(\mathbb{Q})$ generated by the 2-torsion points and $P := (6, 24)$.

Lemma 6.1. *Let D be a square-free integer, and consider the curve C_D, together with the map $\phi : C_D \to E^{(1)}$ defined by*

$$\phi([x_0 : x_1 : x_2 : x_3 : x_4]) := \Big(\frac{6x_0^2}{x_4^2}, \frac{24x_0x_1x_2}{x_4^3}\Big).$$

Let $P := (6, 24) \in E^{(1)}(\mathbb{Q})$. Then

$$\phi(C_D(\mathbb{Q})) \subset H := \{kP \mid k \text{ odd}\}.$$

Proof. This lemma is an easy application of the 2-descent method. The map ϕ is the composition of two maps. First, the forgetful map from C_D to the genus one curve in $\mathbb{P}^3$ given by the equations

$$\begin{cases} F_{014} := 3X_0^2 - 4X_1^2 + X_4^2 = 0, \\ F_{024} := X_0^2 - 2X_2^2 + X_4^2 = 0, \end{cases}$$

given by sending $[x_0 : x_1 : x_2 : x_3 : x_4]$ to $[x_0 : x_1 : x_2 : x_4]$. Multiplying F_{014} by 2 and F_{024} by 6 we obtain the equations

$$\begin{cases} 6X_0^2 - 2(2X_1)^2 = -2X_4^2, \\ 6X_0^2 - 12X_2^2 = -6X_4^2 \end{cases}$$

of a 2-descendent. The second map is the corresponding 4-degree map $\phi_{6,2}$ from these curves to $E^{(1)}$ given by the equations above, and determines that the element $(6, 2)$ is contained in $S^{(2)}(E^{(1)}/\mathbb{Q})$, so $\phi(C_D(\mathbb{Q}))$ is contained in the subset of elements (x, y) of $E^{(1)}(\mathbb{Q})$ with $\psi((x, y)) := (x, x + 2) = (6, 2)$ in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$. However, $P := (6, 24) \in E^{(1)}(\mathbb{Q})$ is a generator of $E^{(1)}(\mathbb{Q})/E^{(1)}(\mathbb{Q})[2]$, and has $\psi(6, 24) = (6, 2)$, hence any such point (x, y) is an odd multiple of P. □

For any prime q, we will denote by $H_D^{(q)} \subset H$ the subset corresponding to

$$H_D^{(q)} := \mathrm{red}_q^{-1}\left(\phi_q(C_D(\mathbb{F}_q)) \cap \mathrm{red}_q(H)\right).$$

First, consider the reduction modulo a prime q dividing D, so a prime of bad reduction. Suppose we have a point $[x_0 : x_1 : x_2 : x_3 : x_4]$ of C_D, so x_0^2, x_1^2, x_2^2, Dx_3^2 and x_4^2 are coprime integers in arithmetic progression. By reducing modulo q one gets that x_0^2, x_1^2, x_2^2, 0 and x_4^2 are in arithmetic progression modulo q, so, after dividing by x_4^2, we may suppose that the arithmetic progression is $-3, -2, -1, 0, 1$.

Proposition 6.2. *Let $q > 3$ be a prime number dividing D. Then*

$$H_D^{(q)} = \left\{kP \mid k \text{ odd and } x(kP) \equiv -18 \pmod{q}\right\},$$

and $H_D^{(q)}$ is independent of D.

Proof. This is an easy application of the ideas above. Since the only points in the reduction of C_D are the ones having $x_0^2 = -3$, $x_1^2 = -2$, $x_2^2 = -1$ and $x_4^2 = 1$, the set $\phi_q(C_D(\mathbb{F}_q))$ contains at most the two points having x-coordinate equal to $6(-3) = -18$. □

Corollary 6.3. *Suppose that $q > 3$ is a prime number such that* $\mathrm{red}_q(H)$ *contains a point Q with $x(Q) \equiv -18 \pmod{q}$. Then infinitely many pairs of square-free integers D and primitive tuples $[x_0 : x_1 : x_2 : x_3 : x_4] \in C_D(\mathbb{Q})$ exist, such that either q divides D or $x_3 \equiv 0 \pmod{q}$.*

Proof. Let O_q be the order of P modulo q, and let k be such that $x(kP) \equiv -18 \pmod{q}$. Then $x(k'P) \equiv -18 \pmod{q}$ for all $k' \equiv k \pmod{O_q}$. So, if k is odd or O_q is odd, $H^{(q)}$ has infinitely many elements. For any point $Q \in H^{(q)}$, we have that $x(Q) = 6z^2$, for certain $z \in \mathbb{Q}$, such that $z^2 \equiv -3 \pmod{q}$. Write $z = a/b$ with a and $b \in \mathbb{Z}$ and coprime. Then, if we denote by $r := (a^2 - b^2)/4$, then $r \in \mathbb{Z}$ and $x_i := a^2 + ir$ are squares for $i = 0, 1, 2$ and 4, and $a^2 + 3r \equiv 0 \pmod{q}$. Define D as the square-free part of $a^2 + 3r$, and we obtain the result by defining x_3 such that $a^2 + 3r = Dx_3^2$. □

Observe, however, that we do not obtain that $C_q(\mathbb{Q}) \neq \emptyset$ for the primes satisfying the hypothesis of the previous corollary. For example, the prime $q = 457$ satisfies the conditions of the corollary, but we will show that $C_{457}(\mathbb{Q}) = \emptyset$.

Now we will consider primes $q > 3$ that do not divide D, and are hence good reduction primes. We will obtain conditions depending on D being a square or not modulo q.

Proposition 6.4. *Let $q > 3$ be a prime number that does not divide D. Then $H_D^{(q)} \subset E^{(1)}(\mathbb{Q})$ depends only on the Legendre symbol (D/q). If we denote by $H^{(q),(D/q)}$ the subgroup corresponding to any (D/q), and by O_q the order of $P \in E^{(1)}(\mathbb{Q})$ modulo q, we have that there are subsets $M_1^{(q)}$ and $M_{-1}^{(q)}$ of $\mathbb{Z}/O_q\mathbb{Z}$ such that*

$$H^{(q),(D/q)} = \{kP \mid k \text{ odd and } \exists m \in M_{(D/q)}^{(q)} \text{ such that } k \equiv m \pmod{O_q}\}.$$

Moreover, $1 \in M_1^{(q)}$ for any $q > 3$, and if $k \in M_{(D/q)}^{(q)}$, then $-k \in M_{(D/q)}^{(q)}$.

Proof. First we show that $H_D^{(q)}$ only depends on (D/q). Suppose that $D \equiv D'a^2 \pmod{q}$, for some $a \neq 0 \in \mathbb{F}_q$. Then the morphism given by $\theta([x_0 : x_1 : x_2 : x_3 : x_4]) = [x_0 : x_1 : x_2 : x_3 a^2 : x_4]$ determines an isomorphism between $C_{D'}$ and C_D defined over $\mathbb{F}_q$, clearly commuting with ϕ, which does not depend on x_3.

In order to define $M_{(D/q)}^{(q)}$, one computes $\phi_q(C_D(\mathbb{F}_q))$ and then intersects it with the subset $\{kP \mid k \text{ odd}\}$ of $E^{(1)}(\mathbb{F}_q)$. Then

$$M_{(D/q)}^{(q)} := \{k \in \mathbb{Z}/O_q\mathbb{Z} \mid kP \in \phi_q(C_D(\mathbb{F}_q))\}.$$

Hence k belongs to $M_{(D/q)}^{(q)}$ if there is some $Q := [x_0 : x_1 : x_2 : x_3 : x_4] \in C_D(\mathbb{F}_q)$ such that $\phi(Q) = kP$. But then $\phi([-x_0 : x_1 : x_2 : x_3 : x_4]) = -kP$.

Finally, if $(D/q) = 1$, we can suppose $D \equiv 1 \pmod{q}$. But then $Q_0 := [1 : 1 : 1 : 1 : 1] \in C_D(\mathbb{F}_q)$, and $\phi(Q_0) = P$. □

The following table shows some examples of $M_{\pm 1}^{(q)}$ for $5 < q < 30$ prime.

q	O_q	$M_1^{(q)}$	$M_{-1}^{(q)}$
7	6	$\{\pm 1\}$	$\{3\}$
11	8	$\{\pm 1\}$	$\{\pm 3\}$
13	6	$\{\pm 1\}$	$\{3\}$
17	6	$\{\pm 1, 3\}$	$\{\ \}$
19	8	$\{\pm 1\}$	$\{\pm 3\}$
23	3	$\{1, 2, 3\}$	$\{\ \}$
29	16	$\{\pm 1\}$	$\{\pm 3, \pm 5, \pm 7\}$

We are going to use the previous result to obtain conditions on D.

Corollary 6.5. *If $C_D(\mathbb{Q}) \neq \emptyset$ then D satisfies the following conditions:*

(i) *D is a square modulo 17, 23, 41, 191, 281, 2027, and 836477.*

(ii) $(D/7) = (D/13)$, $(D/11) = (D/19) = (D/241)$, $(D/47) = (D/73)$, $(D/149) = (D/673)$, $(D/43) = (D/1723)$, $(D/175673) = (D/2953)$, $(D/97) = (D/5689) = (D/95737)$, $(D/577) = (D/2281)$, $(D/83) = (D/4391) = (D/27449)$, $(D/67) = (D/136319)$, $(D/2111) = (D/2521)$.

(iii) *If* $(D/29)=1$ *then* $(D/11)=1$. *If* $(D/149)=1$ *then* $(D/31)=1$. *If* $(D/7019) = 1$ *then* $(D/8123) = 1$. *If* $(D/617) = 1$ *then* $(D/37) = 1$, *and in this case* $(D/7) = 1$.

(iv) *If* $(D/83) = -1$ *then* $(D/11) = -1$. *If* $(D/2347) = -1$ *then* $(D/47) = -1$. *If* $(D/10369) = -1$ *then* $(D/47) = -1$.

Proof. We have computed the sets $M_1^{(q)}$ and $M_{-1}^{(q)}$ for $q < 10^6$ and $O_q \leq 200$. The algorithm to obtain the conditions for the statement is as follows: fix an integer $k \leq 200$ and compute the primes q such that $O_q = k$ and $5 < q < 10^6$. For these primes compute $M_1^{(q)}$ and $M_{-1}^{(q)}$. If $M_{-1}^{(q)}$ is empty, then $(D/q) = 1$ and we obtain (i). If these sets are equal for different primes, then we obtain (ii). Now, for any integer $m > 1$ such that $mk \leq 200$, compute the primes $p < 10^6$ such that $O_p = mk$. Compute $M_1^{(p)}$ and $M_{-1}^{(p)}$. Now check if $M_1^{(p)}$ (resp. $M_{-1}^{(p)}$) mod k is equal to some of the sets $M_1^{(q)}$ (resp. $M_{-1}^{(q)}$) computed above. If this occurs, then we obtain the rest of the conditions.

For example, looking at the previous table we see that $M_{-1}^{(17)} = \{\}$, therefore $(D/17) = 1$. Now, $O_7 = O_{13}$, $M_1^{(7)} = M_1^{(13)}$ and $M_{-1}^{(7)} = M_{-1}^{(13)}$ so we have $(D/7) = (D/13)$. Finally, $O_{29} = 2O_{11}$ and $M_1^{(29)}$ mod O_{11} is equal to $M_1^{(11)}$ and then we obtain that if $(D/29) = 1$ then $(D/11) = 1$. □

7. Computing all the points for $D = 409$

We want to find all the rational points of the curve C_D when we know there are some. We will concentrate at the end on the case $D = 409$, which is the first number that passes all of the tests (see Corollary 8.1), but in most of the section we can suppose that D is any prime integer fulfilling the conditions in Proposition 4.1. Observe first that we do have the 16 rational points $[\pm 7, \pm 13, \pm 17, 1, \pm 23] \in C_{409}(\mathbb{Q})$. Our aim is to show that there are no others.

In recent years, some new techniques have been developed for computing all the rational points of a curve of genus greater than one over $\mathbb{Q}$. These techniques work only under some special hypotheses. For example, Chabauty's method (see [8], [9], [14], [26], [27], [19]) can be used when the Jacobian of the curve has rank less than the genus of the curve, or even when there is a quotient abelian variety of the Jacobian with rank less than its dimension. In our case, however, the Jacobian of the curve C_D is isogenous to a product of elliptic curves, each with rank at least one (in fact, the Jacobian of C_D must have rank ≥ 8 by Proposition 5.2). So we cannot apply this method. Other methods, like the Dem'janenko–Manin's method [13], [18], cannot be applied either. We will instead apply the covering collections technique, as developed by Coombes and Grant [10], Wetherell [28] and others, and specifically a modification of what is now called the elliptic curve Chabauty method developed by Flynn and Wetherell in [16] and by Bruin in [5], [4].

The idea is as follows: suppose we have a curve C over a number field K and an unramified map $\chi : C' \to C$ of degree greater than one, and defined over K. We consider the distinct unramified coverings $\chi^{(s)} : C'^{(s)} \to C$ formed by twists of the given one, and we obtain that

$$C(K) = \bigcup_s \chi^{(s)}(C'^{(s)}(K)),$$

the union being disjoint. In fact, only a finite number of twists do have rational points, and the finite (larger) set of twists with points locally everywhere can be explicitly described. Now one hopes to be able to compute the rational points of all the curves $C'^{(s)}$, and therefore also of the curve C.

We will consider degree 2 coverings of C_D. To construct such coverings, we will use the description given by Bruin and Flynn in [6] of the 2-coverings of curves which are 2-coverings of the projective line. In our case, C_D is not of such form, but a quotient of C_D is of this form. Therefore we will use a 2-covering for such a quotient. Specifically, we will use one of the five genus 1 quotients, particularly the quotient

$$F_D^{(4)} : DX_3^2 = t^4 - 8t^3 + 2t^2 + 8t + 1\,,$$

along with the forgetful map $\phi^{(4)} : C_D \longrightarrow F_D^{(4)}$ given by $t = (X_0 - X_1)/(X_2 - X_1)$.

Observe first that the curve C_D has $\mathbb{Q}$-defined automorphisms τ_i of order 2 defined by $\tau_i(x_j) = x_j$ if $j \neq i$, $\tau_i(x_i) = -x_i$. These, together with their compositions, generate a subgroup Υ of the automorphisms isomorphic to $(\mathbb{Z}/2\mathbb{Z})^4$. For every $\mathbb{Q}$-defined point of C_D, composing with these automorphisms gives 16 different points. Given $Q \in C_D(\mathbb{Q})$, we denote by T_Q the set of these 16 different points. Observe that $\phi^{(4)}(T_Q)$ is formed by 8 distinct points.

Lemma 7.1. *The involutions τ_0, τ_1, τ_2 and τ_3 give rise to the following involutions on $F_D^{(4)}$:*

$$\tau_0(t,X_3)=\left(\frac{1-t}{1+t},\frac{2X_3}{(1+t)^2}\right),\ \tau_1(t,X_3)=\left(\frac{-1}{t},\frac{X_3}{t^2}\right),\ \tau_2(t,X_3)=\left(\frac{t+1}{t-1},\frac{2X_3}{(t-1)^2}\right),$$

and $\tau_3(t, X_3) = (t, -X_3)$. Moreover, if $F_D^{(4)}(\mathbb{Q}) \neq \emptyset$ and $\psi : F_D^{(4)} \to E_D^{(0)}$ is an isomorphism, then the involutions of $E_D^{(0)}$ given by $\epsilon_i := \psi\tau_i\tau_3\psi^{-1}$ for $i = 0, 1, 2$, are independent of ψ. Specifically, $\epsilon_i = \epsilon_{R_i}$ for $R_0 = (0, 0)$, $R_1 = (-D, 0)$ and $R_2 = (-4D, 0)$, where ϵ_Q denotes the translation by $Q \in E_D^{(0)}$.

Proof. Checking the formulae for the involutions on $F_D^{(4)}$ is a straightforward computation.

First, we show that the involutions ϵ_i are independent of the fixed isomorphism ψ. In order to show this, recall that, in any elliptic curve, any involution ϵ that has no fixed points must be of the form $\epsilon_R(S) = S + R$, for a fixed 2-torsion point R. Since $\tau_i\tau_3$ has no fixed points in $F_D^{(4)}$, the corresponding involution ϵ_i in $E_D^{(0)}$ must be equal to some ϵ_{R_i}, hence, determined by the corresponding 2-torsion point R_i, which is equal to $\epsilon_i(0)$. Now, replacing the isomorphism ψ from $F_D^{(4)}$ to $E_D^{(0)}$ is equivalent to conjugating ϵ_i by a translation ϵ_Q of $E_D^{(0)}$ with respect to a point Q in $E_D^{(0)}$, so, in principle we obtain a new involution $\epsilon_{-Q}\epsilon_i\epsilon_Q$, again without fixed points. But $\epsilon_{-Q}\epsilon_i\epsilon_Q(0) = \epsilon_{-Q}(\epsilon_i(Q)) = \epsilon_{-Q}(Q + R_i) = R_i$, so $\epsilon_{-Q}\epsilon_i\epsilon_Q = \epsilon_i$.

Second, since ϵ_i is independent of the chosen isomorphism ψ, and also does not depend on the field K, we can work out with a field $K' := K(\sqrt{D})$ where we have $F_D^{(4)} \cong F_1^{(4)}$, so the proof is reduced to the case $D = 1$. In this case, a simple computation by choosing some point in $F_1^{(4)}(\mathbb{Q})$ shows that $\epsilon_i = \epsilon_{R_i}$ where $R_0 = (0, 0)$, $R_1 = (-1, 0)$ and $R_2 = (-4, 0)$ in $E_1^{(0)}$, which gives the result when we translate these points to the curve $E_D^{(0)}$. □

Now, we want to construct some degree two unramified coverings of $F_D^{(4)}$. All these coverings are, in this case, defined over $\mathbb{Q}$, but we are interested in special equations not defined over $\mathbb{Q}$. The idea is simple: first, write the polynomial $q(t) := t^4-8t^3+2t^2+8t+1$ as the product of two degree 2 polynomials (over some quadratic extension K). In the rest of this section, we will denote $K := \mathbb{Q}(\sqrt{2})$. Then we have the factorization $q(t) = q_1(t)q_2(t)$ over K where $q_1(t) := t^2 - (4+2\sqrt{2})t - 3 - 2\sqrt{2}$ and $q_2(t) := \overline{q_1}(t)$, where $\overline{z}$ denotes the Galois conjugate of $z \in K$ over $\mathbb{Q}$. We could have chosen other factorizations over other quadratic fields, but this one is especially suitable for our purposes as we will show in the sequel. Then, for any $\delta \in K$, the curves F'_δ defined in $\mathbb{A}^3$ by the equations

$$F'_\delta : \begin{cases} \delta y_1^2 = q_1(t) = t^2 - (4+2\sqrt{2})t - 3 - 2\sqrt{2} \\ (D/\delta)y_2^2 = q_2(t) = t^2 - (4-2\sqrt{2})t - 3 + 2\sqrt{2} \end{cases}$$

along with the map ν_δ that gives $X_3 = y_1y_2$ are all the twists of an unramified degree two covering of $F_D^{(4)}$. Observe that, for any δ and δ', such that $\delta\delta'$ is a square in K, we have an isomorphism between F'_δ and $F'_{\delta'}$. So we only need to consider the δ's modulo squares. This also means that we can suppose that $\delta \in \mathbb{Z}[\sqrt{2}]$. However, only very few of them are necessary in order to cover all the rational points of $F_D^{(4)}$. A method to show this type of result is explained in [6], but we will follow a different approach.

Lemma 7.2. *Let $D > 3$ be a prime number such that $F_D^{(4)}(\mathbb{Q}) \neq \emptyset$. Let $\alpha \in \mathbb{Z}[\sqrt{2}]$ be such that $\nu_\alpha(F'_\alpha(K)) \cap F_D^{(4)}(\mathbb{Q}) \neq \emptyset$. Then*

$$F_D^{(4)}(\mathbb{Q}) \subset \nu_\alpha(F'_\alpha(K)) \cup \nu_{\overline{\alpha}}(F'_{\overline{\alpha}}(K)) \cup \nu_{-\alpha}(F'_{-\alpha}(K)) \cup \nu_{-\overline{\alpha}}(F'_{-\overline{\alpha}}(K)).$$

Moreover, for any $Q \in C_D(\mathbb{Q})$, either

$$\phi^{(4)}(T_Q) \cap \nu_\alpha(F'_\alpha(K)) \neq \emptyset \quad \text{or} \quad \phi^{(4)}(T_Q) \cap \nu_{-\overline{\alpha}}(F'_{-\overline{\alpha}}(K))) \neq \emptyset.$$

Proof. Observe that, for any point $P \in F_D^{(4)}$, an easy calculation shows that

$$q_1(t(\tau_0(P))) = \frac{2}{(1+t(P))^2} q_1(t(P)) \;\text{ and }\; q_1(t(\tau_1(P))) = -\frac{(1+\sqrt{2})^2}{(t(P))^2} q_2(t(P)),$$

where $t(R)$ denotes the t-coordinate of the point R. This implies that, if P is in $\nu_\alpha(F'_\alpha(K)) \cap F_D^{(4)}(\mathbb{Q})$, then $\tau_0(P)$ and $\tau_3(P)$ also are, and $\tau_1(P)$ and $\tau_2(P)$ are in $\nu_{-\overline{\alpha}}(F'_{-\overline{\alpha}}(K)) \cap F_D^{(4)}(\mathbb{Q})$. This last fact shows the last assertion of the lemma.

Now, using a fixed point $P \in F_D^{(4)}(\mathbb{Q})$, we choose $\alpha \in \mathbb{Z}[\sqrt{2}]$ such that $P \in \nu_\alpha(F'_\alpha(K))$, and an isomorphism ψ_P of $F_D^{(4)}$ with Jacobian $E := E_D^{(0)}$, by sending P to 0 (this isomorphism is determined, modulo signs, by this fact). Via this isomorphism, one can identify the degree two unramified covering ν_α with a degree two isogeny $\widetilde{\nu} : E' \to E$. Recall that E has the Weierstrass equation $y^2 = x^3 + 5Dx^2 + 4D^2x$, and that the degree two isogenies are determined by a nontrivial 2-torsion point.

By Lemma 7.1, we have $\psi_P(\tau_0\tau_3(P)) = \epsilon(0) = (0,0)$. But $\tau_0\tau_3(P)$ also belongs to $\nu_\alpha(F'_\alpha(K))$, and hence $(0,0)$ must be in $\widetilde{\nu}(E'(\mathbb{Q}))$, thereby determining the isogeny as the one corresponding to $(0,0)$.

Now we use the standard descent via a 2-isogeny. One obtains that the quotient $E(\mathbb{Q})/\widetilde{\nu}(E'(\mathbb{Q}))$ is mapped injectively to the subgroup of $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ generated by -1 and the prime divisors of $4D^2$. Since D is prime, the only possibilities are -1, 2 and D, which become only -1 and D over $K^*/(K^*)^2$. Hence, we need only four twists of $\widetilde{\nu}$ over K in order to cover all the points of $E(\mathbb{Q})$. Note that the twist corresponding to 1 is identified with ν_α. To find the twist corresponding to -1 one can argue in the following way: when replacing the field K with $K(\sqrt{-1})$, -1 becomes equal to 1 modulo squares and not to D or $-D$, and the same applies to α and $-\alpha$. Hence -1 is identified with $\nu_{-\alpha}$. A similar argument, but postulating that $\alpha\overline{\alpha}$ is equal to D modulo squares in K, shows that D corresponds to $\nu_{\overline{\alpha}}$. □

In order to obtain some coverings of C_D from these coverings of $F_D^{(4)}$ we write C_D in a different form, the one given by the following equations in $\mathbb{A}^3$:

$$C_D : \left\{ DX_3^2 = q(t),\; X_4^2 = p(t) \right\}, \tag{7.1}$$

where $p(t) = t^4 - 12t^3 + 2t^2 + 12t + 1$. Then, Lemma 7.2 implies that any rational point of C_D, modulo the automorphisms in Υ, comes from a point in K of one of the curves C'_δ, with $\delta = \alpha$ or $\delta = -\alpha$, given by the following equations in $\mathbb{A}^4$:

$$C'_\delta : \left\{ \delta y_1^2 = q_1(t),\; (D/\delta)y_2^2 = q_2(t),\; X_4^2 = p(t) \right\}$$

(and, moreover, with $t \in \mathbb{Q}$) by the natural map μ_δ. Observe, before continuing, that any rational point in C_D comes from a point in the affine part in the previous form, which is singular at infinity, since D is not a square in $\mathbb{Q}$.

Now we consider the hyperelliptic quotient H_δ of the curve C'_δ, which can be described by the equation

$$H_\delta\,:\,\delta W^2=q_1(t)p(t),$$

where the quotient map η is determined by saying that $W=y_1X_4$.

The proof of the following lemma is a simple computation.

Lemma 7.3. *Let E_δ be the elliptic curve defined by the equation*

$$E_\delta\,:\,\delta y^2=x^3+5\sqrt{2}x^2-x.$$

Then, the equation

$$\varphi:H_\delta\to E_\delta\,,\quad \varphi(t,W)=\Big(\frac{-2(-3+2\sqrt{2})q_1(t)}{(t-\sqrt{2}+1)^2},\frac{3(-4+3\sqrt{2})W}{(t-\sqrt{2}+1)^3}\Big)$$

determines a nonconstant morphism from the genus 2 curve H_δ to E_δ.

Remark 7.4. The group of automorphism of the genus 2 curve H_δ is generated by a non-hyperelliptic involution τ and by the hyperelliptic involution ω. Then, we have that the elliptic curve E_δ is $H_\delta/\langle\tau\rangle$. The other elliptic quotient E'_δ is obtained by $\tau\omega$; that is, $E'_\delta=H_\delta/\langle\tau\omega\rangle$. It is easy to compute that $E'_\delta\,:\,\delta y^2=x^3+9\sqrt{2}x^2-81x$. Therefore, $\mathrm{Jac}(H_\delta)$ is $\mathbb{Q}(\sqrt{2})$-isogenous to $E_\delta\times E'_\delta$. Moreover, E_1 and E'_1 are $\mathbb{Q}(\sqrt{2})$-isomorphic respectively to `384f2` and `384c2` in Cremona's tables, so E_δ and E'_δ are δ-twists of them.

Remark 7.5. The fact that H_δ has an elliptic quotient defined over K is the main reason we consider these specific 2-coverings of C_D. If we carry out the same arguments with other 2-coverings, coming from 2-coverings of $F_D^{(4)}$ or from 2-coverings of other genus 1 quotients $F_D^{(i)}$, we will not obtain such a quotient defined over a quadratic extension of $\mathbb{Q}$.

In the following proposition we will determine a finite subset of $E_\delta(K)$ containing the image of the points Q in $C_\delta(K)$ such that $\mu_\delta(Q)\in C_D(\mathbb{Q})$.

Proposition 7.6. *Let $D>3$ be a prime number such that $C_D(\mathbb{Q})\neq\emptyset$. Consider $P\in C_D(\mathbb{Q})$. Then $\tau\in\Upsilon$ exists such that $\tau(P)=\mu_\delta(Q)$ for $\delta=\alpha$ or $\delta=-\alpha$, with $Q\in C'_\delta(K)$. Let $R:=\varphi(\eta(Q))\in E_\delta(K)$ be the corresponding point in E_δ. Then*

$$R\in\Big\{(x,y)\in E_\delta(K)\;\Big|\;\pi(x,y):=\frac{2(-4+2\sqrt{2}-x(1-\sqrt{2}))}{(6-4\sqrt{2}-x)}\in\mathbb{Q}\Big\}.$$

Proof. Part of the lemma is a summary of what we have proved in lemmas above. Only the last assertion needs a proof. Suppose we have a point $Q\in C'_\delta(K)$ such that $\mu_\delta(Q)\in C_D(\mathbb{Q})$. Then the t-coordinate of Q is in $\mathbb{Q}$, since μ_δ leaves the t-coordinate unchanged. This implies that the x-coordinate of $R:=\varphi(\eta(Q))$, that is $\frac{-2(-3+2\sqrt{2})q_1(t)}{(-1+\sqrt{2}-t)^2}$, must come from a rational number t. This again implies that the sum of the t-coordinates of the two preimages of R is a rational number, but this sum can be expressed in the x-coordinate of R as $\pi(x,y)$. □

The following diagram illustrates all the curves and morphisms involved in our problem:

$$\begin{tikzcd}
 & C'_\delta \arrow[dl, "\mu_\delta"'] \arrow[dd] \arrow[dr, "\eta"] & & \\
C_D \arrow[d, "\phi^{(4)}"'] & & H_\delta \arrow[d, "\varphi"] & \\
F_D^{(4)} & F'_\delta \arrow[l, "\nu_\delta"'] & E_\delta \arrow[r, "\pi"] & \mathbb{P}^1
\end{tikzcd}$$

Hence, to find all the points in $C_D(\mathbb{Q})$, it is enough to find all the points (x, y) in $E_\delta(K)$ such that $\pi(x, y) \in \mathbb{Q}$ for $\delta = \alpha$ or $\delta = -\alpha$. But this is what the so-called elliptic curve Chabauty method does, if the rank of the group of points $E_\delta(K)$ is less than or equal to 1. And this seems to be the case in the cases we are considering.

Example 7.7. Let us consider the case $D = 409$. The 16 points $[\pm 7, \pm 13, \pm 17, 1, \pm 23]$ give the 8 points in $F_{409}^{(4)}$ with $t \in \{-3/2, -5, 2/3, 1/5\}$. Take $\alpha := 21 + 4\sqrt{2}$, which satisfies the hypothesis of Lemma 7.2. Then the 8 points in C_{409} with $t = -3/2$ and $t = -5$ come from the 16 points in C'_α given by $[t, y_1, y_2, X_4] = [-3/2, \pm 1/2, \pm 1/2, \pm 23/4]$ and $[-5, \pm\sqrt{2}, \pm\sqrt{2}, \pm 46]$ respectively, which in turn give the 4 points in H_α given by $[t, W] = [-3/2, \pm 23/8]$ and $[-5, \pm 46\sqrt{2}]$. Finally, these 4 points give the following 2 points E_α:

$$\left(\frac{-2}{49}(-663 + 458\sqrt{2}), \pm\frac{69}{343}(-232 + 163\sqrt{2})\right).$$

The other points with $t = 2/3$ and $t = 1/5$ give rise to points in $E_{-\overline{\alpha}}(K)$, as shown in Lemma 7.2. We will show that these points in $E_\alpha(K)$ are the only points R with $\pi(R) \in \mathbb{Q}$, and that there are no such points in $E_{-\alpha}(K)$.

7.1. The elliptic curve Chabauty method

In order to apply the elliptic curve Chabauty technique [5], [4], we first need to fix a rational prime p such that p is inert over K and E_δ has good reduction over p. The smallest such prime satisfying our conditions is $p = 5$, since by Proposition 4.1 we have $D \equiv \pm 1 \pmod{5}$. Denote by $\widetilde{E_\delta}$ the reduction modulo 5 of E_δ, which is an elliptic curve over $\mathbb{F}_{25} := \mathbb{F}_5(\sqrt{2})$. Then the elliptic curve Chabauty method will allow us to bound, for each point $\widetilde{R}$ in $\widetilde{E_\delta}(\mathbb{F}_{25})$, the number of points R in $E_\delta(K)$ reducing to the point $\widetilde{R}$, and such that $\pi(R) \in \mathbb{Q}$, if the rank of the group of points $E_\delta(K)$ is less than or equal to 1. In the next lemma we will show that, in fact, we only need to consider four (or two) points in $\widetilde{E_\delta}(\mathbb{F}_{25})$, instead of all 32 points.

Lemma 7.8. *Let D be a square-free integer such that $D \equiv \pm 1 \pmod{5}$, and let $\delta \in \mathbb{Z}[\sqrt{2}]$ and $Q \in C'_\delta(K)$ be such that $\mu_\delta(Q) \in C_D(\mathbb{Q})$. Let $R := \varphi(\eta(Q)) \in E_\delta(K)$ be the corresponding point in E_δ. Then $\pi(R) \equiv -1 \pmod{5}$ or $\pi(R) \equiv \infty \pmod{5}$.*

Moreover, if the rank of the group of points $E_\delta(K)$ is equal to 1*, the torsion subgroup has order* 2*, and the reduction of the generator has order* 4*, then only one of the two cases can occur.*

Proof. We repeat the whole construction of the coverings, but modulo 5. First, observe that, since $D \equiv \pm 1 \pmod 5$, the only $\mathbb{F}_5$-rational points of $\widetilde{C_D}$ are the ones with coordinates $[\pm 1 : \pm 1 : \pm 1 : 1 : \pm 1]$. So the t-coordinates of these points are $t = 0, 1, 4$ and ∞. Substituting these values in $q_1(t)$ modulo 5, we always obtain squares in $\mathbb{F}_{25}$. This implies that the twists of the curves involved are all isomorphic modulo 5 to the curves with $\delta = 1$.

Consider the curve $\widetilde{H_1}$ over $\mathbb{F}_{25}$. A simple computation shows that the only points in $\widetilde{H_1}$ whose t-coordinates are $\mathbb{F}_5$-rational are the points with $t = 0$, $t = 1$ and the two points at infinity. Now, the images under φ in $\widetilde{E_1}$ of these points are equal to the points with x-coordinate equal to $-\overline{\xi} = -1 + \sqrt{2}$ in the first two cases, and equal to $\xi = 1 + \sqrt{2}$ for the points at infinity. In the first case we have $\pi(-1+\sqrt{2}) \equiv -1 \pmod 5$, and in the second case we have $\pi(1+\sqrt{2}) \equiv \infty \pmod 5$.

Now, the curve $\widetilde{E_1}$, given by the equation $y^2 = x^3 + 4x$, has 32 rational points over $\mathbb{F}_{25}$, and $\widetilde{E_1}(\mathbb{F}_{25}) \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ as abelian group, with generators points P_4 and P_8 with x-coordinates equal to $\xi = 1 + \sqrt{2}$ and $\sqrt{2}\xi = 2 + \sqrt{2}$ respectively. We then obtain that

$$\left\{R \in \widetilde{E_1}(\mathbb{F}_{25}) \ |\pi(R) = \infty\right\} = \left\{P_4, -P_4\right\}$$

and

$$\left\{R \in \widetilde{E_1}(\mathbb{F}_{25}) \ |\pi(R) = -1\right\} = \left\{2P_8 + P_4, -2P_8 - P_4\right\}.$$

Now, if the rank of the group of points $E_\delta(K)$ is less than or equal to 1, the torsion subgroup has order 2, and the reduction of the generator has order 4, then the reduction of $E_\delta(K)$ is a subgroup of $\widetilde{E_1}(\mathbb{F}_{25})$ isomorphic to $\mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$. However, the subgroup generated by P_4 and $2P_8 + P_4$ is isomorphic to $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$, and therefore the reduction cannot contain both points. □

In order to use the elliptic curve Chabauty method, it is advisable to transform the equation that gives E_δ into a Weierstrass equation, by employing the standard transformation sending (x, y) to $(\delta x, \delta y)$. We obtain the equation

$$y^2 = x^3 + 5\sqrt{2}\delta x^2 - \delta^2 x.$$

Abusing notations, we will denote this elliptic curve by E_δ. Moreover, the map π becomes the map $f : E_\delta \to \mathbb{P}^1$, given by

$$f(x) := \frac{(2\sqrt{2} - 2)x + \delta(4\sqrt{2} - 8)}{\delta(-4\sqrt{2} + 6) - x}.$$

Let us explain first the idea of the elliptic curve Chabauty method. For a given D, we fix a $\delta = \alpha$ or $\delta = -\alpha$, and we want to compute the set

$$\Omega_\delta := \left\{Q \in E_\delta(K) \mid f(Q) \in \mathbb{Q} \text{ and } f(Q) \equiv -1, \infty \pmod 5\right\}.$$

As we have already remarked, we need first to compute the rank of the group $E_\delta(K)$, which should be less than or equal to one. We will also need to know explicitly the

the torsion subgroup of this group, and some non-torsion point if the rank is 1, which is not an ℓ-multiple of a K-rational point for some primes ℓ to be determined (in our cases, they will occur only $\ell = 2$). In the cases where we already know some points in $E_\delta(K)$, those coming from the known points in $C_D(\mathbb{Q})$, we will show that those points are non-torsion points.

We have two cases to consider. The first such case is when we do not know any point $R \in E_\delta(K)$ such that $f(R) \in \mathbb{Q}$. In such a case we show that $\Omega_\delta = \emptyset$ by proving that the reduction of the group $E_\delta(K)$ does not contain any point $\widetilde{Q}$ such that $\widetilde{f}(\widetilde{Q}) \in \mathbb{F}_5$. We do this for the two cases in the following lemma.

Lemma 7.9. *Take $D = 409$ and $\alpha = 21 + 4\sqrt{2}$. Then the elliptic curves E_α and $E_{-\alpha}$ have rank 1 over K and torsion subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z}$ (generated by the point $(0,0)$). The points $P = ((-30\sqrt{2} - 43)/2, (759\sqrt{2} + 1104)/4)$ in $E_\alpha(K)$ and the point $P' \in E_{-\alpha}(K)$ with x-coordinate equal to*

$$\frac{29769295809708\sqrt{2} + 42339835565318}{4185701809},$$

generate the free part of the corresponding Mordell–Weil group.

Moreover, if $R \in \Omega_{-\alpha}$ then $f(R) \equiv \infty \pmod 5$ and if $R \in \Omega_\alpha$ then $f(R) \equiv -1 \pmod 5$.

Proof. The first part of the previous statement was obtained by using the `MAGMA` function `DescentInformation`. For our elliptic curves E_α and $E_{-\alpha}$, this function has unconditionally computed that the rank of both elliptic curves is 1, and it has returned the generators of these Mordell–Weil groups.

The last assertions are shown by proving that the subgroup generated by the reduction modulo 5 of the point P' and the point $(0,0)$ does not contain any point with image by $\widetilde{f}$ equal to -1, and that the subgroup generated by the reduction modulo 5 of the point P and the point $(0,0)$ does not contain any point with image by $\widetilde{f}$ equal to ∞. These last two cases are in fact instances of the previous lemma, since the reductions of the points P and P' have order 4. □

Now, in order to show that $\Omega_{-\alpha}$ is, in fact, empty, we need to use information from some other primes. This is what we do in the following lemma.

Lemma 7.10. *Take $D = 409$ and $\alpha = 21 + 4\sqrt{2}$. Then $\Omega_{-\alpha} = \emptyset$.*

Proof. By using reduction modulo 5, we obtain that any point R in $\Omega_{-\alpha}$ must be of the form $R = (4n + 1)P' + (0,0)$ for some $n \in \mathbb{Z}$, since it must reduce to the point $\widetilde{P' + T}$, and the order of $\widetilde{P'}$ is 4.

Now we reduce modulo 13. One shows easily that the order of P' modulo 13 is equal to 24, and that the points $R \in E_{-\alpha}(K)$ such that $f(R) \in \mathbb{P}^1(\mathbb{Q})$ reduce to the points $6P'$ or $12P' + (0,0)$. Hence the points R must be of the form $R = (24n+6)P'$ or $(24n + 12)P' + (0,0)$. Comparing with the result obtained from the reduction modulo 5, we obtain the result that there is no such point. □

The second case is where we already know some points $R \in \Omega_\delta$. Then our objective will be to show there are no more, by showing that the set

$$\Omega_{\delta,R} := \bigl\{Q \in E_\delta(K) \mid Q \in \Omega_\delta \text{ and } Q \equiv R \,(\operatorname{mod} 5)\bigr\}$$

only contains the point R. This is done by translating the problem of computing the number of points in $\Omega_{\delta,R}$ into a problem of computing the number of p-adic zeros of some formal power series, and using Strassmann's theorem to do so.

Proposition 7.11. *Take $\alpha = 21 + 4\sqrt{2}$, and consider the point*

$$R = \Bigl(\frac{-2}{49}(-663 + 458\sqrt{2})\alpha, \frac{69}{343}(-232 + 163\sqrt{2})\alpha^2\Bigr).$$

Then

$$\Omega_\alpha = \bigl\{Q \in E_\alpha(K) \mid f(Q) \in \mathbb{Q} \text{ and } f(Q) \equiv -1 \,(\operatorname{mod} 5)\bigr\} = \bigl\{R, -R\bigr\}.$$

Proof. First observe that the order of the reduction of P modulo 5 is 4. Also, any point R' in Ω_α reduces modulo 5 to one of the points $\pm R$, so it is of the form $\pm R + 4nP$. We are going to prove there is only one point in Ω_α reducing to R, and we deduce the other case by using the -1-involution.

Observe that any point in $E_\alpha(K)$ that reduces to 0 modulo 5 is of the form $4nP$ for some $n \in \mathbb{Z}$. We are going to compute the z-coordinate of such points, where $z = -x/y$ if $P = (x, y)$, as a formal power series in n. Denote by z_0 the z-coordinate of $4P$. The idea is to use the formal logarithm $\log_E$ and the formal exponential $\exp_E$ of the formal group law associated to E_α. These are formal power series in z, one inverse to the other insofar as the composition is concerned, and such that

$$\log_E\bigl(z\text{-coord}(G + G')\bigr) = \log_E\bigl(z\text{-coord}(G)\bigr) + \log_E\bigl(z\text{-coord}(G')\bigr)$$

for any G and G' reducing to 0 modulo 5, and where the power series are evaluated in the completion of K at 5. Thus, we obtain that

$$z\text{-coord}(n(4P)) = \exp_E(n \log_E(z_0)),$$

which is a power series in n.

Now, we are going to compute $f(R + 4nP)$ as a power series in n. To do so, we use that, by the addition formulae,

$$x\text{-coord}(R + G) = \frac{w(z)(1 + y_0 w(z))^2 - (a_2 w(z) + z + x_0 w(z))(z - x_0 w(z))^2}{w(z)(z - x_0 w(z))^2}$$

where $R = (x_0, y_0)$, $a_2 = 5\sqrt{2}\alpha$, z is the z-coordinate of a point G reducing to 0 modulo 5, and $w(z) = -1/y$ evaluated as a power series in z. This function is a power series in z, starting as $x\text{-coord}(R + G) = x_0 + 2y_0 z + (3x_0^2 + 2a_2 x_0 + a_4)z^2 + O(z^3)$, where $a_4 = -\alpha^2 = y^2/x - (x^2 + 5\sqrt{2}\alpha x)$. Hence we obtain that $f(R+4nP) = f(x\text{-coord}(R+n(4P))$ can be expressed as a power series $\Theta(n)$ in n

with coefficients in K. We express this power series as $\Theta(n) = \Theta_1(n) + \sqrt{2}\Theta_2(n)$, with $\Theta_i(n)$ now being a power series in $\mathbb{Q}$. Then $f(R + 4nP) \in \mathbb{Q}$ for some $n \in \mathbb{Z}$ if and only if $\Theta_2(n) = 0$ for that n. Observe also that, since $f(R) \in \mathbb{Q}$, we will obtain that $\Theta_2(0) = 0$, so $\Theta_2(n) = j_1 n + j_2 n^2 + j_3 n^3 + \cdots$. To conclude, we will use Strassmann's theorem: if the 5-adic valuation of j_1 is strictly smaller than the 5-adic valuation of j_i for any $i > 1$, then this power series has only one zero at $\mathbb{Z}_5$, and this zero is $n = 0$. In fact, one can easily show that this power series satisfies that the 5-adic valuation of j_i is always greater or equal to i, so, if we show that $j_1 \not\equiv 0 \pmod{5^2}$ we have concluded.

In order to do all this explicitly, we will work modulo some power of 5. In fact, working modulo 5^2 will be sufficient. We have that $z_0 = z\text{-coord}(4P) \equiv -10\sqrt{2} + 5 \pmod{5^2}$, and that $z\text{-coord}(n(4P)) \equiv (15\sqrt{2} + 5)n \pmod{5^2}$. Finally, we obtain that $\Theta(n) \equiv 19 + (15\sqrt{2} + 20)n \pmod{5^2}$, hence $\Theta_2(n) \equiv 15n \pmod{5^2}$, so $j_1 \equiv 15 \pmod{5^2}$ which completes the proof. □

An alternative way of proving this result is to use the built-in `MAGMA` function `Chabauty`. The answer is that there are only 2 points R' in $E_\alpha(K)$ such that $f(R') \in \mathbb{Q}$, both having $f(R') = 13/2$. Since we already have two points $\pm R$, both giving $f(R) = 13/2$, we are done.

8. Explicit computations and conjectures

We have followed two different approaches to compute for which square-free integers D there are nonconstant arithmetic progressions of five squares over $\mathbb{Q}(\sqrt{D})$. On the one hand, for each D we have checked if D passes all the sieves from the previous sections, obtaining the following result.

Corollary 8.1. *Let $D < 10^{13}$ be a square-free integer such that $C_D(\mathbb{Q}) \neq \emptyset$, then $D = 409$ or $D = 4688329$.*

Proof. First, for each D we have checked all the local conditions (Proposition 4.1) and the conditions coming from the Mordell–Weil sieve (Corollary 6.5). Only 1048 values of D have passed these sieves. To discard all the values except $D = 409$ and $D = 4688329$, we first apply a test derived from Proposition 6.2. We test if, for any prime q dividing such D, there is an odd multiple kP of the point $P := (6, 24) \in E^{(1)}(\mathbb{Q})$ reducing to a point with x-coordinate equal to -18 modulo q. To explicitly verify this condition, we first compute if there is a point Q in $E^{(1)}(\mathbb{F}_q)$ with x-coordinate equal to -18, the order O_q of P in $E^{(1)}(\mathbb{F}_q)$ and the discrete logarithm $\log(Q, P)$, i.e., the number k such that $Q = kP$, if it exists. In case there is no such Q, or there is no such logarithm, or both k and O_q are even, then D does not pass the test. In the case that D passes this first test, we combine this information with the information from the computation of the $M_D^{(q)}$ for the first 100 primes to discard some other cases.

After this last test there are 34 values of D that survive, and we then employ a test based on the ternary forms criterion given by Proposition 5.5, by using a short program in SAGE implemented by Gonzalo Tornaria. We check that for these values $r(D, 3x^2+9y^2+16z^2) \neq r(D, x^2+3y^2+144z^2)$. Hence for those values of D, $L(E_D^{(2)}, 1) \neq 0$, so the analytic rank of $E_D^{(2)}$ is zero, hence their rank is also 0.

Only $D = 409$ and $D = 4688329$ survive all these tests, but for these values there are points in $C_D(\mathbb{Q})$. □

On the other hand, remember that if we take $t = (X_0 - X_1)/(X_2 - X_1)$ then an affine model of C_D is defined by:

$$C_D : \left\{ DX_3^2 = t^4 - 8t^3 + 2t^2 + 8t + 1,\ X_4^2 = t^4 - 12t^3 + 2t^2 + 12t + 1 \right\}.$$

Therefore the curve $F^{(3)}$ that consists of removing the variable X_3 from C_D has the equation $F^{(3)} : X_4^2 = t^4 - 12t^3 + 2t^2 + 12t + 1$, and a Weierstrass equation is given by $E^{(1)} : y^2 = x(x+2)(x+6)$. Then we have an isomorphism $\psi : E^{(1)} \longrightarrow F^{(3)}$ defined by

$$\psi(P) = \Big(\frac{6-x}{6+3x-y}, \frac{-72 - 108x - 18x^2 + x^3 + 48y}{(6+3x-y)^2} \Big),$$

if $P = (x,y) \neq (-2,0), (-3,-3), (6,24)$ and $\psi(6,24) = (2/3, 23/9)$, $\psi(-2,0) = \infty_1$ and $\psi(-3,-3) = \infty_2$, where ∞_1 and ∞_2 denote the two branches at infinity at the desingularization of $F^{(3)}$ at the unique singular point $[0:1:0] \in \mathbb{P}^2$. This construction allows us to construct all the nonconstant arithmetic progressions of five squares over all quadratic fields. Let $P = (2,-8)$ be a generator of the free part of $E^{(1)}(\mathbb{Q})$, and let n be a positive integer. Let $(t_n, z_n) = \psi([n]P)$. Now, consider the square-free factorization of the number

$$t_n^4 - 8t_n^3 + 2t_n^2 + 8t_n + 1 = D_n w_n^2,$$

where $D_n \in \mathbb{Z}$ is square-free, $w_n \in \mathbb{Q}$. Then the sequence

$$(-t_n^2 - 2t_n + 1)^2,\ (t_n^2+1)^2,\ (t_n^2 - 2t_n - 1)^2,\ D_n\, w_n^2,\ z_n^2$$

defines a nonconstant arithmetic progression of 5 squares over $\mathbb{Q}(\sqrt{D_n})$, and we have points $Q_n := [-t_n^2 - 2t_n + 1 : t_n^2 + 1 : t_n^2 - 2t_n - 1 : w_n : z_n] \in C_{D_n}(\mathbb{Q})$.

Remark 8.2. Observe that the pairs (D_n, Q_n) constructed in this way are different for different n. On the other hand, we cannot be sure that all the fields $\mathbb{Q}(\sqrt{D_n})$ are different. However, we do have an infinite number of integers D such that $C_D(\mathbb{Q}) \neq \emptyset$. This is because for any integer D, the curve C_D, being of genus 5 (greater than 1), always has a finite number of rational points. Since we have an infinite number of pairs (D_n, Q_n) with $Q_n \in C_{D_n}(\mathbb{Q})$, we have an infinite number of different D_n.

Remark 8.3. If we replace $[n]P$ by $Q \in \{[n_1]T_1 + [n_2]T_2 + [m]P_0 \,|\, n_1, n_2 \in \{0,1\}, m \in \{n, -n-1\}\}$, where $T_1 = (-2,0)$ and $T_2 = (-6,0)$ is a basis of $E^{(1)}(\mathbb{Q})_{\text{tors}}$, we obtain the same arithmetic progression (up to equivalence). Note that if $n = 0$, then we obtain $D_0 = 1$ and the previous sequence is the constant arithmetic progression.

In Tables 1 and 2 we summarize the computations that we have carried out using the previous algorithm. We have normalized the elements of the arithmetic progressions to be integers and to have no squares in common. We have separated the results into two tables. Table 1 gives n and the factorization of D_n appears. In Table 2, for each value of n, the corresponding factorization of X_0 appear. For all the values of n computed, we have obtained that the fourth element of the arithmetic progression is $\sqrt{D_n}$ (in our earlier notation, $w_n = 1$). That is, if we denote by $r = (D_n - X_0^2)/3$, then the sequence $\{X_k^2 = X_0^2 + k\,r \,|\, k \in \{0, \dots, 4\}\}$ defines an arithmetic progression over $\mathbb{Q}(\sqrt{D_n})$.

n	D_n
1	409
2	4688329
3	$457 \cdot 548240447113$
4	1995548940913036680732 01
5	$4343602906873 \cdot 5331395003998418925451 3$
6	$2593 \cdot 9697 \cdot 4100179090153 \cdot 29331869174167888116692693659 3$
7	33082351395282824357312248053607753315606400013911972464229586192 1
8	$24697 \cdot 303049 \cdot 921429638596379458921 \cdot 2918241104073873997601 53 \cdot 3462757049033071137768291886369$

Table 1. Factorization of D_n

n	X_0
1	7
2	$47 \cdot 89$
3	$31 \cdot 113 \cdot 577$
4	$7 \cdot 176201 \cdot 515087$
5	$2111 \cdot 133967 \cdot 1134755801$
6	$119183 \cdot 12622601 \cdot 2189366343649$
7	$2^{10} \cdot 3 \cdot 17 \cdot 73 \cdot 103787 \cdot 112261 \cdot 963877 \cdot 20581582583$
8	$2^{38} \cdot 3^{2} \cdot 5 \cdot 7 \cdot 23 \cdot 102179447 \cdot 1017098920090613939$

Table 2. Factorization of X_0

One can see that the size of the D_n we encounter grows very quickly, but we do not know if the D_n constructed in this way always satisfy $D_n < D_{n+1}$. We guess that this condition holds. Even more, the previous table and Corollary 8.1 suggest that, in fact, there is no square-free integer D such that $C_D(\mathbb{Q}) \neq \emptyset$ and $D_n < D < D_{n+1}$.

If we only use the results in Section 4 (Proposition 4.1) and Section 6 (Corollary 6.5), we obtain the result that the number of square-free integers D that pass both tests have positive (but small) density. This is possibly true if we also use the condition of the rank, for example Proposition 5.5, since the number of twists with positive rank of a fixed elliptic curve should also have positive density. However, we suspect that the number of square-free integers D such that C_D has rational points should have zero density.

Data. All the MAGMA and SAGE sources are available on the first author's webpage.

References

[1] Bombieri, E., Granville, A. and Pintz, J.: Squares in arithmetic progressions. *Duke Math. J.* **66** (1992), no. 3, 369–385.

[2] Bombieri, E. and Zannier, U.: A note on squares in arithmetic progressions. II. *Atti Accad. Naz. Lincei Cl. Sci. Fis. Mat. Natur. Rend. Lincei (9) Mat. Appl* **13** (2002), no. 2, 69–75.

[3] Bosma, W., Cannon, J. J., Fieker, C. and Steel, A.: *Handbook of Magma Functions.* Edition 2. 15–6, 2009. http://magma.maths.usyd.edu.au/magma/

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

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

[6] Bruin, N. and Flynn, E. V.: Towers of 2-covers of hyperelliptic curves. *Trans. Amer. Math. Soc* **357** (2005), no. 11, 4329–4347.

[7] Bruin, N. and Stoll, M.: The Mordell–Weil sieve: proving non-existence of rational points on curves. *LMS J. Comput. Math.* **13** (2010), 272–306.

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

[9] Coleman, R. F.: Effective Chabauty. *Duke Math. J* **52** (1985), no. 3, 765–770.

[10] Coombes, K. R. and Grant, D.: On heterogeneous spaces. *J. London Math. Soc. (2)* **40** (1989), no. 3, 385–397.

[11] Cremona, J. E.: *Algorithms for modular elliptic curves.* Cambridge University Press, Cambridge, 1992.

[12] Cremona, J. E.: Elliptic curve data. http://www.warwick.ac.uk/~masgaj/ftp/data/.

[13] Dem'janenko, V. A.: Rational points of a class of algebraic curves. *Izv. Akad. Nauk SSSR Ser. Mat.* **30** (1966), 1373–1396. English translation: *Amer. Math. Soc. Transl., Ser. II* **66** (Amer. Math. Soc., Providence, RI, 1968) 246–272.

[14] Flynn, E. V.: A flexible method for applying Chabauty's theorem. *Compositio Math.* **105** (1997), no. 1, 79–94.

[15] Flynn, E. V.: The Hasse principle and the Brauer–Manin obstruction for curves. *Manuscripta Math.* **115** (2004), no. 4, 437–466.

[16] Flynn, E. V. and Wetherell, J. L.: Covering collections and a challenge problem of Serre. *Acta Arith.* **98** (2001), no. 2, 197–205.

[17] González-Jiménez, E. and Steuding, J.: Arithmetic progressions of four squares over quadratic fields. *Publ. Math. Debrecen* **77** (2010), no. 1–2, 125–138.

[18] Manin, Y.: The p-torsion of elliptic curves is uniformly bounded. *Izv. Akad. Nauk SSSR Ser. Mat.* **33** (1969), 459–465.

[19] McCallum, W. and Poonen, B.: The method of Chabauty and Coleman. In *Explicit methods in Number Theory: rational points and diophantine equations.* Panoramas et Syntèses 36, Société Math. de France, 2012.

[20] Poonen, B.: Heuristics for the Brauer–Manin obstruction for curves. *Experiment. Math.* **15** (2006), no. 4, 415–420.

[21] Rohrlich, D. E.: Galois theory, elliptic curves, and root numbers. *Compositio Math.* **100** (1996), no. 3, 311-349.

[22] Scharaschkin, V.: *Local-global problems and the Brauer–Manin obstruction.* Ph.D. thesis, University of Michigan, 1999.

[23] Silverberg, A.: Open questions in arithmetic algebraic geometry. In *Arithmetic Algebraic Geometry,* 85–142. IAS/Park City Mathematics Series 9, Amer. Math. Soc., Providence, RI, 2001.

[24] Silverman, J. H.: *The arithmetic of elliptic curves.* Graduate Texts in Mathematics 106, Springer-Verlag, New York, 1986.

[25] Stein, W. et al.: *Sage: Open Source Mathematical Software (Version 4.0).* The Sage Group, 2009, http://www.sagemath.org.

[26] Stoll, M.: Independence of rational points on twists of a given curve. *Compos. Math.* **142** (2006), no. 5, 1201–1214.

[27] Stoll, M.: Finite descent obstructions and rational points on curves. *Algebra Number Theory* **1** (2007), no. 4, 349–391.

[28] Wetherell, J. L.: *Bounding the number of rational points on certain curves of high rank.* Ph.D. thesis, University of California, Berkeley, 1997.

[29] Xarles, X.: Squares in arithmetic progression over number fields. *J. Number Theory* **132** (2012), no. 3, 379–389.

[30] Yoshida, S.: Some variants of the congruent number problem. II. *Kyushu J. Math.* **56** (2002), no. 1, 147–165.

Received December 12, 2011; revised December 14, 2012.

Enrique González-Jiménez: Departamento de Matemáticas, Universidad Autónoma de Madrid and Instituto de Ciencias Matemáticas (ICMat), 28049 Madrid, Spain.
E-mail: enrique.gonzalez.jimenez@uam.es

Xavier Xarles: Departament de Matemàtiques, Universitat Autònoma de Barcelona, 08193 Bellaterra, Barcelona, Catalonia, Spain.
E-mail: xarles@mat.uab.cat

The first author was supported in part by grants MTM 2009-07291 (Ministerio de Ciencia e Innovación, Spain) and CCG08-UAM/ESP-3906 (Universidad Autónoma de Madrid, Comunidad de Madrid, Spain). The second author was partially supported by grant MTM 2009-10359 (Ministerio de Ciencia e Innovación, Spain).