GALOIS THEORY, DISCRIMINANTS AND TORSION SUBGROUP OF ELLIPTIC CURVES

IRENE GARCÍA–SELFA, ENRIQUE GONZÁLEZ–JIMÉNEZ, AND JOSÉ M. TORNERO

ABSTRACT. We find a tight relationship between the torsion subgroup and the image of the mod 2 Galois representation associated to an elliptic curve defined over the rationals. This is shown using some characterizations for the squareness of the discriminant of the elliptic curve.

1. Introduction.

In what follows we will denote by C_n and S_n the cyclic group of order n and the symmetric group acting on n elements, respectively.

Let E be an elliptic curve defined over $\mathbb{Q}$. Let p be a prime number and let $E[p]$ be the group of points of order p on $E(\overline{\mathbb{Q}})$, where $\overline{\mathbb{Q}}$ denotes an algebraic closure of $\mathbb{Q}$. The action of the absolute Galois group $\mathrm{G}_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $E[p]$ defines a mod p Galois representation

$$\rho_{E,p} : \mathrm{G}_{\mathbb{Q}} \longrightarrow \mathrm{Aut}(E[p]) \cong \mathrm{GL}_2(\mathbb{F}_p).$$

Let $\mathbb{Q}(E[p])$ be the number field generated by the coordinates of the points of $E[p]$. Therefore, the Galois extension $\mathbb{Q}(E[p])/\mathbb{Q}$ has Galois group

$$\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \cong \rho_{E,p}(\mathrm{G}_{\mathbb{Q}})$$

For $p = 2$ it is known that $\rho_{E,2}(\mathrm{G}_{\mathbb{Q}})$ can be determined in terms of the discriminant $\Delta(E)$ and $E(\mathbb{Q})[2]$, the points of order 2 defined over the rationals (cf. [20, 19, 21]):

$$\rho_{E,2}(\mathrm{G}_{\mathbb{Q}}) \cong \begin{cases} S_3 & \text{if } \sqrt{\Delta(E)} \notin \mathbb{Q} \text{ and } \#E(\mathbb{Q})[2] = 1, \\ C_3 & \text{if } \sqrt{\Delta(E)} \in \mathbb{Q} \text{ and } \#E(\mathbb{Q})[2] = 1, \\ C_2 & \text{if } \sqrt{\Delta(E)} \notin \mathbb{Q} \text{ and } \#E(\mathbb{Q})[2] > 1, \\ \{\mathrm{id}\} & \text{if } \sqrt{\Delta(E)} \in \mathbb{Q} \text{ and } \#E(\mathbb{Q})[2] > 1. \end{cases} \tag{1}$$

Note that $\mathrm{GL}_2(\mathbb{F}_2) \cong S_3$, the non-split Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_2)$ is isomorphic to C_3 and the conjugated Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_2)$ is isomorphic to C_2.

An elliptic curve E defined over the rationals has always an integral short Weierstrass form. That is, E has a model of the form

$$E: \; Y^2 = X^3 + AX + B, \text{ with } A, B \in \mathbb{Z}.$$

Then the discriminant of this model is $\Delta(E) = -2^4(4A^3 + 27B^2)$. Any change of variables over the rationals preserving this short form is of the type $(x, y) = (u^2x', u^3y')$ with $u \in \mathbb{Q}$, $u \neq 0$. Therefore, if E' is the curve obtained after such a change, we have $u^{12}\Delta(E') = \Delta(E)$. Then the squareness of the discriminant of E does not depend on the short model of E but on E itself.

Our aim is finding if there is a relationship between the torsion group of $E(\mathbb{Q})$ (noted $E(\mathbb{Q})_{\mathrm{tors}}$ in what follows), the discriminant of E and $\rho_{E,2}(\mathrm{G}_{\mathbb{Q}})$.

Assume E is an elliptic curve which has a non–trivial torsion subgroup. Taking into account Mazur's exhaustive classification [16, 17], the possible structures of

Date: June 30, 2009.

2000 *Mathematics Subject Classification.* 11G05 (primary); 11R16 (secondary).

Key words and phrases. Elliptic curves, Cubic equations, Torsion subgroup, Galois theory.

$E(\mathbb{Q})_{\rm tors}$ are C_n for $n = 2 \dots 10, 12$ and $C_2 \times C_{2n}$ for $n = 1 \dots 4$. The easiest cases are those in which the order of $E(\mathbb{Q})_{\rm tors}$ is even and they will be treated at section 2.

The four remaining cases, $E(\mathbb{Q})_{\rm tors} = C_n$, with $n = 3, 5, 7, 9$ will be treated separately at sections 4, 5, 6, 7, respectively. In these cases, thanks to (1), the squareness of $\Delta(E)$ determines the image of $\rho_{E,2}$. We will prove that there are no elliptic curves over the rationals with square discriminant and points of order $5, 7$ and 9 respectively and we will give a parametrization of the elliptic curves with square discriminant and a point of order 3.

Section 3 consists of the necessary background for elliptic curves with points of odd order.

Before stating the main theorems at the last section, we will give a parametrization of all elliptic curves over the rationals having square discriminant at section 8. Some remarks on the case of trivial torsion will be given there too.

At section 9, we will state the main theorems of this paper whose proofs will have been stablished by then.

Finally, in an appendix, we give a complete parametrization of the integer solutions of the Diophantine equations $x^2 + 3y^2 = 4z^3$. These solutions will be needed at sections 4 and 8.

Acknowledgements. We would like to thank to F. Beukers, H. Cohen, H. Darmon, L. Dieulefait, J. González and J. Fernández for useful comments during the preparation of this paper. Special thanks are due to F. Beukers for suggesting the complete parametrization of the Diophantine equation $x^2 + 3y^2 = 4z^3$.

First and third authors were supported partially by FQM–218 and P08–FQM–03894 (Junta de Andalucía) and MTM 2007–66929 (Ministerio de Educación y Ciencia, Spain). Research of the second author was supported in part by grant MTM 2006–10548 (Ministerio de Educación y Ciencia, Spain) and CCG07–UAM/ESP–1814 (Universidad Autónoma de Madrid – Comunidad de Madrid, Spain).

2. The even case.

Let $E : Y^2 = F(X) = X^3 + AX + B$ be an elliptic curve over $\mathbb{Q}$ such that $E(\mathbb{Q})[2]$ has an even positive number of points. Therefore, by (1), the squareness of $\Delta(E)$ determines the image of the mod 2 Galois representation attached to E. By definition $\Delta(E) = 2^4(\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2$, where $\alpha_1, \alpha_2, \alpha_3$ are the roots of $F(X)$. Then if $E(\mathbb{Q})_{\rm tors}$ is non–cyclic we have that $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{Q}$ and $\Delta(E)$ is a square over $\mathbb{Q}$. Meanwhile, if $E(\mathbb{Q})_{\rm tors}$ is cyclic then there is only a point of order 2 on $E(\mathbb{Q})$ and therefore $F(X) = (X - a)(X^2 + aX + b)$ where $a, b \in \mathbb{Q}$ satisfy $A = b - a^2$, $B = -ab$ and $a^2 - 4b$ is a non-square over $\mathbb{Q}$. Since $\Delta(E) = 2^4\Delta(F)$ we have $\Delta(E) = 2^4(a^2 - 4b)(2a^2 + b)^2$ is not a square in $\mathbb{Q}$. This proves the following:

$$\rho_{E,2}(\mathrm{G}_{\mathbb{Q}}) \cong \begin{cases} C_2 & \text{if } \#E(\mathbb{Q})[2] = 2, \\ \{\mathrm{id}\} & \text{if } \#E(\mathbb{Q})[2] = 4. \end{cases}$$

3. Families of elliptic curves with a torsion point of odd order.

In this section we are going to introduce the necessary background related to elliptic curves defined over the rationals with a point of prescribed odd order. There are well-known rational parametrizations for the modular curve $X_1(N)$ with $N \in \{3, 5, 7, 9\}$ (see e.g. Kubert [15]). Therefore these parametrizations give us families of elliptic curves defined over $\mathbb{Q}$ with a point of order $N \in \{3, 5, 7, 9\}$.

An old characterization of elliptic curves containing a rational point of order 3 is given by the Hessian form. Nevertheless we are going to use a new one (cf. [12]) since this will fit better our purposes.

Let us introduce the construction given in [12]; every elliptic curve with a rational point of order 3 can be written in the following form:

$$E_3(\alpha,\beta)\,:\,Y^2=X^3+(27\alpha^4+6\alpha\beta)X+\beta^2-27\alpha^6,\quad \alpha,\beta\in\mathbb{Z}.$$

For the remaining cases that will be used below, an analogous expression can be achieved by means of the Tate normal form [15]:

$$\mathcal{T}ate(b,c)\,:\,Y^2+(1-c)XY-bY=X^3-bX^2,\quad b,c\in\mathbb{Q}^*.$$

Denote by $E_n(\alpha)$ the one-parameter family of curves having a rational point of order n. Then

$$\begin{array}{rcl} E_5(\alpha) & = & \mathcal{T}ate(\alpha,\alpha),\\ E_7(\alpha) & = & \mathcal{T}ate(\alpha^2(\alpha-1),\alpha(\alpha-1))),\\ E_9(\alpha) & = & \mathcal{T}ate(\alpha^2(\alpha-1)(\alpha(\alpha-1)+1),\alpha^2(\alpha-1)). \end{array}$$

Now we can take the above equations to a short Weierstrass form and find the parametric family containing all elliptic curves with points of order 5, 7 and 9. The actual families are:

$$\begin{array}{rcl} E_5(\alpha):Y^2 & = & X^3-27\left(\alpha^4-12\alpha^3+14\alpha^2+12\alpha+1\right)X\\ & & +\,54\left(\alpha^2+1\right)\left(\alpha^4-18\alpha^3+74\alpha^2+18\alpha+1\right) \end{array}$$

$$\begin{array}{rcl} E_7(\alpha):Y^2 & = & X^3-27\left(\alpha^8-12\alpha^7+42\alpha^6-56\alpha^5+35\alpha^4-14\alpha^2+4\alpha+1\right)X\\ & & +\,54\left(\alpha^{12}-18\alpha^{11}+117\alpha^{10}-354\alpha^9+570\alpha^8-486\alpha^7+\right.\\ & & \left.273\alpha^6-222\alpha^5+174\alpha^4-46\alpha^3-15\alpha^2+6\alpha+1\right) \end{array}$$

$$\begin{array}{rcl} E_9(\alpha):Y^2 & = & X^3-27\left(\alpha^3-3\alpha^2+1\,\right)(\,\alpha^9-9\alpha^8+27\alpha^7-48\alpha^6+54\alpha^5-\\ & & \left.45\alpha^4+27\alpha^3-9\alpha^2+1\right)X\\ & & +\,54\left(\alpha^{18}-18\alpha^{17}+135\alpha^{16}-570\alpha^{15}+1557\alpha^{14}-2970\alpha^{13}+\right.\\ & & 4128\alpha^{12}-4230\alpha^{11}+3240\alpha^{10}-2032\alpha^9+1359\alpha^8-1080\alpha^7+\\ & & \left.735\alpha^6-306\alpha^5+27\alpha^4+42\alpha^3-18\alpha^2+1\right) \end{array}$$

Therefore, an elliptic curve E defined over $\mathbb{Q}$ with a rational point of order $n=3$ (resp. $n=5$, 7 or 9) is $\mathbb{Q}$–isomorphic to $E_3(\alpha,\beta)$ (resp. $E_n(\alpha)$ for $n=5,7$ or 9) for some $\alpha,\beta\in\mathbb{Z}$ (resp. $\alpha\in\mathbb{Q}$).

These kind of arguments have proved fruitful in the last years, as a number of results have appeared based on them [1, 14, 11, 13]. Now we can write the discriminant Δ_n for the above elliptic curves E_n, to obtain

$$\begin{array}{rcl} \Delta_3(\alpha,\beta) & = & -2^4\cdot3^3\cdot(5\alpha^3+\beta)(9\alpha^3+\beta)^3\\ \Delta_5(\alpha) & = & 2^{12}\cdot3^{12}\cdot\alpha^5(\alpha^2-11\alpha-1)\\ \Delta_7(\alpha) & = & 2^{12}\cdot3^{12}\cdot\alpha^7(\alpha-1)^7(\alpha^3-8\alpha^2+5\alpha+1)\\ \Delta_9(\alpha) & = & 2^{12}\cdot3^{12}\cdot\alpha^9(\alpha-1)^9(\alpha^2-\alpha+1)^3(\alpha^3-6\alpha^2+3\alpha+1) \end{array}$$

In the following section we will study the rationality of the square root of the above discriminants to decide whether the corresponding Galois group is C_3 or S_3.

4. The case $n=3$

Elliptic curves with points of order three must yield a discriminant with the form $\Delta_3(\alpha,\beta)$ for some $\alpha,\beta\in\mathbb{Z}$. So, in order to find an elliptic curve E having square discriminant we are bound to find integral solutions to the equation

$$\omega^2=-3\cdot(5\alpha^3+\beta)(9\alpha^3+\beta).$$

Let us denote $g = \gcd(5\alpha^3 + \beta, 9\alpha^3 + \beta)$. This necessarily leads to

$$5\alpha^3 + \beta = \pm gu^2, \pm 3gv^2 \text{ and } 9\alpha^3 + \beta = \mp 3gv^2, \mp gu^2, \text{ respectively}$$

for some integers u and v. Solving the above Diophantine systems of equations is equivalent to finding the integer solutions to

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

where $(x, y, z) = (ug^2, vg^2, \mp\alpha g)$. Thus, for the first two systems we obtain that the elliptic curves $E_3(\alpha, \beta)$ have square discriminant for:

$$(\alpha, \beta) = \left(\mp\frac{z}{g}, \pm\frac{x^2 + 5z^3}{g^3}\right), \tag{2}$$

and for the last two systems we obtain

$$(\alpha, \beta) = \left(\mp\frac{z}{g}, \pm\frac{3y^2 + 5z^3}{g^3}\right). \tag{3}$$

In all those cases $x, y, z \in \mathbb{Z}$ satisfies $x^2 + 3y^2 = 4z^3$. At the appendix, we give parametrizations of all integer solutions of the Diophantine equation $x^2+3y^2 = 4z^3$ at Lemma 1 in terms of parameters (a, b, c, d). Then we can clear denominators and obtain $\mathbb{Q}$-isomorphic elliptic curves

$$E^{(i)}(a, b, c, d) : Y^2 = P^{(i)}(a, b, c, d)(X)$$

attached to the parametrization (i), for $i = 1, 2$, where:

$$\begin{aligned}
P^{(1)}(a,b,c,d)(X) = {} & X^3 - 9(c^2+cd+d^2)^3(a^2+ab+b^2)(3a^6c^2+3a^6cd+a^6d^2+9a^5bc^2-3a^5bcd\\
& -3a^5bd^2-30a^4b^2cd-15a^3b^3c^2-15a^3b^3cd+25a^3b^3d^2+30a^2b^4cd+30a^2b^4d^2+9ab^5c^2\\
& +21ab^5cd+9ab^5d^2+3b^6c^2+3b^6cd+b^6d^2)X\\
& +9(c^2+cd+d^2)^4(6a^{12}c^4+12a^{12}c^3d+12a^{12}c^2d^2+6a^{12}cd^3+a^{12}d^4+36a^{11}bc^4\\
& +36a^{11}bc^3d+18a^{11}bc^2d^2-6a^{11}bcd^3-6a^{11}bd^4+72a^{10}b^2c^4-54a^{10}b^2c^3d-72a^{10}b^2c^2d^2\\
& -78a^{10}b^2cd^3-18a^{10}b^2d^4+30a^9b^3c^4-318a^9b^3c^3d-102a^9b^3c^2d^2-132a^9b^3cd^3-4a^9b^3d^4\\
& -81a^8b^4c^4-378a^8b^4c^3d+162a^8b^4c^2d^2-252a^8b^4cd^3+45a^8b^4d^4-108a^7b^5c^4-108a^7b^5c^3d\\
& +108a^7b^5c^2d^2-576a^7b^5cd^3+216a^7b^5d^4-72a^6b^6c^4-144a^6b^6c^3d-468a^6b^6c^2d^2\\
& -396a^6b^6cd^3+600a^6b^6d^4-108a^5b^7c^4-324a^5b^7c^3d-216a^5b^7c^2d^2+684a^5b^7cd^3\\
& +900a^5b^7d^4-81a^4b^8c^4+54a^4b^8c^3d+810a^4b^8c^2d^2+1386a^4b^8cd^3+756a^4b^8d^4+30a^3b^9c^4\\
& +438a^3b^9c^3d+1032a^3b^9c^2d^2+1002a^3b^9cd^3+374a^3b^9d^4+72a^2b^{10}c^4+342a^2b^{10}c^3d\\
& +522a^2b^{10}c^2d^2+384a^2b^{10}cd^3+114a^2b^{10}d^4+36ab^{11}c^4+108ab^{11}c^3d+126ab^{11}c^2d^2\\
& +78ab^{11}cd^3+18ab^{11}d^4+6b^{12}c^4+12b^{12}c^3d+12b^{12}c^2d^2+6b^{12}cd^3+b^{12}d^4)
\end{aligned}$$

$$\begin{aligned}
P^{(2)}(a,b,c,d)(X) = {} & X^3 - 3(c^2+cd+d^2)^3(a^2+ab+b^2)(a^6c^2+a^6cd+7a^6d^2+3a^5bc^2+39a^5bcd\\
& +39a^5bd^2+60a^4b^2c^2+150a^4b^2cd+60a^4b^2d^2+115a^3b^3c^2+115a^3b^3cd-5a^3b^3d^2+60a^2b^4c^2\\
& -30a^2b^4cd-30a^2b^4d^2+3ab^5c^2-33ab^5cd+3ab^5d^2+b^6c^2+b^6cd+7b^6d^2)X\\
& -(c^2+cd+d^2)^4(2a^{12}c^4+4a^{12}c^3d-24a^{12}c^2d^2-26a^{12}cd^3-37a^{12}d^4+12a^{11}bc^4-156a^{11}bc^3d\\
& -414a^{11}bc^2d^2-534a^{11}bcd^3-366a^{11}bd^4-228a^{10}b^2c^4-1446a^{10}b^2c^3d-2880a^{10}b^2c^2d^2\\
& -3246a^{10}b^2cd^3-1434a^{10}b^2d^4-1250a^9b^3c^4-5902a^9b^3c^3d-10758a^9b^3c^2d^2-9508a^9b^3cd^3\\
& -2876a^9b^3d^4-4059a^8b^4c^4-16002a^8b^4c^3d-23382a^8b^4c^2d^2-14868a^8b^4cd^3-2925a^8b^4d^4\\
& -8604a^7b^5c^4-25740a^7b^5c^3d-26676a^7b^5c^2d^2-10944a^7b^5cd^3-936a^7b^5d^4-11112a^6b^6c^4\\
& -22224a^6b^6c^3d-13428a^6b^6c^2d^2-2316a^6b^6cd^3+480a^6b^6d^4-8604a^5b^7c^4-8676a^5b^7c^3d\\
& -1080a^5b^7c^2d^2+396a^5b^7cd^3+468a^5b^7d^4-4059a^4b^8c^4-234a^4b^8c^3d+270a^4b^8c^2d^2\\
& -126a^4b^8cd^3+504a^4b^8d^4-1250a^3b^9c^4+902a^3b^9c^3d-552a^3b^9c^2d^2+698a^3b^9cd^3+526a^3b^9d^4\\
& -228a^2b^{10}c^4+534a^2b^{10}c^3d+90a^2b^{10}c^2d^2+912a^2b^{10}cd^3+150a^2b^{10}d^4+12ab^{11}c^4+204ab^{11}c^3d\\
& +126ab^{11}c^2d^2+222ab^{11}cd^3-78ab^{11}d^4+2b^{12}c^4+4b^{12}c^3d-24b^{12}c^2d^2-26b^{12}cd^3-37b^{12}d^4)
\end{aligned}$$

with the following discriminants

$$\begin{aligned}\Delta\left(E^{(1)}\right) &= 2^4 3^6 (c^2+cd+d^2)^8 (a^3d+3a^2bc+3a^2bd+3ab^2c-b^3d)^6 \\ &\quad (2a^3c+a^3d+3a^2bc-3a^2bd-3ab^2c-6ab^2d-2b^3c-b^3d)^2 \\ \Delta\left(E^{(2)}\right) &= 2^4 3^4 (c^2+cd+d^2)^8 (a^3d+3a^2bc+3a^2bd+3ab^2c-b^3d)^2 \\ &\quad (2a^3c+a^3d+3a^2bc-3a^2bd-3ab^2c-6ab^2d-2b^3c-b^3d)^6\end{aligned}$$

Therefore we have proved the following result:

Proposition 1. *Let E be an elliptic curve defined over $\mathbb{Q}$ with a rational point of order 3 such that $\sqrt{\Delta(E)} \in \mathbb{Q}$. Then there exist $a,b,c,d \in \mathbb{Z}$ such that E is $\mathbb{Q}$-isomorphic to either $E^{(1)}(a,b,c,d)$ or $E^{(2)}(a,b,c,d)$.*

5. The case $n = 5$

Let us have a look at the case $n = 5$. If we throw away quadratic factors in $\Delta_5(\alpha)$ we will find out that curves E with points of order 5, for which $\sqrt{\Delta(E)} \in \mathbb{Q}$ are parametrized by the affine rational points of the elliptic curve

$$\mathcal{D}_5 \,:\, z^2 = \alpha(\alpha^2 - 11\alpha - 1),$$

where the discriminant of the right–hand side polynomial is, remarkably, 5^3.

This is a well–known elliptic curve, in fact is $\mathbb{Q}$-isogenous to the modular curve $X_0(20)$. The elliptic curve $\mathcal{D}_5$ is denoted by `20A4` in Cremona's tables [7] or `20C` in Antwerp tables [3]. Looking on that tables, or using a computer algebra package like `SAGE` or `MAGMA` ([24], [4] resp.), we check that $\mathcal{D}_5(\mathbb{Q}) = \{(0,0)\} \cup \{[0:1:0]\}$. Therefore the only affine rational point is $(0,0)$, which implies $\alpha = 0$. This precise value does not yield an elliptic curve, but a singular cubic on the family $E_5(\alpha)$. This proves the following result:

Proposition 2. *Let E be an elliptic curve with $C_5 \subset E(\mathbb{Q})_{\text{tors}}$. Then $\sqrt{\Delta(E)} \notin \mathbb{Q}$.*

6. The case $n = 7$

Move now to $n = 7$, where the analogous argument to the case $n = 5$ shows that curves with points of order seven for which $\sqrt{\Delta(E)} \in \mathbb{Q}$ are parametrized by the affine rational points of the hyperelliptic curve

$$\mathcal{D}_7 \,:\, z^2 = \alpha(\alpha-1)(\alpha^3 - 8\alpha^2 + 5\alpha + 1),$$

where, by the way, we have that the discriminant for the right–hand side polynomial is 7^4. We have now a hyperelliptic curve of genus 2, a much harder nut to crack; but we are lucky. Using `MAGMA` we obtain that the rank of the Jacobian of this genus 2 curve is 0, which makes it perfect for Chabauty's algorithm [5]. This method computes the full list of points in the jacobian, then all rational points in the curve, which turn out to be $\mathcal{D}_7(\mathbb{Q}) = \{(0,0),(1,0)\} \cup \{[0:1:0]\}$. Again the affine rational points annhilate the discriminant of $E_7(\alpha)$ and hence we have proven the following result.

Proposition 3. *Let E be an elliptic curve with $E(\mathbb{Q})_{\text{tors}} \cong C_7$. Then $\sqrt{\Delta(E)} \notin \mathbb{Q}$.*

7. The case $n = 9$

Finally, the case $n = 9$. This can also be dealt with in a similar way, but a little extra work is needed. Following the steps as the above sections, the hyperelliptic curve parametrizing curves with $E(\mathbb{Q})_{\rm tors} \cong C_9$ and square discriminant is

$$\mathcal{D}_9 \,:\, z^2 = \alpha(\alpha-1)(\alpha^2-\alpha+1)(\alpha^3-6\alpha^2+3\alpha+1)\,.$$

Lemma. $\mathcal{D}_9(\mathbb{Q}) = \{(0,0),(1,0)\} \cup \{[0:1:0]\}\,.$

Proof. Let $u \in \mathrm{Aut}_{\mathbb{Q}}(\mathcal{D}_9)$ defined by

$$u(X,Y) = \left(\frac{1}{1-X}, \frac{Y}{(1-X)^4}\right).$$

We have that u has order 3 and Riemann-Hurwitz formulae tell us that the quotient curve $C/\langle u\rangle$ has genus 1. In fact this curve is an elliptic curve defined over $\mathbb{Q}$, since $(0,0) \in C(\mathbb{Q})$ and u is defined over $\mathbb{Q}$. We will denote this elliptic curve by $\mathcal{E}_9$. A Weierstrass equation for $\mathcal{E}_9$ is given by $v^2 = u^3 - 27$ and the quotient morphism is given by:

$$\begin{array}{rcl} \pi : \mathcal{D}_9 & \longrightarrow & \mathcal{E}_9 \\ (\alpha, z) & \mapsto & (u,v) = \left(\dfrac{\alpha^3-3\alpha^2+1}{\alpha(\alpha-1)}, \dfrac{z(\alpha^2-\alpha+1)}{\alpha^2(\alpha-1)^2}\right) \end{array}$$

Using `SAGE` or `MAGMA` we compute that $\mathcal{E}_9$ is $\mathbb{Q}$-isogenous to the modular curve $X_0(36)$, and it is the elliptic curve denotes by `36A3` in Cremona's tables or `36C` in Antwerp tables. The Mordell-Weil group of this elliptic curve is:

$$\mathcal{E}_9(\mathbb{Q}) = \{(3,0),[0:1:0]\} \cong \mathbb{Z}/2\mathbb{Z}.$$

Now, to compute the set $\mathcal{D}_9(\mathbb{Q})$ we just need to compute the preimages of the points of $\mathcal{E}_9(\mathbb{Q})$ by the quotien morphism that are defined over $\mathbb{Q}$ and then we obtain the desired result. □

Then we have proved the following result:

Proposition 4. *Let E be an elliptic curve with $E(\mathbb{Q})_{\rm tors} \cong C_9$. Then $\sqrt{\Delta(E)} \notin \mathbb{Q}$.*

8. The generic elliptic curve with square discriminant.

Let $E \,:\, Y^2 = X^3 + AX + B$ be an elliptic curve with $A, B \in \mathbb{Z}$. Let us study when the discriminant $\Delta(E)$ is a square. This is equivalent to looking for integer solutions to the Diophantine equation

$$4A^3 + 27B^2 = -C^2.$$

Making the change of variables $(x,y,z) = (C, 3B, -A)$ we obtain that the integer solutions of the generalized Fermat equation $x^2+3y^2 = 4z^3$ give us all the elliptic curves defined over the rationals with square discriminant. Lemma 1 from the appendix gives us a complete parametrization of the above Diophantine equation, which yields to the following elliptic curve:

$$\begin{aligned} E_{alt}(a,b,c,d) \,:\, Y^2 \;\; = \;\; & X^3 - 3^4(c^2+cd+d^2)(a^2+ab+b^2)X \\ & +3^5(c^2+cd+d^2)(a^3d+3a^2bc+3a^2bd+3ab^2c-b^3d) \end{aligned}$$

with discriminant

$$\Delta(E_{alt}) = 2^4 3^{12}(c^2{+}cd{+}d^2)^2(2a^3c{+}a^3d{+}3a^2bc{-}3a^2bd{-}3ab^2c{-}6ab^2d{-}2b^3c{-}b^3d)^2$$

Propositions 2, 3 and 4, together with Section 2, tell us that the above elliptic curve has torsion subgroup either trivial, C_3 or non-cyclic. Then we have proved the following result:

Proposition 5. *Let E be an elliptic curve defined over $\mathbb{Q}$ such that $\sqrt{\Delta(E)} \in \mathbb{Q}$. Then there exist $a, b, c, d \in \mathbb{Z}$ such that E is $\mathbb{Q}$-isomorphic to $E_{alt}(a, b, c, d)$. Moreover, $E(\mathbb{Q})_{\text{tors}}$ is either trivial, non-cyclic or C_3.*

Remark 1. Let $P(X)$ be an irreducible polynomial with integer coefficients and degree 3 such that the cubic number field attached to $P(X)$ is cyclic. Then the elliptic curve $E : Y^2 = P(X)$ satisfies $E(\mathbb{Q})_{\text{tors}}$ is either trivial or C_3. For example, let be $P_m(X) = X^3 + mX^2 - (m+3)X + 1 \in \mathbb{Z}[X]$, $m \in \mathbb{Z}$ and $E_m : Y^2 = P_m(X)$. The irreducible polynomial $P_m(X)$ defines a cubic fields K_m that has been studied by several authors. This family has been called the *simplest cubic field* ([22]). Its discriminant satisfies $\Delta(P_m) = (m^2 + 3m + 9)^2$, hence $K_m = \mathbb{Q}(E[2])$ is cyclic and therefore $\rho_{E_m,2}(\mathrm{G}_{\mathbb{Q}}) \cong \mathrm{Gal}(K_m/\mathbb{Q}) = C_3$. Therefore $E_m(\mathbb{Q})_{\text{tors}}$ is trivial or C_3. Moreover, it has been proved [10] that if $m^2 + 3m + 9$ is square-free, then $E_m(\mathbb{Q})_{\text{tors}}$ is trivial.

Remark 2. We have checked on the extended Cremona's tables [8] of elliptic curves with conductor less than 130.000. Among them, 452.724 curves have torsion subgroup either trivial or C_3. At the table below appears the specific proportions of curves according to their torsion group and the squareness of their discriminant:

$E(\mathbb{Q})_{\text{tors}}$	$\sqrt{\Delta(E)} \in \mathbb{Q}$	$\sqrt{\Delta(E)} \notin \mathbb{Q}$
$\{\mathcal{O}\}$	0.00383	0.9553
C_3	0.00008	0.0408

9. Main theorems.

To end up we will summarize our results in the following theorems.

Theorem 1. *Let E be an elliptic curve defined over $\mathbb{Q}$. Then*

(1) *If $E(\mathbb{Q})_{\text{tors}}$ is non–cyclic then $\sqrt{\Delta(E)} \in \mathbb{Q}$.*

(2) *If $E(\mathbb{Q})_{\text{tors}} \cong C_n$ for $n = 2, 4, 5 \ldots 10, 12$ then $\sqrt{\Delta(E)} \notin \mathbb{Q}$.*

(3) *$E(\mathbb{Q})_{\text{tors}} \cong C_3$ and $\sqrt{\Delta(E)} \in \mathbb{Q}$ if and only if there exist $a, b, c, d \in \mathbb{Z}$ such that E is $\mathbb{Q}$-isomorphic to either $E^{(1)}(a, b, c, d)$ or $E^{(2)}(a, b, c, d)$ and the corresponding polynomial $P^{(i)}(a, b, c, d))$ is irreducible.*

(4) *$E(\mathbb{Q})_{\text{tors}}$ is trivial and $\sqrt{\Delta(E)} \in \mathbb{Q}$ if and only if there exist $a, b, c, d \in \mathbb{Z}$ such that E is $\mathbb{Q}$-isomorphic to $E_{alt}(a, b, c, d)$ and $a, b, c, d \notin \mathcal{S}_2, \mathcal{S}_3$ where*

$$\begin{aligned} \mathcal{S}_2 &= \left\{ (a,b,c,d) \in \mathbb{Z}^4 \,\middle|\, \Psi_2(a,b,c,d)(X) = \prod_{i=1}^{3} (X - \alpha_i) \text{ such that } \alpha_1, \alpha_2, \alpha_3 \in \mathbb{Z} \right\} \\ \mathcal{S}_3 &= \left\{ (a,b,c,d) \in \mathbb{Z}^4 \,\middle|\, \exists (\alpha, \beta) \in \mathbb{Q}^2, \text{such that} \left\{ \begin{array}{l} \Psi_3(a,b,c,d)(\alpha) = 0 \\ \Psi_2(a,b,c,d)(\alpha) = \beta^2 \end{array} \right\} \right. \end{aligned}$$

and $\Psi_n(a, b, c, d)(X)$ denotes the n-division polynomial attached to $E_{alt}(a, b, c, d)$.

Theorem 2. *Let E be an elliptic curve defined over $\mathbb{Q}$. Then*

(1) *$E(\mathbb{Q})_{\text{tors}}$ is non–cyclic if and only if $\rho_{E,2}(\mathrm{G}_{\mathbb{Q}}) = \{\mathrm{id}\}$.*

(2) *$E(\mathbb{Q})_{\text{tors}} \cong C_{2n}$ if and only if $\rho_{E,2}(\mathrm{G}_{\mathbb{Q}}) \cong C_2$.*

(3) *If $E(\mathbb{Q})_{\text{tors}} \cong C_n$ for $n = 5, 7, 9$, then $\rho_{E,2}(\mathrm{G}_{\mathbb{Q}}) = \mathrm{GL}_2(\mathbb{F}_2)$.*

(4) *If $E(\mathbb{Q})_{\text{tors}} \cong C_3$ then $\rho_{E,2}(\mathrm{G}_{\mathbb{Q}}) \cong C_3$ if and only if there exist $a, b, c, d \in \mathbb{Z}$ such that E is $\mathbb{Q}$-isomorphic to either $E^{(1)}(a, b, c, d)$ or $E^{(2)}(a, b, c, d)$. Otherwise, $\rho_{E,2}(\mathrm{G}_{\mathbb{Q}}) = \mathrm{GL}_2(\mathbb{F}_2)$.*

(5) *If $E(\mathbb{Q})_{\text{tors}}$ is trivial then $\rho_{E,2}(\mathrm{G}_{\mathbb{Q}}) \cong C_3$ if and only if there exist $a, b, c, d \in \mathbb{Z}$ such that E is $\mathbb{Q}$-isomorphic to $E_{alt}(a, b, c, d)$. Otherwise, $\rho_{E,2}(\mathrm{G}_{\mathbb{Q}}) = \mathrm{GL}_2(\mathbb{F}_2)$.*

The next table summarizes part of the main results of this paper:

$E(\mathbb{Q})_{\rm tors}$	$\sqrt{\Delta(E)} \in \mathbb{Q}$?	$\rho_{E,2}(\mathrm{G}_{\mathbb{Q}})$
$\{\mathcal{O}\}$	Yes / No	C_3 / S_3
C_2	No	C_2
C_3	Yes / No	C_3 / S_3
C_4	No	C_2
C_5	No	S_3
C_6	No	C_2
C_7	No	S_3
C_8	No	C_2
C_9	No	S_3
C_{10}	No	C_2
C_{12}	No	C_2
$C_2 \times C_2$	Yes	$\{\mathrm{id}\}$
$C_2 \times C_4$	Yes	$\{\mathrm{id}\}$
$C_2 \times C_6$	Yes	$\{\mathrm{id}\}$
$C_2 \times C_8$	Yes	$\{\mathrm{id}\}$

10. Appendix: The generalized Fermat equation $x^2+3y^2=4z^3$

The generalized Fermat equation $Ax^p + By^q = Cz^r$, where $A, B, C \in \mathbb{Z}^*$ and $p, q, r \in \mathbb{Z}_{>0}$, have been studied by several people for the last decades. Starting with the huge work on Diophantine equations due to L.J. Mordell [18]. After that the main results are due to H. Darmon and A. Granville [9], who proved that the generalized Fermat equation has infinite primitive solutions (i.e. $gcd(x, y, z) = 1$) in the case $1/p + 1/q + 1/r > 1$. Then F. Beukers [2] gave parametrizations for the solutions of this equation in the above case. H. Cohen in his huge new books about number theory calls this equation Super-Fermat equation and he also provides solutions for several cases. In particular, H. Cohen [6, Proposition 14.2.1(ii)] displays primitive solutions to the equation we are interested in. However, we would like to have all integer solutions, not just the primitive ones. The following parametrization was pointed out to us by F. Beukers:

Lemma 1. *The integer solutions of the equation $x^2 + 3y^2 = 4z^3$ are parametrized by the following family of four variables:*

$$\mathcal{F} : \left\{ \begin{array}{lcl} x & = & (c^2+cd+d^2)(3a^2b(c-d)+a^3(2c+d)-b^3(2c+d)-3ab^2(c+2d)) \\ y & = & (c^2+cd+d^2)(3ab^2c+a^3d-b^3d+3a^2b(c+d)) \\ z & = & (c^2+cd+d^2)(a^2+ab+b^2) \end{array} \right.$$

Proof. Let (x, y, z) be an integer solution of the equation $x^2 + 3y^2 = 4z^3$. Over $\mathbb{Q}(\sqrt{-3})$we have $(x+\sqrt{-3}y)(x-\sqrt{-3}y) = 4z^3$. We are going to work over the ring of algebraic integers of $\mathbb{Q}(\sqrt{-3})$, noted $\mathcal{O} = \mathbb{Z}[\rho]$ where $\rho = (1+\sqrt{-3})/2$. This ring is a P.I.D., where it is easy to check that $\gcd(x+\sqrt{-3}y, x-\sqrt{-3}y) = r \in \mathbb{Z}$, for all $x, y \in \mathbb{Z}$. Therefore $x + \sqrt{-3}y = r \cdot \mu$, $x - \sqrt{-3}y = r \cdot \bar{\mu}$ with $\mu \in \mathcal{O}$ and $\gcd(\mu, \bar{\mu}) = 1$.

Let $p \neq 3$ be a non inert prime dividing r. Thus $p = \alpha\bar{\alpha}$ for some $\alpha \in \mathcal{O}$. Suppose that α divides μ, then we have $r = r'p$ and $\mu = \alpha\mu'$ for some $r' \in \mathbb{Z}$ and $\mu' \in \mathcal{O}$. In other words, $x + \sqrt{-3}y = (r'\alpha\bar{\alpha})(\alpha\mu')$. Therefore

$$4z^3 = r^2\mu\bar{\mu} = (r')^2p^3\mu'\bar{\mu}',$$

that is, p divides z. Then we can remove all the primes as above obtaining $4w^3 = s^2\gamma\bar{\gamma}$ such that $s, \gamma, \bar{\gamma}$ are pairwise coprimes. This yields $s = 2t^3$ and $\gamma = \beta^3$ for some $t \in \mathbb{Z}$ and $\beta \in \mathcal{O}$. Now collecting all the factors back we obtain

$$x + \sqrt{-3}y = 2(a + b\rho)^3(c + d\rho)(c^2 + cd + d^2)$$

for some $a, b, c, d \in \mathbb{Z}$. Its easy to check that $z = \mathcal{N}_{\mathcal{O}}((a + b\rho)(c + d\rho))$, where $\mathcal{N}_{\mathcal{O}}$ denotes the norm on $\mathcal{O}$. In order to attach the parametrization, we only have to expand the above expression and compute the coefficient of $\sqrt{-3}$ (corresponding to y) and the part in $\mathbb{Z}$ (corresponding to x). □

References

[1] M.A. Bennett; P. Ingram: Torsion subgroups of elliptic curves in short Weierstrass form. Trans. Amer. Math. Soc. **357** (2005) 3325–3337

[2] F. Beukers: The Diophantine equation $Ax^p + By^q = Cz^r$, Duke Math.J. 91(1998), 61-88.

[3] B. J. Birch; W. Kuyk (eds.): Modular Functions of One Variable IV. Lecture Notes in Mathematics **476**, Springer-Verlag, 1975.

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

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

[6] H. Cohen: Number Theory, vol. II: Analytic and modern tools. Springer, 2007.

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

[8] J. E. Cremona. Elliptic curve data. Available on `http://www.warwick.ac.uk/~masgaj/ftp/data/`, 2006.

[9] H. Darmon; A. Granville: On the equation $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$. Bull. London Math. Soc. 27 (1995) 513-543.

[10] S. Duquesne. Integral points on elliptic curves defined by simplest cubic fields. Experiment. Math. 10 (2001), no. 1, 91–102.

[11] I. García–Selfa; M.A. Olalla; J.M. Tornero: Computing the rational torsion of an elliptic curve using Tate normal form. J. Number Theory **96** (2002) 76–88.

[12] I. García–Selfa; J.M. Tornero: A complete diophantine characterization of the rational torsion of an elliptic curve. Available at the arXiv as math.NT/0703578.

[13] I. García–Selfa; J.M. Tornero: Thue equations and torsion groups of elliptic curves. J. Number Theory **129** (2009) 367–380.

[14] P. Ingram: Diophantine analysis and torsion on elliptic curves. Proc. Lond. Math. Soc. **94** (2007) 137–154.

[15] D.S. Kubert: Universal bounds on the torsion of elliptic curves. Proc. London Math. Soc. **33** (2) (1976) 193–237.

[16] B. Mazur: Modular curves and the Eisenstein ideal. Inst. Hautes Études Sci. Publ. Math. **47** (1977) 33–186.

[17] B. Mazur: Rational isogenies of prime degree. Invent. Math. **44** (1978) 129–162.

[18] L.J. Mordell: Diophantine equations. Academic Press, 1969.

[19] J.-P. Serre, Abelian ℓ-Adic Representations and Elliptic Curves. W. A. Benjamin, Inc., 1968.

[20] J.-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. Invent. Math. **15** (1972), 259–331.

[21] J.-P. Serre and J. Tate, Good reduction of abelian varieties. Ann. of Math. **88** (1968), 492–517.

[22] D. Shanks: The simplest cubic number fields, Math. Comp. 28 (1974), 1137–1152.

[23] J.H. Silverman: The arithmetic of elliptic curves. Springer, 1986.

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

Departamento de Matemáticas, Universidad de Huelva. Facultad de Ciencias Experimentales. Campus de "El Carmen", Avenida de las Fuerzas Armadas, s/n. 21071 Huelva (Spain).

E-mail address: irene.garcia@dmat.uhu.es

Departamento de Matemáticas, Universidad Autónoma de Madrid. 28049 Madrid (Spain).

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

Departamento de Álgebra, Universidad de Sevilla. P.O. 1160. 41080 Sevilla (Spain).

E-mail address: tornero@us.es