Publ. Math. Debrecen
77/1-2 (2010), 125–138

Arithmetic progressions of four squares over quadratic fields

By ENRIQUE GONZÁLEZ-JIMÉNEZ (Madrid) and JÖRN STEUDING (Würzburg)

Abstract. Let d be a squarefree integer. Does there exist four squares in arithmetic progression over $\mathbb{Q}(\sqrt{d}\,)$? We shall give a partial answer to this question, depending on the value of d. In the affirmative case, we construct explicit arithmetic progressions consisting of four squares over $\mathbb{Q}(\sqrt{d}\,)$.

1. Introduction

Non-constant arithmetic progressions consisting of rational squares have been studied since ancient times. While it is not difficult to obtain an arithmetic progression of three rational squares (e.g. $1^2, 5^2, 7^2$), there are no four distinct rational squares in arithmetic progression as already stated by Fermat and proved by Euler (among others). However, the situation is different over number fields. It is easy to construct four squares in arithmetic progression over a quadratic number field; e.g. $1^2, 5^2, 7^2, (\sqrt{73}\,)^2$ over $\mathbb{Q}(\sqrt{73}\,)$. It is even possible to find five squares in arithmetic progressions; e.g. $7^2, 13^2, 17^2, (\sqrt{409}\,)^2, 23^2$ over $\mathbb{Q}(\sqrt{409}\,)$. By Faltings' proof of the Mordell conjecture [7] in any finite algebraic extension of $\mathbb{Q}$ there can be at most finitely many arithmetic progressions of at least five squares. Recently Xarles [25] has proved that six squares in arithmetic progression over quadratic number fields do not exist. The case of length five over quadratic fields has been treated by the first author and Xarles [12].

In this paper we consider the following natural problem:

2000 *Mathematics Subject Classification:* Primary: 14G35, 14H45; Secondary: 11F11, 11G10.
Key words and phrases: arithmetic progressions of four squares, θ-congruent numbers, Euler's concordant forms, quadratic fields.

Let d be an squarefree integer. Do there exist four squares in arithmetic progression over $\mathbb{Q}(\sqrt{d}\,)$? In the affirmative case, give an algorithm to construct explicit examples.

For special values of d the following table indicates for which quadratic fields $\mathbb{Q}(\sqrt{d}\,)$ there exist or do not exist non-constant arithmetic progressions of four squares. Here '?' indicates that in this case we do not know whether there exists a non-constant four term arithmetic progression of squares or not.

$p \geq 5$ prime	Is there a non-constant arithmetic progression of four squares over $\mathbb{Q}(\sqrt{d}\,)$?							
p mod 24	$d=p$	$d=2p$	$d=3p$	$d=6p$	$d=-p$	$d=-2p$	$d=-3p$	$d=-6p$
1	?	?	?	?	?	?	?	?
5	no	?	no	?	?	?	?	no
7	no	no	?	?	no	?	?	no
11	?	?	no	?	no	?	?	?
13	?	no	?	?	no	no	?	no
17	?	?	no	?	?	?	no	no
19	no	?	no	?	?	no	?	?
23	yes	yes	?	yes	yes	yes	yes	?

Table 1

The proof of the correctness of the table will be given in Section 5.

We shall show that four squares in arithmetic progression lead to points on an elliptic curve. This approach is not new; it seems to be a folklore result, however, we shall provide our own parametrization of arithmetic progressions of four squares over a number field k by k-rational points on the modular curve $X_0(24)$. More precisely, there exists a non-constant arithmetic progression of four squares over a number field k if and only if the Mordell–Weil group of the elliptic curve $X_0(24)$ over k contains more than eight points; in this case, there exist infinitely many arithmetic progressions of four squares over k if and only if this group has positive rank. For the specific case of a quadratic number field $\mathbb{Q}(\sqrt{d}\,)$ this characterization reduces our problem to the problem of determining the rank of the quadratic d-twists of the underlying elliptic curve.

The above characterization allows us to link our problem with two other problems, both being generalizations of the famous congruent number problem. These problems are related to θ-congruent numbers and Euler's concordant forms.

This paper is organized as follows: Section 2 is devoted to construct a parametrization of four term arithmetic progressions of squares over a number field k by k-rational points of the elliptic curve $X_0(24)$. Here we derive some particular results when k is a quadratic field. In Section 3 we introduce the notion of θ-congruent numbers and state some well-known results for the case when θ is either equal to $\pi/3$ or $2\pi/3$, which are the relevant cases with respect to the main problem of this paper. Section 4 deals with Euler's concordant forms. In Section 5

we apply results from the previous sections in order to obtain a partial answer to our problem. Here we also give examples of arithmetic progressions of four squares over $\mathbb{Q}(\sqrt{d})$ for all cases $|d| \leq 40$ for which such arithmetic progressions do exist. Moreover, we give another construction using pythagorean triples and Thue equations. The last section contains some average results related to our main problem.

2. Four squares in arithmetic progression

Four squares a^2, b^2, c^2 and d^2 over a field k are in arithmetic progression if and only if $b^2 - a^2 = c^2 - b^2$ and $c^2 - b^2 = d^2 - c^2$. This is equivalent to $[a, b, c, d] \in \mathbb{P}^3(k)$ being in the intersection of the two quadric surfaces $a^2+c^2 = 2b^2$ and $b^2 + d^2 = 2c^2$, resp. lying on the curve

$$C : \begin{cases} a^2 + c^2 = 2b^2, \\ b^2 + d^2 = 2c^2. \end{cases} \tag{1}$$

Therefore, k-rational points of C parametrize arithmetic progressions of four squares over k. Note that the eight points $[\pm 1, \pm 1, \pm 1, \pm 1]$ belong to C, however, these points correspond to constant arithmetic progressions. The next step is to compute an explicit equation for C. 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. For this purpose we are going to compute a Weierstrass equation for C. The system of equations (1) is equivalent to $a^2 + 2d^2 = 3c^2$, $b^2 = 2c^2 - d^2$. A parametrization (up to sign) of the first conic is given by

$$(a, d, c) = (2t^2 - 4t - 1, 2t^2 + 2t - 1, 2t^2 + 1), \quad t \in k,$$

where the inverse is given by $t = \frac{d-c}{a-c}$ if $a \neq c$ and $t = -\frac{1}{2}$ if $a = c$. Therefore, if we substitute the values of a, d and c in the second equation, we obtain the quartic equation

$$\mathcal{Q} : b^2 = 4t^4 - 8t^3 + 8t^2 + 4t + 1. \tag{2}$$

Our next aim is to find a Weierstrass model for $\mathcal{Q}$. Note that there is only one point at infinity, namely $[0 : 1 : 0]$. This point is a node. We denote by ∞_1 and ∞_2 the two branches at infinity at the desingularization of $\mathcal{Q}$. A Weierstrass model for $\mathcal{Q}$ is $E : y^2 = x(x + 3)(x - 1)$, where the isomorphism $\phi : \mathcal{Q} \to E$ is defined by

$$\phi(P) = \left(\frac{1 + b + 2t}{2t^2}, \frac{1 + b + 3t + bt + 4t^2 - 2t^3}{2t^3} \right) \quad \text{if} \quad P = (t, b) \neq (0, \pm 1),$$

and $\phi(0,-1)=(-1,2)$, $\phi(0,1)=[0:1:0]$, $\phi(\infty_1)=(1,0)$, $\phi(\infty_2)=(-1,-2)$. The inverse is defined by

$$\phi^{-1}(P)=\left(\frac{x+y-1}{x^2-1},\frac{x^3+5x^2+2xy-2y-x+3}{(x^2-1)(x+1)}\right) \quad \text{if} \quad P=(x,y),\ x\neq\pm 1.$$

Therefore, by the above construction we have proved

Theorem 1. *Let k be a field of $\mathrm{char}(k)\neq 2,3$, then arithmetic progressions of four squares in k are parametrized by k-rational points of the elliptic curve*

$$E: y^2=x(x+3)(x-1).$$

This parametrization is as follows:

- *Let $[a,b,c,d]\in\mathbb{P}^3(k)$ such that a^2,b^2,c^2,d^2 form an arithmetic progression. If $a\neq c$ and $d\neq c$, let $t=\frac{d-c}{a-c}$ and define*

$$P=\left(\frac{1+b+2t}{2t^2},\frac{1+b+3t+bt+4t^2-2t^3}{2t^3}\right),$$

and

$$P=\begin{cases}[0:1:0] & \text{if} \quad [a,b,c,d]=[-1,1,1,1],\\ (-1,2) & \text{if} \quad [a,b,c,d]=[-1,-1,1,1],\\ (3,-6) & \text{if} \quad [a,b,c,d]=[1,1,1,1],\\ (-3,0) & \text{if} \quad [a,b,c,d]=[1,-1,1,1],\\ (1,0) & \text{if} \quad [a,b,c,d]=[-1,1,-1,1],\\ (-1,-2) & \text{if} \quad [a,b,c,d]=[-1,-1,-1,1].\end{cases}$$

Then $P\in E(k)$.

- *Let $P\in E(k)$. If $P=(x,y)$, $x\neq\pm 1$, let $t=\frac{x+y-1}{x^2-1}$ and define*

$$[a,b,c,d]=\left[2t^2-4t-1,\frac{x^3+5x^2+2xy-2y-x+3}{(x^2-1)(x+1)},2t^2+1,2t^2+2t+1\right],$$

and

$$[a,b,c,d]=\begin{cases}[-1,-1,1,1] & \text{if} \quad P=(-1,2),\\ [-1,-1,-1,1] & \text{if} \quad P=(-1,-2),\\ [-1,1,-1,1] & \text{if} \quad P=(1,0),\\ [-1,1,1,1] & \text{if} \quad P=[0:1:0].\end{cases}$$

Then a^2, b^2, c^2, d^2 form an arithmetic progression in k.

It is natural to ask for which number fields k there exist arithmetic progressions of four squares over k. In order to investigate this problem we shall make use of the theory of elliptic curves.

Proposition 1. *Let k be a number field. Then there exists a non-constant arithmetic progression of four squares over k if and only if $\#E(k) > 8$. Furthermore, there exist infinitely many such progressions if and only if* $\operatorname{rank} E(k) \neq 0$.

Proof. Firstly, note that the points $[\pm 1, \pm 1, \pm 1, \pm 1]$ in $\mathbb{P}^3(k)$ give constant arithmetic progressions. Therefore, using the parametrization ϕ, it follows that the points $\phi([\pm 1, \pm 1, \pm 1, \pm 1])$ belong to $E(k)$, and this set has cardinality 8. This concludes the proof. □

As a corollary we obtain

Corollary 1. *There is no non-constant arithmetic progression of four rational squares.*

This statement is due to Fermat, however, the first proof is attributed to Euler who applied Fermat's method of infinite descent. For the sake of completeness and since some of the data that appear will be useful later, we give the short

Proof. Using `SAGE` [22] or `MAGMA` [4], one can check that E is the curve `24A1` in Cremona's tables [5], resp. `24B` in the Antwerp tables [1]. In other words, E is the modular curve $X_0(24)$. Checking these tables or using one of the above mentioned computer algebra systems, one can prove $E(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$. There are no $\mathbb{Q}$-rational points on E apart from those eight points $[\pm 1, \pm 1, \pm 1, \pm 1]$ which correspond to constant arithmetic progressions. □

Next we shall consider the case of quadratic number fields. Here the question translates to study the Mordell-Weil group $E(\mathbb{Q}(\sqrt{d}\,))$. However, instead of treating the elliptic curve E over $\mathbb{Q}(\sqrt{d}\,)$ directly, we are going to study the quadratic d-twist of the elliptic curve E over $\mathbb{Q}$, i.e., the elliptic curve

$$E^d : dy^2 = x(x+3)(x-1).$$

It should be noted that E and E^d are $\mathbb{Q}(\sqrt{d}\,)$-isomorphic.

Corollary 2. *Let d be a squarefree integer. Then there is a non-constant arithmetic progression of four squares over $\mathbb{Q}(\sqrt{d}\,)$ if and only if* $\operatorname{rank} E^d \neq 0$*; in this case, there exist infinitely many such progressions.*

PROOF. We are going to compute the structure of $E(\mathbb{Q}(\sqrt{d}\,))$. Since the 2-torsion subgroup of E is defined over $\mathbb{Q}$, by applying KWON's results [18] we see that $E(\mathbb{Q}(\sqrt{d}\,))_{\rm tors}$ and $E(\mathbb{Q})_{\rm tors}$ are equal. Thus Proposition 1 shows that if there exists a non-constant arithmetic progression of four squares over $\mathbb{Q}(\sqrt{d}\,)$, then there exist infinitely many or, equivalently, rank $E(\mathbb{Q}(\sqrt{d}\,)) \neq 0$. Now, since

$$\operatorname{rank} E(\mathbb{Q}(\sqrt{d}\,)) = \operatorname{rank} E(\mathbb{Q}) + \operatorname{rank} E^d(\mathbb{Q}), \tag{3}$$

the statement follows from $\operatorname{rank} E(\mathbb{Q}) = 0$. □

Therefore, the problem to decide for which quadratic fields $\mathbb{Q}(\sqrt{d}\,)$ there exist non-constant arithmetic progressions of four squares is reduced to the question whether the rank of $E^d(\mathbb{Q})$ is positive or not. In Section 5 we give a partial solution to this problem and for some quadratic number fields we also give explicit four term arithmetic progressions of squares.

For number fields of higher degree we have the following result:

Theorem 2. *There are infinitely many cyclic cubic number fields in each of which there exist infinitely many non-constant arithmetic progressions of four squares.*

PROOF. Applying [8, Theorem 6.1] to the elliptic curve $E = X_0(24)$, we find $\#E(\mathbb{Q}) = 8 > 6$. Hence, for infinitely many cyclic cubic extensions $K/\mathbb{Q}$ we have $\operatorname{rank} E(K) > \operatorname{rank} E(\mathbb{Q}) = 0$. □

3. θ-congruent numbers

A positive integer n is called a congruent number if there exists a right triangle with rational sides and area equal to n. The problem to decide whether a given integer is a congruent number has been studied since Diophantus. In 1983, TUNNELL [23] found a deterministic criterion for this problem; if the Birch and Swinnerton–Dyer conjecture is true, then his criterion also can be used to determine congruent numbers. The notion of congruent numbers was extended by FUJIWARA [9] to rational θ-triangles, that are triangles with rational sides where one angle is equal to θ. Note that for such a triangle, $\cos\theta = s/r$ for some coprime integers r, s with $r > 0$. It follows that $\sin\theta = \alpha_\theta/r$, where $\alpha_\theta := \sqrt{r^2 - s^2}$ is uniquely determined by θ. Then θ-congruent numbers are defined as follows:

Definition 1. Let be $\theta \in [0, \pi)$. A positive integer n is a θ-congruent number if there exists a rational θ-triangle whose area is equal to $n\alpha_\theta$.

Therefore, $\pi/2$-congruent numbers coincide with the ordinary congruent numbers (in which case $r = 1$ and $s = 0$). Generalizing the case of ordinary congruent numbers, there is a characterization of θ-congruent numbers in terms of rational points on elliptic curves.

Theorem 3 ([9], [10]). *For $\theta \in [0, \pi)$ and $n \in \mathbb{N}$, define the elliptic curve*

$$E_{n,\theta} : y^2 = x(x + (r + s)n)(x - (r - s)n).$$

Then, n is a θ-congruent number if and only if there exists a rational point on $E_{n,\theta}$ of order greater than 2. Moreover, if $n \neq 1, 2, 3, 6$, then n is a θ-congruent number if and only if $\operatorname{rank} E_{n,\theta}(\mathbb{Q}) > 0$.

Remark. Note that the elliptic curve $E_{n,\theta}$ is the n-twist of $E_{1,\theta}$. Therefore, whenever $n \neq 1, 2, 3, 6$, to prove that n is a θ-congruent number is equivalent to show that the rank of the n-twist of the elliptic curve $E_{1,\theta}$ is non-zero. Another interesting remark is that $E_{n,\pi-\theta}$ is the $(-n)$-twist of $E_{1,\theta}$.

Several papers [9], [10], [13], [15], [16], [26], [27] have been studying the θ-congruent number problem for $\theta \neq \pi/2$. For our purposes the cases $\theta = \pi/3$ and $\theta = 2\pi/3$ are of special interest (see Section 5). In these cases, the curve $E_{1,\pi/3}$ is the curve `24A1` and $E_{1,2\pi/3}$ is the curve `48A1` in Cremona's tables, respectively.

The following table resumes all known results on $\pi/3$-congruent and $2\pi/3$-congruent numbers (see [9], [15], [16], [26], [27]). Here '?' indicates that in this case we do not know whether n is θ-congruent or not.

$p \geq 5$ prime	Is n a $\pi/3$-congruent number?				Is n a $2\pi/3$-congruent number?			
$p \bmod 24$	$n = p$	$n = 2p$	$n = 3p$	$n = 6p$	$n = p$	$n = 2p$	$n = 3p$	$n = 6p$
1	?	?	?	?	?	?	?	?
5	no	?	no	?	?	?	?	no
7	no	no	?	?	no	?	?	no
11	?	?	no	?	no	?	?	?
13	?	no	?	?	no	no	?	no
17	?	?	no	?	?	?	no	no
19	no	?	no	?	?	no	?	?
23	yes	yes	?	yes	yes	yes	yes	?

Table 2

Let n be a squarefree positive integer from one of the residue classes $1, 7$ or $13 \bmod 24$. Yoshida [26], [27] proved along the lines of Tunnell's approach to the congruent number problem that n is not a $2\pi/3$-congruent number if the number of representations of n by the ternary quadratic forms

$$X^2 + 3Y^2 + 144Z^2 \qquad \text{and} \qquad 3X^2 + 9Y^2 + 16Z^2$$

with integral X, Y, Z are not equal; if the conjecture of Birch and Swinnerton–Dyer is true, then also the converse implication holds, i.e., n is $2\pi/3$-congruent if the number of representations are identical. In particular, it follows from the theory of quadratic forms that all primes $p \equiv 7$ or $13 \bmod 24$ are not $2\pi/3$-congruent numbers. Moreover, if $n \neq 1$ is squarefree with $n \equiv 1, 7$ or $19 \bmod 24$, then he showed that n is not a $\pi/3$-congruent number if the number of integer representations of n by the ternary quadratic forms

$$X^2 + 12Y^2 + 15Z^2 + 12YZ \qquad \text{and} \qquad 3X^2 + 4Y^2 + 13Z^2 + 4YZ$$

are not equal; if the conjecture of Birch and Swinnerton–Dyer is true, then also the converse implication is true. Here it follows that no prime $p \equiv 7 \bmod 24$ is a $\pi/3$-congruent number. For other residue classes Yoshida obtained analogous statements with, of course, different quadratic forms, which explain the 'no's in the above table. Note that all affirmative 'yes' rely on primes $p \equiv 23 \bmod 24$ by a theorem of Kan [16]. We collect these results on primes in the following theorem; for the other cases we refer to the mentioned papers.

Theorem 4 ([16], [26], [27])**.** *There is no prime number $p \equiv 7, 11, 13 \bmod 24$ which is a $2\pi/3$-congruent number, and there is no prime number $p \equiv 5, 7, 19 \bmod 24$ which is a $\pi/3$-congruent number where $p > 5$. On the contrary, any prime $p \equiv 23 \bmod 24$ is a θ-congruent number for both $\theta = \pi/3$ and $\theta = 2\pi/3$.*

A classical conjecture, supported by numerical evidence (based on computations from the 1970s), states that all squarefree positive integers congruent 5, 6 or 7 modulo 8 are congruent numbers. In fact, this conjecture is a direct consequence of the Birch and Swinnerton–Dyer conjecture. Similar to this conjecture the following one covers the cases of $\pi/3$- and $2\pi/3$-congruent numbers, respectively.

Conjecture 1. *Let n be a squarefree positive integer.*

- *If $n \equiv 11, 13, 17, 23 \bmod 24$, then n is a $\pi/3$-congruent number.*
- *If $n \equiv 5, 17, 19, 23 \bmod 24$, then n is a $2\pi/3$-congruent number.*

4. Euler's concordant forms

Another equivalent formulation of the congruent number problem is the following: a positive integer n is a congruent number if and only if the system of

diophantine equations

$$\begin{cases} x^2 + ny^2 = t^2 \\ x^2 - ny^2 = z^2 \end{cases}$$

has a solution $x, y, z, t \in \mathbb{Z}$ with $xy \neq 0$. In 1780, Euler [6] gave another generalization of the congruent number problem. He was interested to classify those pairs of distinct non-zero integers M and N for which there exist $x, y, z, t \in \mathbb{Z}$ with $xy \neq 0$ such that

$$\begin{cases} x^2 + My^2 = t^2 \\ x^2 + Ny^2 = z^2 \end{cases}$$

This is known as Euler's concordant forms problem. If the above diophantine system has a solution, then the pair (M, N) is said to be concordant, otherwise discordant. In the particular case when $M = -N$ this yields the congruent number problem. As for the congruent number problem and its generalization to θ-congruent numbers, there is a characterization due to Ono [20] for Euler's concordant forms problem in terms of rational points of an elliptic curve.

Theorem 5. [20] *For $M, N \in \mathbb{Z}$ such that $NM(M - N) \neq 0$, define the elliptic curve*

$$E_{M,N} : y^2 = x(x + M)(x + N).$$

Then, the pair (M, N) is concordant if and only if there exists a rational point on $E_{M,N}$ of order $\neq 1, 2$ or 4. In particular, if $\operatorname{rank} E_{M,N}(\mathbb{Q})$ *is positive, then (M, N) is concordant.*

Using Waldspurger's results and Shimura's correspondence *a la* Tunnell, Ono obtained several results on the ranks of twists of $E_{M,N}$. In particular, if the number of integer representations of an odd positive squarefree integer n by the ternary quadratic forms

$$X^2 + 2Y^2 + 12Z^2 \quad \text{and} \qquad 2X^2 + 3Y^2 + 4Z^2$$

is not equal, then $(M, N) = (6n, -18n)$ is discordant; if the conjecture of Birch and Swinnerton–Dyer is true, then also the converse implication is true. Moreover, for r being an odd integer with $1 \leq r \leq 24$, he showed that there are infinitely many positive squarefree integers $n \equiv r \bmod 24$ such that

- $(M, N) = (6n, -18n)$ is discordant.
- $(M, N) = (9n, -3n)$ is discordant, where $r \neq 7, 15, 23$.

5. Four squares in arithmetic progressions over quadratic fields

The existence of a non-constant four term arithmetic progression of squares over a quadratic field is determined by the rank of twist of the elliptic curve $E = X_0(24)$. For a real-quadratic field $\mathbb{Q}(\sqrt{d}\,)$ the elliptic curve E^d is equal to $E_{d,\pi/3}$, whereas for an imaginary-quadratic field $\mathbb{Q}(\sqrt{-d}\,)$ it is $E_{d,2\pi/3}$.

Thus, we may use the information of Table 2 to deduce information about the rank of $E^d(\mathbb{Q})$ from $E_{d,\pi/3}$ and $E_{d,2\pi/3}$, respectively, corresponding to d being positive or negative. This proves the information provided by Table 1 from the introduction. Moreover assuming Conjecture 1 we have that there exists a non-constant arithmetic progression of four squares over $\mathbb{Q}(\sqrt{d}\,)$ if $d \equiv 11, 13, 17, 23 \bmod 24$ in the real case and $d \equiv 1, 5, 7, 19 \bmod 24$ in the imaginary case.

Further, note that for $(M, N) = (-1, 3)$ or $(3, -1)$ we have $E_{d,\pi/3} = E_{M,N}$; moreover, if $(M, N) = (1, -3)$ or $(-3, 1)$, then $E_{d,2\pi/3} = E_{M,N}$. In these cases we can use Ono's results [20] on the rank of $E_{M,N}(\mathbb{Q})$.

5.1. Explicit examples. Using `MAGMA`, we may compute the rank of $E^d(\mathbb{Q})$; if this rank is positive, using the parametrization from Theorem 1, we can also compute an explicit arithmetic progression of four squares. The following two tables list explicit examples of such progressions according to $\mathbb{Q}(\sqrt{d}\,)$ being an imaginary-quadratic or a real-quadratic number field for the range $|d| \le 40$. Each of the tables consists of three colums; the first column indicates the value of d, the second and third one give an example for $a, r \in \mathbb{Q}(\sqrt{d}\,)$ such that $a^2, a^2 + r, a^2 + 2r, a^2 + 3r$ forms an arithmetic progressions of squares over $\mathbb{Q}(\sqrt{d}\,)$, where $\alpha := \sqrt{d}$.

d	a	r
-5	$(-4\alpha - 73)/2$	$42\alpha - 840$
-10	$(-60\alpha - 629)/2$	$-14322\alpha - 55440$
-14	$-6\alpha - 361$	$8580\alpha - 65520$
-15	$(\alpha - 19)/4$	$\alpha - 15$
-17	$3339440\alpha - 57973177$	$219447603254880\alpha - 2180390987174400$
-19	$(-26589360\alpha + 21015523)/2$	$22024049983320\alpha + 2196495218332800$
-21	$-160\alpha - 2393$	$-590920\alpha - 3141600$
-22	$-1224720\alpha - 2179673$	$-3235062111120\alpha + 19986461510400$
-23	$(2625\alpha + 11951)/4$	$-1231230\alpha + 6592950$
-29	$(22143940\alpha - 361130617)/2$	$3478556113902870\alpha - 13110939890248200$
-33	$-612000\alpha + 1945781$	$673901512480\alpha + 8195655283200$
-34	$319440\alpha + 650807$	$-95395404720\alpha + 2288266041600$
-39	$(36\alpha - 683)/2$	$10450\alpha - 51480$

d	a	r
6	$(2\alpha+1)/2$	$25\alpha+60$
10	$(10\alpha-19)/2$	$33\alpha-60$
11	$(-1320\alpha+2843)/2$	$-7242060\alpha+23839200$
13	$1440\alpha+5183$	$1323960\alpha+4773600$
17	$-15\alpha-1511$	$-555360\alpha+1591200$
21	$-36\alpha+163$	$2200\alpha-10080$
22	$(-750\alpha+3529)/2$	$453705\alpha-2009700$
23	$19476668640\alpha+90283636367$	$17257835760495310780 80\alpha+$ 8274631385821773772800
30	$(18\alpha+19)/2$	$-413\alpha+1260$
34	$6860\alpha-12239$	$-12575640\alpha+43982400$
35	$-84\alpha+487$	$-28968\alpha+171360$
37	$38306628360\alpha-276487794001$	$1002167851379543172324 0\alpha-$ $2411497061202847297680 0$
39	$720\alpha+3869$	$7990640\alpha+49795200$

5.2. Pythagorean triples. Next we use Pythagorean triples to construct arithmetic progressions of four squares over quadratic number fields. In the following cases the arithmetic progression consists of four integers, all of them being a square over a specific quadratic number field.

It is well-known that for arbitrary $a, b \in \mathbb{Z}$ the triple $(a^2-b^2, 2ab, a^2+b^2)$ defines a Pythagorean triple. Then $(a^2+b^2)^2-4n, (a^2+b^2)^2, (a^2+b^2)^2+4n$ forms an arithmetic progression of three squares where $n=ab(a^2-b^2)$. If we add a new square term, $\alpha^2=(a^2+b^2)^2+8ab(a^2-b^2)$ say, we obtain an arithmetic progression of four squares over $\mathbb{Q}(\sqrt{(a^2+b^2)^2+8ab(a^2-b^2)}\,)$. In order to construct a quadratic number field $\mathbb{Q}(\sqrt{d}\,)$, where d is a squarefree integer, we define the Thue equation

$$F(x,y)=(x^2+y^2)^2+8xy(x^2-y^2)=d.$$

Of course, here we are interested in the set of integer solutions. Using `MAGMA`, we have observed that for $|d|<100$ there exist integer solutions in the cases $d=-71,-47,-23,73$, all of them being congruent to 1 mod 24. By the above construction this yields the following arithmetic progressions:

d	Four square in arithmetic progression over $\mathbb{Q}(\sqrt{d}\,)$
-71	$(\sqrt{-71}\,)^2, 7^2, 13^2, 17^2$
-47	$(\sqrt{-47}\,)^2, 17^2, 25^2, 31^2$
-23	$(\sqrt{-23}\,)^2, 1, 5^2, 7^2$
73	$1, 5^2, 7^2, (\sqrt{73}\,)^2$

It is straightforward to compute that $(a^2+b^2)^2+8ab(a^2-b^2) \equiv 1 \bmod 24$ for $a, b \in \mathbb{Z}$ with coprime a, b and $a \not\equiv b \bmod 2$. Therefore, our construction is restricted to the case of number fields $\mathbb{Q}(\sqrt{d}\,)$ with $d \equiv 1 \bmod 24$. Moreover, all arithmetic progressions discovered by this method satisfy that the difference of any two successive members is divisible by 24.

6. Average results

We conclude by discussing some average results for the central values of L-functions associated with elliptic curves. Let E be an elliptic curve over $\mathbb{Q}$ and denote by $L(E,s)$ its elliptic curve L-function. Roughly speaking, the yet unproved Birch and Swinnerton–Dyer conjecture states that the order of vanishing of $L(E,s)$ at $s=1$ is equal to the rank of E. Kolyvagin [17] has shown that if E is a modular elliptic curve with $L(E,1) \neq 0$, then the rank of E is equal to zero. By the proof of Wiles *et al.* [24], [2] of the Shimura–Taniyama conjecture any elliptic curve over $\mathbb{Q}$ is modular, however, the corresponding statement for quadratic number fields is not known to be true. Note that

$$L(E(\mathbb{Q}(\sqrt{d}\,)),s) = L(E,s)L(E^d,s),$$

where E^d denotes the quadratic twist of E by d; here it suffices to consider squarefree integers d. This formula directly corresponds to (3). Hence in our case, in order to have rank zero for $E(\mathbb{Q}(\sqrt{d}\,))$ we need the non-vanishing of $L(E^d,1)$ since $L(E,1) = 0.53\ldots$; this computation has been made using `SAGE`.

We may ask for the statistical behaviour as d varies. Goldfeld [11] has conjectured that a positive proportion of $0 < |d| \leq X$ have the property that $L(E^d,1)$ is non-vanishing. This has been established only in exceptional cases. For instance, Heath-Brown [14] confirmed this conjecture for the congruent number elliptic curve. Moreover, Ono and Skinner [21, Corollary 2] have proved that if E is an elliptic curve over $\mathbb{Q}$ with conductor ≤ 100, then either E^{-p} or E^p has rank zero for a positive proportion of primes p. In the special case of our elliptic curve we obtain:

Corollary 3. *For a positive proportion of primes p, there are either no non-constant arithmetic progressions of four squares in $\mathbb{Q}(\sqrt{-p}\,)$ or $\mathbb{Q}(\sqrt{p}\,)$.*

If the Birch and Swinnerton–Dyer conjecture is true, then the vanishing of $L(E^d,1)$ would imply that the rank of $E(\mathbb{Q}(\sqrt{d}\,)$ is positive, and so from (3) and Proposition 1 it would follow that there exist infinitely many non-constant arithmetic progressions of four squares over $\mathbb{Q}(\sqrt{d}\,)$. M. R. Murty and V. K. Murty

[19] have shown that for $L(E,1) \neq 0$ there are infinitely many fundamental discriminants $d < 0$ such that $L(E^d, s)$ has a simple zero at $s = 1$; this result was independently obtained by Bump, Friedberg and Hoffstein [3]. Hence, in our special case we may deduce that there exist infinitely many imaginary quadratic fields $\mathbb{Q}(\sqrt{d}\,)$ each of which containing infinitely many non-constant arithmetic progressions of four squares subject to the truth of the Birch and Swinnerton–Dyer conjecture.

Acknowledgements. Research of the first author was supported in part by grant MTM 2009-07291 (Ministerio de Educación y Ciencia, Spain) and CCG08-UAM/ESP–3906 (Universidad Autónoma de Madrid – Comunidad de Madrid, Spain). Research of the second author was supported in part by grant MTM 2006-01859 (Ministerio de Educación y Ciencia, Spain).

References

[1] B. J. Birch and W. Kuyk (eds.), Modular Functions One Variable IV, Lecture Notes Mathematics, 476, *Springer-Verlag*, 1975.

[2] C. Breuil, B. Conrad, F. Diamond and R. Taylor, On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises, *J. Amer. Math. Soc.* **14** (2001), 843–939.

[3] D. Bump, S. Friedberg and J. Hoffstein, Nonvanishing theorems for L-functions of modular forms and their derivatives, *Invent. Math.* **102** (1990), 543–618.

[4] J. J. Cannon and W. Bosma (Eds.), Handbook of Magma Functions, Edition 2.14, 2007.

[5] J. E. Cremona, Algorithms for Modular Elliptic Curves, *Cambridge University Press*, 1992.

[6] L. Euler, De binis formulis speciei $xx+myy$ et $xx+nyy$ inter se concordibus et discordibus, Memoires de l'academie des sciences de St.-Petersbourg 8, 1822,, 3–16.

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

[8] J. Fearnley, H. Kisilevsky and M. Kuwata, Vanishing and non-vanishing dirichlet twists of L-functions of elliptic curves, `arXiv:0711.1771`.

[9] M. Fujiwara, θ-congruent numbers, Number Theory, (K. Győry et al. Walter de Gruyter, eds.), *Berlin*, 1998, 235–241.

[10] M. Fujiwara, Some properties of θ-congruent numbers, *Natur. Sci. Rep. Ochanomizu Univ.* **52**, no. 2 (2002), 1–8.

[11] D. Goldfeld, Conjectures on elliptic curves over quadratic fields, Number Theory, Carbondale, Vol. 751, Lecture Notes in Math., *Springer*, 1979, 108–118.

[12] E. González-Jiménez and X. Xarles, Five squares in arithmetic progression over quadratic fields, arXiv: 0909.1663.

[13] T. Goto, Calculation of Selmer groups of elliptic curves with rational 2-torsions and θ-congruent number problem, *Comment. Math. Univ. St. Paul.* **50**, no. 2 (2001), 147–172.

[14] D. R. Heath-Brown, The size of the Selmer groups for the congruent number problem, II, *Invent. Math.* **118** (1994), 331–370.

[15] T. Hibino and M. Kan, θ-congruent numbers and Heegner points, *Arch. Math. (Basel)* **77**, no. 4 (2001), 303–308.

[16] M. Kan, θ-congruent numbers and elliptic curves, *Acta Arith.* **94**, no. 2 (2000), 153–160.

[17] V. Kolyvagin, Finiteness of $E(\mathbb{Q})$ and Ш$(E,\mathbb{Q})$ for a subclass of Weil curves, *Izv. Akad. Nauk. USSR, Ser. Mat.* **52** (1988), 522–540 (in *Russian*).

[18] S. Kwon, Torsion subgroups of elliptic curves over quadratic extensions, *J. Number Theory* **62** (1997), 144–162.

[19] M. R. Murty and V. K. Murty, Mean values of derivatives of modular L-series, *Ann. of Math.* **133** (1991), 447–475.

[20] K. Ono, Euler's concordant forms, *Acta Arith.* **78** (1996), 101–123.

[21] K. Ono and C. Skinner, Non-vanishing of modular L-functions, *Invent. Math.* **134** (1998), 651–660.

[22] W. Stein *et al.*, Sage: Open Source Mathematical Software (Version 3.0), The Sage Group, 2008, `http://www.sagemath.org`.

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

[24] A. Wiles, Modular elliptic curves and Fermat's last theorem, *Ann. Math.* **141** (1995), 443–551.

[25] X. Xarles, Squares in arithmetic progression over number fields, arXiv: 0909.1642.

[26] S. Yoshida, Some variants of the congruent number problem I, *Kyushu J. Math.* **55** (2001), 387–404.

[27] S. Yoshida, Some variants of the congruent number problem II, *Kyushu J. Math.* **56** (2002), 147–165.

ENRIQUE GONZÁLEZ-JIMÉNEZ
UNIVERSIDAD AUTÓNOMA DE MADRID
DEPARTAMENTO DE MATEMÁTICAS
AND INSTITUTO DE CIENCIAS MATEMÁTICAS
(CSIC-UAM-UC3M-UCM)
MADRID
SPAIN

E-mail: enrique.gonzalez.jimenez@uam.es

JÖRN STEUDING
WÜRZBURG UNIVERSITY
INSTITUT FÜR MATHEMATIK
97074 WÜRZBURG
GERMANY

E-mail: steuding@mathematik.uni-wuerzburg.de

(Received May 20, 2009; revised February 25, 2010)