Arch. Math. 95 (2010), 233–241

0003-889X/10/030233-9
published online August 31, 2010
DOI 10.1007/s00013-010-0166-5

Archiv der Mathematik

Three cubes in arithmetic progression over quadratic fields

Enrique González-Jiménez

Abstract. We study the problem of the existence of arithmetic progressions of three cubes over quadratic number fields $\mathbb{Q}(\sqrt{D})$, where D is a squarefree integer. For this purpose, we give a characterization in terms of $\mathbb{Q}(\sqrt{D})$-rational points on the elliptic curve $E : y^2 = x^3 - 27$. We compute the torsion subgroup of the Mordell–Weil group of this elliptic curve over $\mathbb{Q}(\sqrt{D})$ and we give an explicit answer, in terms of D, to the finiteness of the free part of $E(\mathbb{Q}(\sqrt{D}))$ for some cases. We translate this task to computing whether the rank of the quadratic D-twist of the modular curve $X_0(36)$ is zero or not.

Mathematics Subject Classification (2010). 11B25, 14H52.

Keywords. Arithmetic progressions, Cubes, Quadratic fields, Elliptic curves, Twists.

1. Introduction. Nowadays, the study of arithmetic progressions consisting of perfect nth powers is of considerable interest in Number Theory. Thanks to the development of new techniques to solve Diophantine equations, several problems related to arithmetic progressions are being solved. For example, Darmon and Merel [5] proved that there are no non-trivial arithmetic progressions of three nth powers. The present article studies the oldest and simplest problem in this direction, that is, the case of three cubes in arithmetic progression.

According to Dickson's *History of the Theory of Numbers* [6, Vol. II, pp. 572–573], Legendre [12] established that there are no non-trivial arithmetic progressions of three cubes over $\mathbb{Q}$. We will study in this paper when there exists a non-trivial arithmetic progression of three cubes over a quadratic number field.

The author was partially supported by the grants CCG08-UAM/ESP-3906 and MTM 2009-07291.

Note that, for the number field case, important progress has been made in the last years. Xarles [17], for instance, has proved that for any positive integers n and d, the length of any arithmetic progression of nth powers over a number field of degree d is bounded by a constant depending only on n and d. In particular, for the case of squares over quadratic fields, Xarles [17] has proved that the length of any arithmetic progression of squares over any quadratic field is less than six. The case of length four and five has been treated in [8,9], respectively. Therefore the study of arithmetic progressions of squares over a quadratic field can be considered done.

A next task could be to study the case of arithmetic progressions of cubes over quadratic fields. As a first step in this project, the goal of this paper is to study when there exists a three-term arithmetic progression consisting of cubes over $\mathbb{Q}(\sqrt{D})$, where D is a squarefree integer. For this purpose, first we will parametrize the set of arithmetic progressions of three cubes by the rational points of the elliptic curve $E : y^2 = x^3 - 27$. Therefore, to find three cubes in arithmetic progression over $\mathbb{Q}(\sqrt{D})$ we should compute the Mordell–Weil group $E(\mathbb{Q}(\sqrt{D}))$. Finally we will reduce our problem to the determination of the rank of the quadratic twists of the modular curve $X_0(36)$. We will use the work of Barthel [1] and Frey [7] to obtain an answer to this question for some D.

2. Parametrization. Let x_0^3, x_1^3, x_2^3 be three cubes in a field k, and assume that they form an arithmetic progression. Therefore, they satisfy $x_1^3 - x_0^3 = x_2^3 - x_1^3$. That is, the point $[x_0, x_1, x_2] \in \mathbb{P}^2(k)$ belongs to the projective curve $C : X_0^3 - 2X_1^3 + X_2^3 = 0$. It is easy to check that if $\mathrm{char}(k) \neq 2, 3$ then C is an irreducible smooth projective curve of genus 1 with two trivial points: $[1, 1, 1], [-1, 0, 1] \in C(k)$. Note that this two points correspond to the trivial arithmetic progressions: the constant progression $1, 1, 1$ and $-1, 0, 1$.

Since the genus of C is 1 and C has at least one rational point, C is an elliptic curve defined over k. Let us compute a Weierstrass model for C. We have that $[-1, 0, 1]$ is an inflection point of C. Let move the point $[-1, 0, 1]$ to $[0, 1, 0]$ and its tangent line to the line $w = 0$. The tangent line at $[-1, 0, 1]$ is $X_0 + X_2 = 0$, then the linear change of variables that sends $[X_0, X_1, X_2]$ to $[u, v, w] = [X_0, X_1, X_0+X_2]$ gives us the equation $-2v^3+3u^2w-3uw^2+w^3 = 0$. Now assuming that $\mathrm{char}(k) \neq 2, 3$, we can make a change of variables to obtain an isomorphism to the elliptic curve $E : zy^2 = x^3 - 27z^3$. This isomorphism is as follows:

$$\varphi : C \longrightarrow E, \quad \varphi([x_0, x_1, x_2]) = [6x_1, 9(x_0 - x_2), x_0 + x_2]$$

and its inverse is given by:

$$\varphi^{-1} : E \longrightarrow C, \quad \varphi^{-1}([x, y, z]) = \left[\frac{9z + y}{18}, \frac{x}{6}, \frac{9z - y}{18}\right].$$

Therefore, we have proved the following proposition:

Proposition 1. *Let k be a field of $\mathrm{char}(k) \neq 2, 3$, then arithmetic progressions of three cubes in k are parametrized by k-rational points of the elliptic curve $E : zy^2 = x^3 - 27z^3$. This parametrization is as follows:*

- *Let $x_0, x_1, x_2 \in k$ such that x_0^3, x_1^3, x_2^3 form an arithmetic progression. Then $P = [6x_1, 9(x_0 - x_2), x_0 + x_2] \in E(k)$.*
- *Let $P = [x, y, z] \in E(k)$. Define $x_0 = 9z + y, x_1 = 3x, x_2 = 9z - y$. Then x_0^3, x_1^3, x_2^3 form an arithmetic progression.*

Corollary 2. *Let k be a field of $\mathrm{char}(k) \neq 2, 3$, then a necessary condition for the existence of a non-trivial arithmetic progressions of three cubes is the existence of a point $(x, y) \in E(k)$ such that $x \neq 3$. That is, $\mathbb{Z}/2\mathbb{Z} \subsetneq E(k)$.*

We will see that in general the condition $\mathbb{Z}/2\mathbb{Z} \subsetneq E(k)$ is not sufficient. As a corollary we obtain:

Corollary 3. *There are no non-trivial arithmetic progressions of three rational cubes.*

This statement is due to Legendre [12], as we mentioned above. For the sake of completeness, we will give a short proof using the above corollary.

Proof. With `Sage` [14] or `Magma` [3], one can check that E is the curve `36A3` in Cremona's tables [4], resp. `36C` in the Antwerp tables [2]. Checking these tables or using one of the above mentioned computer algebra systems, one can prove $E(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$. There are no $\mathbb{Q}$-rational affine points on E apart $(3, 0)$ which corresponds to the constant arithmetic progressions. □

Remark 1. Let k be a field. If $\mathrm{char}(k) = 2$ or 3 looking for arithmetic progressions over k is not interesting. If $\mathrm{char}(k) = 2$ and x_0^3, x_1^3, x_2^3 is an arithmetic progression, then its length is 2 instead of 3, since $x_2^3 = x_0^3$. Now, if $\mathrm{char}(k) = 3$ then $C : X_0^3 - 2X_1^3 + X_2^3 = 0$ is three copies of $X_0 + X_1 + X_2 = 0$, that is $C(k) \cong \mathbb{P}^1(k)$.

Our purpose in this paper is to obtain an answer to the following question: Are there non-constant arithmetic progressions of three cubes over a quadratic number field? Also, may the answer be affirmative, we would like to give an explicit algorithm to construct them. Our main tool for this will be the characterization given at Proposition 1.

Note that thanks to the above parametrization it is easy to check that for any $\alpha \in \mathbb{Q}$, in the algebraic extension of $\mathbb{Q}$ generated by the squarefree part of $\alpha^3 - 27$, there exists a non-constant arithmetic progression of three cubes over that field. Nevertheless, this construction is not useful for our purpose, since we do not have control of the discriminant of this quadratic field.

Therefore, for a squarefree integer D, our goal is to compute the Mordell–Weil group of the elliptic curve $E : y^2 = x^3 - 27$ over $\mathbb{Q}(\sqrt{D})$. The torsion subgroup will be computed in Section 3. In order to compute the rank, we will translate this problem into computing the rank of the quadratic D-twist of E over $\mathbb{Q}$. This will be done in Section 4.

3. Torsion subgroup. In this section we are going to give a complete characterization of the torsion subgroup of the elliptic curve $E : y^2 = x^3 - 27$ over a quadratic number field $\mathbb{Q}(\sqrt{D})$. We will denote by $E(\mathbb{Q}(\sqrt{D}))_{\mathrm{tors}}$ this subgroup. We can now prove the following result.

Proposition 4. *Let D be a squarefree integer. Then the torsion subgroup of the elliptic curve $E : y^2 = x^3 - 27$ over $\mathbb{Q}(\sqrt{D})$ is*

$$E(\mathbb{Q}(\sqrt{D}))_{\text{tors}} \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} & \text{if } D = -3, \\ \mathbb{Z}/2\mathbb{Z} & \text{if } D \neq -3. \end{cases}$$

Proof. Kamienny [10] proved that the only primes possibly dividing the order of the torsion subgroup of an elliptic curve over a quadratic field are $2, 3, 5, 7, 11$ and 13. Then it is enough to compute for which quadratic fields the elliptic curve $E : y^2 = x^3 - 27$ has a torsion point of order $n \in \{2, 3, 4, 5, 7, 11, 13\}$. Note that we need to check $n = 4$ since there is a point of order 2 defined over $\mathbb{Q}$.

To achieve this we look for the irreducible factors of degree one or two of the nth division polynomial of E in $\mathbb{Z}[x]$. The set of these factors is $\{x, x - 3, x^2 + 3x + 9, x^2 - 6x - 18\}$. Therefore the only possible values of D such that $E(\mathbb{Q}(\sqrt{D}))_{\text{tors}}$ increases with respect $E(\mathbb{Q})_{\text{tors}}$ are $D = 3$ and $D = -3$. A straightforward computation shows that $E(\mathbb{Q}(\sqrt{3}))_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z}$ and $E(\mathbb{Q}(\sqrt{-3}))_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$. □

4. Rank. The aim of this section is to compute the rank of the elliptic curve $E : y^2 = x^3 - 27$ over a quadratic field. We are going to translate this problem to an easier one: to compute the rank of a quadratic twist of an elliptic curve over $\mathbb{Q}$.

Proposition 5. *Let D be a squarefree integer, $E : y^2 = x^3 - 27$ and $F^D : y^2 = x^3 + D^3$. Then*

$$\operatorname{rank} E(\mathbb{Q}(\sqrt{D})) = \operatorname{rank} F^D(\mathbb{Q}).$$

Proof. Let denote by E^D the D-quadratic twist of E. That is, $E^D : y^2 = x^3 - 27D^3$. It is well known that for an arbitrary elliptic curve E_0 defined over $\mathbb{Q}$, we have

$$\operatorname{rank} E_0(\mathbb{Q}(\sqrt{D})) = \operatorname{rank} E_0(\mathbb{Q}) + \operatorname{rank} E_0^D(\mathbb{Q}). \tag{1}$$

Applying the above equality to E we have $\operatorname{rank} E(\mathbb{Q}(\sqrt{D})) = \operatorname{rank} E^D(\mathbb{Q})$, since $E(\mathbb{Q})$ is finite.

Now, we have that $F^1 : y^2 = x^3 + 1$ is $\mathbb{Q}$-isogenous to $E^1 = E$. This isogeny has the following equations

$$\psi : F^1 \longrightarrow E^1, \quad \psi(x, y) = \left(\frac{x^3 + 4}{x^2}, \frac{x^3 - 8}{x^3}\, y \right).$$

Therefore F^D is $\mathbb{Q}$-isogenous to E^D, thus $\operatorname{rank} F^D(\mathbb{Q}) = \operatorname{rank} E^D(\mathbb{Q})$. This finishes the proof. □

The study of the rank of the quadratic twists of an elliptic curve is an important area in the theory of elliptic curves. In particular, the quadratic twists of the elliptic curve F^1 have been deeply studied by Barthel [1] and Frey [7]. Their results will be applied in the context of arithmetic progressions of three cubes in the next section.

5. Arithmetic progressions of three cubes over quadratic fields.

Theorem 6. *Let D be a squarefree integer. Then there is a non-trivial arithmetic progression of three cubes over $\mathbb{Q}(\sqrt{D})$ if and only if the D-quadratic twist of $X_0(36)$ has positive rank.*

Proof. First we apply the characterization given at Proposition 1 for the case $k = \mathbb{Q}(\sqrt{D})$ obtaining that arithmetic progressions of three cubes over $\mathbb{Q}(\sqrt{D})$ are parametrized by $E(\mathbb{Q}(\sqrt{D}))$. Corollary 2 together with Proposition 4 tell us that the only possible D such that there exists a non-trivial arithmetic progression of three cubes over $\mathbb{Q}(\sqrt{D})$ coming from a torsion point of $E(\mathbb{Q}(\sqrt{D}))$ is $D = -3$. Let $[x_0, x_1, x_2] \in \varphi^{-1}E(\mathbb{Q}(\sqrt{-3}))_{\text{tors}}$, then its corresponding arithmetic progression x_0^3, x_1^3, x_2^3 is equivalent to the arithmetic progression $-1, 0, 1$ or $1, 1, 1$.

Now we are going to obtain non-torsion points on $E(\mathbb{Q}(\sqrt{D}))$ coming from non-torsion points on $E^D(\mathbb{Q})$. This will be done thanks to the following map

$$\phi : E^D \longrightarrow E, \quad \phi(x, y) = \Big(\frac{x}{D}, \frac{y}{D^2}\sqrt{D}\Big).$$

Let $(x, y) \in E^D(\mathbb{Q})$ then $\varphi^{-1} \circ \phi(x, y) = [9D^2 - y\sqrt{D}, 3xD, 9D^2 + y\sqrt{D}] = [x_0, x_1, x_2]$ and denote by $\mathcal{S}$ the arithmetic progression x_0^3, x_1^3, x_2^3.

First assume that $\mathcal{S}$ is equivalent to the arithmetic progression $-1, 0, 1$. Then $x = 0$ and $y^2 = -27D^3$, and since $y \in \mathbb{Q}$ we have $D = -3$ and $y = 27$, that corresponds to the point $(0, 3\sqrt{-3}) \in E(\mathbb{Q}(\sqrt{-3}))[3]$. Now assume that $\mathcal{S}$ is the constant arithmetic progression. Then we have $y = 0$ since $(9D^2 - y\sqrt{D})^3 = (9D^2 + y\sqrt{D})^3$. That is, $\mathcal{S}$ correspond to the point $(3, 0) \in E(\mathbb{Q})[2]$. Therefore we have proved that if $P \in E^D(\mathbb{Q})$ is a non-torsion point, then $\varphi^{-1} \circ \phi(x, y)$ gives a non-trivial arithmetic progression of three cubes over $\mathbb{Q}(\sqrt{D})$. To finish the proof just mind that a Weierstrass model for $X_0(36)$ is $y^2 = x^3 + 1$, therefore by Proposition 5 the proof is done. □

Corollary 7. *Let d be a squarefree positive integer coprime with 6 and*

$$A_d = \sum_{(m,n,k)\in S} (-1)^n \text{ where } S = \left\{ (m, n, k) \in \mathbb{Z}^3 \;\middle|\; \begin{array}{l} m^2 + n^2 + k^2 = d \\ m \equiv 1 \,(\mathrm{mod}\, 3) \\ n \equiv 0 \,(\mathrm{mod}\, 3) \\ m + n \equiv 1 \,(\mathrm{mod}\, 2) \end{array} \right\}.$$

(a) *Assuming the Birch and Swinnerton-Dyer conjecture, if $A_d = 0$ then there is a non-trivial arithmetic progression of three cubes over $\mathbb{Q}(\sqrt{-d})$.*

(b) *If $A_d \neq 0$ then there is no non-trivial arithmetic progression of three cubes over $\mathbb{Q}(\sqrt{-d})$.*

Proof. Barthel [1] and Frey [7] found independently a modular form $\Phi \in S_{3/2}(144, 1)$ such that its image by the Shimura correspondence is the modular form $f \in S_2(36, 1)$ attached to the elliptic curve $F : y^2 = x^3 + 1$. Note that $F = X_0(36)$. That is, if we denote by $\mathcal{S}h$ the Shimura correspondence [13] that maps a weight $3/2$ modular form to a weight 2 modular form then $\mathcal{S}h(\Phi) = f$.

Now, the q-expansion of Φ is

$$\Phi(q) = \sum_{n \geq 1} A_n q^n.$$

Applying Waldspurger's results [16] to the elliptic curve F, they show that if d is a squarefree positive integer coprime with 6 then

$$L(F^{-d}, 1) = 0 \quad \text{if and only if} \quad A_d = 0.$$

Therefore, if $A_d \neq 0$ we have that $L(F^{-d}, 1) \neq 0$ and by Kolyvagin [11] the rank of $F^{-d}(\mathbb{Q})$ is equal to zero. This proves (b), by Theorem 6. Assuming the Birch and Swinnerton-Dyer conjecture it follows that if $A_d = 0$ then $F^{-d}(\mathbb{Q})$ is infinite. Again by Theorem 6, we have (a). □

Corollary 8. *Let D be a squarefree integer and $\varepsilon \in \{\pm 1\}$.*

(a) *There is a non-trivial arithmetic progression of three cubes over $\mathbb{Q}(\sqrt{D})$ if:*
   (i) *$D = \varepsilon p$ where $p > 3$ is a prime such that $p \equiv 3 \pmod 4$.*
   (ii) *Assuming the Birch and Swinnerton-Dyer conjecture:*
   - *$D > 0$ and D even coprime with 3.*
   - *$D < 0$ and $D \equiv 1, 5 \pmod{12}$.*

(b) *There is no non-trivial arithmetic progression of three cubes over $\mathbb{Q}(\sqrt{D})$ if:*
   (i) *D such that if a prime p divides D then $p \equiv 5 \pmod{12}$ or $p = 3$.*
   (ii) *$D = -p$ where p is a prime such that $p \equiv 1 \pmod{12}$ and $x^4 + 3 = 0$ has not solution over $\mathbb{F}_p$.*

Proof. This corollary is basically a translation of the results of Barthel [1] and Frey [7] on the study of the rank of the D-quadratic twist of the elliptic curve $y^2 = x^3 + 1$ to our context using the Theorem 6. Note that Barthel only treated the case of D negative and she only used Waldspurger's results and Shimura's correspondence à la Tunnell [15] to obtain her results. Meanwhile, Frey treated also the positive case. He used several techniques like Heegner points, 2-descent and the above method used by Barthel too.

Frey [7, Proposition 5] proved that if p is a prime >3 such that $p \equiv 3 \pmod 4$ then $\operatorname{rank} F^{\varepsilon p}(\mathbb{Q}) = 1$. This implies (a)(i).

Barthel showed that the functional equation of $L(F^D, s)$ satisfies that $L(F^D, 1) = 0$ if $D > 0$ and D even coprime with 3 or $D < 0$ and $D \equiv 1, 5 \pmod{12}$. Therefore assuming the Birch and Swinnerton-Dyer conjecture, we have that for the above values of D, the rank of $F^D(\mathbb{Q})$ is positive. This proves (a)(ii).

By [7, Proposition 3 and Bemerkung p. 82] we have that if all the prime divisors of D are 5 modulo 12 then the rank of $F^D(\mathbb{Q})$ is zero. Now let D be with the above condition. Then applying the equality (1) to the elliptic curve F^{-3} and $-D$ and taking into account that F^{-3} is $\mathbb{Q}$-isogenous to F^1 we have that

$$\operatorname{rank} F^{3D}(\mathbb{Q}) = \operatorname{rank} F^{-D}(\mathbb{Q}) = 0,$$

which proves (b)(i).

Table 1.

D	$P=(x,y)\in E^D(\mathbb{Q})$ with $\operatorname{ord} P=\infty$
-30	$(-54,756)$
-26	$(-26,676)$
-23	$(987505/24336,-2386987127/3796416)$
-21	$(189,2646)$
-19	$(-38,361)$
-11	$(-6,189)$
-7	$(7,98)$
-6	$(9,81)$
2	$(10,28)$
7	$(1785/4,75411/8)$
10	$(946/9,28756/27)$
11	$(178849/400,-75621007/8000)$
14	$(217,3185)$
19	$(1173649/2025,1270868732/91125)$
21	$(126,-1323)$
22	$(22825/36,-3446443/216)$
23	$(4655599441/56851600,-201357032252761/428661064000)$
26	$(28249/100,4697693/1000)$

Finally, if p is a prime such that $p\equiv 1\,(\mathrm{mod}\,12)$ and $x^4+3=0$ has not solution over $\mathbb{F}_p$ then $A_p\neq 0$ (cf. [1, Proposition 2] or [7, Korollar 2]) and then by Corollary 7 the proof of (b)(ii) is finished. □

Remark 2. Frey [7, Satz 4, p. 73] states that if p is a prime such that $p\equiv 1\,(\mathrm{mod}\,12)$ and it is not completely split over $\mathbb{Q}(\sqrt[4]{3\varepsilon})$, then $\operatorname{rank} F^{\varepsilon p}(\mathbb{Q})=0$. He proved the case $\varepsilon=-1$ at Korollar 2. But the case $\varepsilon=1$ is not true. For example, for $p=37$ we have that $\operatorname{rank} F^{37}(\mathbb{Q})=2$ and $37\mathcal{O}=\mathfrak{p}_1\mathfrak{p}_2$ is the ideal prime factorization, where $\mathcal{O}$ is the ring of integers of $\mathbb{Q}(\sqrt[4]{3})$.

5.1. Computational results. Using the functionality `mwrank` on `Sage`, we may compute the rank of $E^D(\mathbb{Q})$; if this rank is non-zero, we can also compute an explicit arithmetic progression of three cubes over $\mathbb{Q}(\sqrt{D})$: Let $P=(x,y)\in E^D(\mathbb{Q})$ of infinite order, then $(9D^2+y\sqrt{D})^3,(3xD)^3,(9D^2-y\sqrt{D})^3$ is an arithmetic progression over $\mathbb{Q}(\sqrt{D})$. Table 1 lists explicit examples of such progressions for the range $|D|\leq 30$. At the first column indicates the value of D and the second gives a point $P=(x,y)\in E^D(\mathbb{Q})$ of infinite order.

Example 1. Let $P=(10,28)$ be a generator of the free part of the Mordell–Weil group $E^2(\mathbb{Q})$. The morphism $\phi: E^2\to E$ applied to the point P gives

$$\phi(10,28)=\left(5,7\sqrt{2}\right)\in E(\mathbb{Q}(\sqrt{2})).$$

Now, the isomorphism $\varphi^{-1} : E \to C$ gives

$$\varphi^{-1}([5, 7\sqrt{2}, 1]) = \left[\frac{9+7\sqrt{2}}{18}, \frac{5}{6}, \frac{9-7\sqrt{2}}{18}\right] \in C(\mathbb{Q}(\sqrt{2})),$$

that corresponds to the arithmetic progression $(9+7\sqrt{2})^3, (15)^3, (9-7\sqrt{2})^3$ over $\mathbb{Q}(\sqrt{2})$.

Acknowledgements. We thank José M. Tornero for useful comments.

References

[1] L. Barthel, Courbes elliptiques et formes modulaires de poids 3/2, Séminaire de Théoire des Nombres de Bordeaux 1984–1985, Exposé 17, 1985.

[2] B. J. Birch and W. Kuyk (Eds.), Modular functions of one variable, IV, Lecture Notes in Mathematics **476**, Springer-Verlag, 1975.

[3] J. J. Cannon and W. Bosma (Eds.), Handbook of Magma Functions, Edition 2.15-6 (2009).

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

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

[6] L. E. Dickson, History of the Theory of Numbers, Chelsea, New York, 1971.

[7] G. Frey, Der Rang der Lösungen von $Y^2 = X^3 \pm p^3$ über $\mathbb{Q}$, Manuscripta Math. **48** (1984), 71–101.

[8] E. González-Jiménez and J. Steuding, Arithmetic progressions of four squares over quadratic fields, Publ. Math. Debrecen **77** (2010), 125–138.

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

[10] S. Kamienny, Torsion points on elliptic curves and q-coefficients of modular forms, Invent. Math. **109** (1992), 221–229.

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

[12] A. M. Legendre, Theorie des nombres, Paris, 1798, 409; Mém. Acad. R. Sc. de l'Institut de France, 6, année 1823, 1827, §51, p. 47.

[13] G. Shimura, On modular forms of half-integral weight, Math. Ann. **97** (1973), 440–481.

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

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

[16] J.-L. Waldspurger, Sur les coefficients de Fourier des formes modulaires de poids demi-entier, J. Math. Pures Appl. **60** (1981), 375–484.

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

Enrique González-Jiménez
Departamento de Matemáticas,
Universidad Autónoma de Madrid and Instituto de Ciencias
Matemáticas (CSIC-UAM-UC3M-UCM), 28049 Madrid, Spain
e-mail: enrique.gonzalez.jimenez@uam.es

Received: 24 November 2009