The automorphism group of the non-split Cartan modular curve of level 11

Valerio Dose, Julio Fernández, Josep González and René Schoof

March 26, 2014

Abstract

We derive equations for the modular curve $X_{ns}(11)$ associated to a non-split Cartan subgroup of $GL_2(F_{11})$. This allows us to compute the automorphism group of the curve and show that it is isomorphic to Klein’s four group.

Introduction

Let $p$ be a prime. The modular curve $X_{ns}(p)$ associated to a non-split Cartan subgroup of $GL_2(F_p)$ is an algebraic curve that is defined over $\mathbb{Q}$. It admits a so-called modular involution $w$, also defined over $\mathbb{Q}$. One may conjecture that, for large $p$, the modular involution is the only non-identity automorphism of $X_{ns}(p)$, even over $\mathbb{C}$. However, for very small primes $p$ this is not the case. Indeed, for $p = 2, 3$ and $5$ the genus of $X_{ns}(p)$ is $0$, while for $p = 7$ the genus is $1$. See [1], Table A.1. For these primes the curve $X_{ns}(p)$ admits therefore infinitely many automorphisms. The present paper is devoted to $p = 11$ and the genus $4$ curve $X_{ns}(11)$. We prove the following.

Theorem. The automorphism group over $\mathbb{C}$ of the modular curve $X_{ns}(11)$ is isomorphic to Klein’s four group. It is generated by the modular involution $w$ and the involution $\varrho$ described in Corollary [1].

Our proof for this result is presented in section [3]. It relies on an explicit description of the regular differentials and the Jacobian of $X_{ns}(11)$. These are discussed in section [2]. We make use of equations for the curve $X_{ns}(11)$, which are obtained in section [4].

1 Equations

In this section we derive equations for the modular curve $X_{ns}(11)$. We do this by exploiting the modular curve $X^+_{ns}(11)$ associated to the normalizer of a non-split Cartan subgroup of level 11.

We recall some definitions [1]. For any prime $p$, the ring of $2 \times 2$ matrices over $F_p$ contains subfields that are isomorphic to $F_{p^2}$. A non-split Cartan subgroup $U$ of $GL_2(F_p)$ is by definition the unit group of such a subfield. The modular curve $X_{ns}(p)$ classifies $U$–isomorphism classes of pairs $(E, \phi)$, where $E$ is an elliptic curve and $\phi$ is an isomorphism from the group of $p$-torsion...
points \( E[p] \) to \( \mathbf{F}_p \times \mathbf{F}_p \). Two such pairs \((E, \phi)\) and \((E', \phi')\) are \(U\)-isomorphic if there is an isomorphism \( f : E \rightarrow E' \) for which the matrix \( \phi'f\phi^{-1} \) is in \( U \).

The group \( U \) has index 2 in its normalizer \( U^+ \subset \text{GL}_2(\mathbf{F}_p) \). The modular involution \( w \) of \( X_{ns}(p) \) maps \((E, \phi)\) to \((E, \alpha \phi)\), where \( \alpha \) is any matrix in \( U^+ \setminus U \). In a way that is analogous to the moduli description for \( X_{ns}(p) \), the modular curve \( X^+_{ns}(p) \) classifies \( U^+\)-isomorphism classes of pairs \((E, \phi)\). There are natural morphisms

\[
X_{ns}(p) \xrightarrow{\pi} X^+_{ns}(p) \xrightarrow{\mathbf{j}} X(1).
\]

Here \( X(1) \) indicates the \( j \)-line. It parametrizes elliptic curves up to isomorphism. The morphism \( \mathbf{j} \) maps \((E, \phi)\) to the \( j \)-invariant of \( E \). It has degree \( \frac{1}{2}p(p-1) \), while the morphism \( \pi \) has degree 2.

Both curves \( X_{ns}(p) \) and \( X^+_{ns}(p) \) are defined over \( \mathbf{Q} \). A point \((E, \phi)\) of \( X_{ns}(p) \) or \( X^+_{ns}(p) \) is defined over an extension \( \mathbf{Q} \subset K \) if and only if \( E \) is defined over \( K \) and, for all \( \sigma \in \text{Gal}(K/\mathbf{Q}) \), the matrix \( \phi \sigma \phi^{-1} \) is in \( U \) or \( U^+ \) respectively. This implies that, for \( p > 2 \), the curve \( X_{ns}(p) \) does not contain any points defined over \( \mathbf{R} \). On the other hand, the curve \( X^+_{ns}(p) \) has real and usually also rational points. Indeed, for every imaginary quadratic order \( R \) with class number 1 there is a unique elliptic curve \( E \) over \( \mathbf{C} \) with complex multiplication by \( R \). The \( j \)-invariant of \( E \) is in \( \mathbf{Q} \). Moreover, when \( p \) is prime in the ring \( R \), there is a unique rational point \((E, \phi)\) on \( X^+_{ns}(p) \). These points are called \textit{CM points} or \textit{Heegner points}. See \cite{10}, Section A.5.

**Remark 1.** Suppose that \((E, \phi)\) is a rational point of \( X^+_{ns}(p) \). Then \( E \) is defined over \( \mathbf{Q} \) and the image of \( \text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \) in \( \text{Aut}(E[p]) \) is isomorphic through \( \phi \) to a subgroup \( G \) of \( \text{GL}_2(\mathbf{F}_p) \) which is contained in the normalizer of a non-split Cartan subgroup \( U \). The points of \( X_{ns}(p) \) lying above \((E, \phi)\) are defined over the fixed field of \( U \cap G \), which is an imaginary quadratic extension of \( \mathbf{Q} \). In the case of Heegner points, CM theory implies that this extension is isomorphic to the quotient field of the endomorphism ring of \( E \).

Now we turn to the case \( p = 11 \). In \cite{3}, Proposition 4.3.8.1, Ligozat derived a Weierstrass equation for the genus 1 curve \( X^+_{ns}(11) \). It is given by

\[
Y^2 + Y = X^3 - X^2 - 7X + 10.
\]

By choosing the point at infinity as origin, we can view \( X^+_{ns}(11) \) as an elliptic curve and equip it with the usual group law. The rational points of \( X^+_{ns}(11) \) are then an infinite cyclic group generated by the point \( P = (4, -6) \). See \cite{3}. The translations by the rational points form an infinite group of automorphisms of \( X^+_{ns}(11) \). They are all defined over \( \mathbf{Q} \). It follows that there are infinitely many isomorphisms over \( \mathbf{Q} \) between \( X^+_{ns}(11) \) and the curve given by Ligozat. For a particular choice of such an isomorphism, Halberstadt derived in \cite{6}, Section 2.2, an explicit formula for the degree 55 morphism \( j : X^+_{ns}(11) \rightarrow X(1) \). In view of the symmetry phenomenon described at the end of this section, it is convenient to compose his isomorphism with the translation-by-\( P \) morphism. Explicitly, our function \( j(X, Y) \) is the value of Halberstadt’s \( j \)-function in the point

\[
\left( \frac{4X^2 + X - 2 + 11Y}{(X - 4)^2}, \frac{2X^2 + 17X - 34 + 11Y)(1 - 3X)}{(X - 4)^3} \right),
\]

that is,

\[
j(X, Y) = (X + 2)(4 - X)^5 (11(X^2 + 3X - 6)(Y - 5)(X^3 + 4X^2 + X + 22 + (1 - 3X)Y))^3 \\
\times \left( \frac{(3X^2 - 3X - 14 - (3 + 2X)Y)(12X^3 + 28X^2 - 41X - 62 + (3X^2 + 20X + 37)Y)^3}{( - 7X^2 - 15X + 62 + (X + 18)Y)^2(4X^3 + 2X^2 - 21X - 6 + (X^2 + 3X + 5)Y)} \right)^{11}.
\]
Proposition 1. The modular curve $X_{ns}(11)$ is given by the equations
\[
Y^2 + Y = X^3 - X^2 - 7X + 10, \\
T^2 = -(4X^3 + 7X^2 - 6X + 19).
\]

Proof. We first compute the ramification locus of the morphism $\pi : X_{ns}(11) \to X_{ns}^+(11)$. Since $\pi$ is defined over $\mathbb{Q}$, this locus is stable by the action of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. By Proposition 7.10 in [1], the function $j(X,Y)-1728$ has exactly seven simple zeroes on $X_{ns}^+(11)$, and six of them are the ramification points of $\pi$. All the other zeroes are double. Let us consider the quotient map $X_{ns}^+(11) \to \mathbb{P}^1$ induced by the elliptic involution. It corresponds to the quadratic function field extension $\mathbb{Q}(X) \subset \mathbb{Q}(X,Y)$ with non-trivial automorphism given by $Y \mapsto -1 - Y$. One easily checks that the trace and norm of the function $j(X,Y)-1728$ admit the polynomial $4X^3+7X^2-6X+19$ as an irreducible factor of multiplicity 1 and 2 respectively. The function $F$ on $X_{ns}^+(11)$ defined by this cubic polynomial has exactly six simple zeroes. It follows that the zeroes of $F$ are simple zeroes of $j(X,Y)-1728$. Therefore they are the ramification points of $\pi$.

The function field $\mathbb{Q}(X_{ns}(11))$ is obtained by adjoining a function $G$ to $\mathbb{Q}(X_{ns}^+(11))$ whose square is in $\mathbb{Q}(X_{ns}^+(11))$. The coefficients of the divisor on $X_{ns}^+(11)$ of $G^2$ are odd at the ramified points and even at the others. Since the same holds for the above function $F$, the divisor of $FG^2$ is of the form $2D$ for some divisor $D$ of $X_{ns}^+(11)$ defined over $\mathbb{Q}$. The group $\text{Pic}^0(X_{ns}^+(11))$ is naturally isomorphic to the group of rational points of $X_{ns}^+(11)$. Since the latter is isomorphic to $\mathbb{Z}$, there are no elements of order 2 in $\text{Pic}^0(X_{ns}^+(11))$. It follows that $D$ is principal. This means that there is a function $T$ in $\mathbb{Q}(X_{ns}(11))$ and a non-zero $\lambda \in \mathbb{Q}$ for which $\lambda T^2 = F$. The function field of $X_{ns}(11)$ is then equal to $\mathbb{Q}(X,Y,T)$.

It remains to determine $\lambda$, which is unique up to squares. Consider the point $Q = (5/4,7/8)$ of $X_{ns}^+(11)$. Since $j(Q) = 1728$, the elliptic curve parametrized by the point $Q$ admits complex multiplication by the ring $\mathbb{Z}[i]$ of Gaussian integers. By Remark [1] the two points of $X_{ns}(11)$ lying above $Q$ are defined over $\mathbb{Q}(i)$. Since $F(Q) = 121/4$ is a square, we may take $\lambda = -1$. This proves the proposition.

Corollary 1. In addition to the modular involution $w$, the curve $X_{ns}(11)$ admits an “exotic” involution $q$. The modular involution switches $(X,Y,T)$ and $(X,Y,-T)$, while $q$ switches $(X,Y,T)$ and $(X,-1-Y,T)$. Together, $w$ and $q$ generate a subgroup of $\text{Aut}(X_{ns}(11))$ isomorphic to Klein’s four group.

Although it is not relevant for the proofs in this paper, let us explain how the “exotic” automorphisms of $X_{ns}(11)$ were first detected. The rational points of $X_{ns}^+(11)$ form an infinite cyclic group generated by the point $P = (4,-6)$. For each $n \in \mathbb{Z}$, the elliptic curve over $\mathbb{Q}$ parametrized by the point $[n]P$ in $X_{ns}^+(11)(\mathbb{Q})$ has the following property: the image $G$ of the Galois representation attached to its $p$-torsion points is contained in the normalizer of a non-split Cartan subgroup $U$. By Remark [1] the fixed field of $U \cap G$ is an imaginary quadratic field. In his tesi di laurea, one of the authors —Valerio Dose— used the methods of [1] to compute this quadratic field $K$ for several values of $n$. The first few values are given in the table below. There is a striking symmetry: the quadratic fields attached to the points $[n]P$ and $[-n]P$ are always the same. There does not seem to be a “modular reason” for this, as it may happen that the elliptic curve associated to $[n]P$ has complex multiplication by some quadratic order of discriminant $\Delta < 0$ but the elliptic curve associated to $[-n]P$ has not. In the first case $K$ is the CM field, but in the second case it is not. The phenomenon, which surprised us at first, is explained by the existence of the “exotic” involution $q$. 

3
2 Differentials

In this section we analyze the space of regular differentials $\Omega^1_{X_{ns}(11)}$ of the curve $X_{ns}(11)$.

By [2], Section 8, the Jacobian $J_{ns}(11)$ of $X_{ns}(11)$ is isogenous over $\mathbb{Q}$ to the new part of the Jacobian of $X_0(121)$. See [4] for an easy proof of this result. By Cremona’s Tables [3], there are exactly four $\mathbb{Q}$–isogeny classes of elliptic curves of conductor 121, which are represented by

| points | $j$ | CM | $K$ |
|--------|-----|----|-----|
| [6]P   | $2^{3}3^{3}5^{3}11^{3}17^{6}29^{3}53^{3}191^{3}/769^{11}$ | – | $\mathbb{Q}(-3\cdot14327)$ |
| [5]P   | $-2^{1}3^{3}5^{3}23^{2}29^{3}$ | $\Delta = -163$ | $\mathbb{Q}(-163)$ |
| [4]P   | 0 | $\Delta = -3$ | $\mathbb{Q}(-3)$ |
| [3]P   | $2^{6}3^{3}$ | $\Delta = -4$ | $\mathbb{Q}(-1)$ |
| [2]P   | $-2^{1}5^{3}3^{5}11^{3}$ | $\Delta = -67$ | $\mathbb{Q}(-67)$ |
| $P$    | $2^{4}3^{3}5^{3}$ | $\Delta = -12$ | $\mathbb{Q}(-3)$ |
| $\infty$ | $2^{3}3^{3}11^{3}$ | $\Delta = -16$ | $\mathbb{Q}(-3)$ |
| [−1]P  | $-2^{1}5^{3}3^{5}1^{3}$ | $\Delta = -27$ | $\mathbb{Q}(-3)$ |
| [−2]P  | $2^{8}3^{5}5^{6}11^{3}53^{3}/23^{11}$ | – | $\mathbb{Q}(-67)$ |
| [−3]P  | $-2^{9}3^{3}5^{3}13^{1}7^{1}3^{1}181^{3}/43^{11}$ | – | $\mathbb{Q}(-3)$ |
| [−4]P  | $2^{18}3^{3}5^{7}11^{3}23^{3}29^{3}103^{3}/67^{11}$ | – | $\mathbb{Q}(-3)$ |
| [−5]P  | $-2^{4}3^{3}5^{1}17^{6}29^{3}367^{3}2381^{3}/397^{11}$ | – | $\mathbb{Q}(-163)$ |
| [−6]P  | $-2^{3}3^{1}11^{3}17^{6}19^{3}23^{3}41^{3}53^{3}167^{3}277^{3}23431^{3}/80233^{11}$ | – | $\mathbb{Q}(-3\cdot14327)$ |

It follows that $J_{ns}(11)$ is isogenous over $\mathbb{Q}$ to the product of these four elliptic curves. The following proposition describes a low degree morphism from the curve $X_{ns}(11)$ to each of its elliptic quotients, and provides a basis for $\Omega^1_{X_{ns}(11)}$ from the respective pull-backs. We make use of the equations for $X_{ns}(11)$ given in Proposition 1. It is also convenient to introduce the function $Z = (2Y + 1)/T$ in $\mathbb{Q}(X_{ns}(11))$.

**Proposition 2.** The curve $X_{ns}(11)$ admits morphisms defined over $\mathbb{Q}$ of degree 6, 2, 2 and 6 to the elliptic curves $A$, $B$, $C$ and $D$ respectively. Moreover, the corresponding pull-backs of the 1-dimensional $\mathbb{Q}$-vector spaces of regular differentials are the 1-dimensional subspaces of $\Omega^1_{X_{ns}(11)}$ generated by

$$
\omega_A = \frac{dX}{Z}, \quad \omega_B = \frac{dX}{2Y+1}, \quad \omega_C = \frac{dX}{T} \quad \text{and} \quad \omega_D = \frac{(3X-1)dX}{Z}
$$

respectively.
Proof. By Corollary 1, the function field extension $Q(X) \subset Q(X, Y, T)$ is Galois, with Galois group isomorphic to Klein’s four group. Since the elliptic curve given by the Weierstrass equation $T^2 = -(4X^3 + 7X^2 - 6X + 19)$ is isomorphic to $C$, we have the following commutative diagram of degree 2 morphisms

$$
\begin{array}{c}
X_{ns}(11) \\
\downarrow \phi_H \\
B \\
\uparrow \phi_B \\
C \\
\downarrow \phi_C \\
H \\
\downarrow P^1
\end{array}
$$

Here $H$ is the genus 2 curve given by

$$Z^2 = -(4X^3 - 4X^2 - 28X + 41)(4X^3 + 7X^2 - 6X + 19),$$

and the morphisms $\phi_B$, $\phi_H$ and $\phi_C$ are defined as follows:

$$\phi_B(X, Y, T) = (X, Y), \quad \phi_H(X, Y, T) = (X, (2Y + 1)T), \quad \phi_C(X, Y, T) = (X, T).$$

In particular, we can take $\omega_B$ and $\omega_C$ as in the statement.

We now describe degree 6 morphisms from $X_{ns}(11)$ to the curves $A$ and $D$ factoring through $\phi_H$. To see that $H$ admits degree 3 morphisms to $A$ and $D$, we use Goursat’s formulas as described in the appendix of [7]. Substituting $X = x + \frac{1}{3}$ and $Z = \frac{44}{3}z$ in the hyperelliptic equation of $H$, we obtain

$$tz^2 = (x^3 + 3ax + 2b)(2dx^3 + 3cx^2 + 1)$$

with

$$a = -\frac{22}{9}, \quad b = \frac{847}{216}, \quad c = \frac{27}{242}, \quad d = \frac{9}{44} \quad \text{and} \quad t = -3.$$

Note that the discriminants $\Delta_1 = a^3 + b^2$ and $\Delta_2 = c^3 + d^2$ are both non-zero. Then, the maps $(x, z) \mapsto (u, v)$, with

$$(u, v) = \left(12 \Delta_1 \frac{-2dx + c}{x^3 + 3ax + 2b}, \frac{16dx^3 - 12cx^2 - 1}{(x^3 + 3ax + 2b)^2} \right),$$

$$(u, v) = \left(12 \Delta_2 \frac{x^2(ax - 2b)}{2dx^3 + 3cx^2 + 1}, \frac{x^3 + 12ax - 16b}{(2dx^3 + 3cx^2 + 1)^2}) \right),$$

are degree 3 morphisms from $H$ to the genus 1 curves given by the equations

$$tv^2 = u^3 + 12(2a^2d - bc)u^2 + 12 \Delta_1 (16ad^2 + 3c^2)u + 512 \Delta_1^2 d^3,$$

$$tv^2 = u^3 + 12(2bc^2 - ad)u^2 + 12 \Delta_2 (16b^2c + 3a^2)u + 512 \Delta_2^2 b^3$$

respectively. Moreover, the pull-back of the differential $du/v$ of the first curve to $\Omega^1_H$ is a rational multiple of $dx/z$ and hence of $dX/Z$, while the pull-back of the differential $du/v$ of the second curve is a rational multiple of $x dx/z$ and hence of $(3X - 1)dX/Z$.

Finally, for the above values of $a$, $b$, $c$, $d$ and $t$, the two genus 1 curves can be checked to be isomorphic over $Q$ to the elliptic curves $A$ and $D$ respectively. This proves the proposition.
Remark 2. Since the Jacobian of $H$ is isogenous to $A \times D$, we know that there do exist non-constant morphisms from $H$ to the curves $A$ and $D$, but we know of no a priori reason why there should exist morphisms of degree 3. In fact, this was only established by a numerical computation involving the period lattices of the curves $H$, $A$ and $D$. Another reason for suspecting that there exist such morphisms is the fact that the Fourier coefficients of the weight 2 eigenforms associated to the elliptic curves $A$ and $D$ are congruent modulo 3.

3 Automorphisms

In this section we prove the theorem. We use the notations of Proposition 1 and Proposition 2.

Let $\sigma$ be an automorphism of the curve $X_{ns}(11)$. Then $\sigma$ induces an automorphism of the Jacobian $J_{ns}(11)$. We recall that this Jacobian is isogenous over $\mathbb{Q}$ to the product of the elliptic curves $A$, $B$, $C$ and $D$ introduced in section 2.

Let us analyze the isogeny relations over $\mathbb{Q}$ among these four elliptic curves. The curve $D$ cannot be isogenous over $\mathbb{Q}$ to $A$, $B$ or $C$ because it is the only one whose $j$-invariant is not integral. The curve $B$ has complex multiplication by the quadratic order of discriminant $-11$, so it cannot be isogenous over $\mathbb{Q}$ to $A$, $C$ or $D$ because none of these three curves admits complex multiplication. Lastly, there is a degree 2 isogeny between $A$ and $C$ defined over $\mathbb{Q}(\sqrt{-11})$.

Therefore, all endomorphisms of $J_{ns}(11)$ are defined over $\mathbb{Q}(\sqrt{-11})$. Furthermore, the action of $\sigma$ on $\Omega^1_{X_{ns}(11)}$ with respect to the basis $\omega_B$, $\omega_D$, $\omega_A$, $\omega_C$ is given by multiplication by a matrix of the form

$$
\begin{pmatrix}
\pm 1 & 0 & 0 & 0 \\
0 & \pm 1 & 0 & 0 \\
0 & 0 & a & b \\
0 & 0 & c & d
\end{pmatrix}
$$

(3.1)

for certain $a, b, c, d \in \mathbb{Q}(\sqrt{-11})$. Note that the eigenvalues corresponding to $\omega_B$ and $\omega_D$ must be roots of unity in this quadratic field, namely $\pm 1$, because $\sigma$ has finite order.

Let us now consider the functions $x = \omega_D/\omega_A = 3X - 1$ and $y = \omega_C/\omega_A = 2Y + 1$ on the elliptic curve $B$. They satisfy the equation

$$
\frac{1}{4} y^2 = \frac{1}{27} x^3 - \frac{22}{9} x + \frac{847}{108}.
$$

Then the action of $\sigma$ on $\Omega^1_{X_{ns}(11)}$ yields

$$
\sigma(x) = \frac{\pm x}{a + cy} \quad \text{and} \quad \sigma(y) = \frac{b + dy}{a + cy}.
$$

In other words, $\sigma$ induces an automorphism of the curve $B$ which, in projective coordinates, is given by

$$
(x : y : z) \mapsto (\pm x : bz + dy : az + cy).
$$

In particular, $\sigma$ maps the origin $(0 : 1 : 0)$ of the elliptic curve $B$ to the point $(0 : d : c)$. This implies $c = 0$. Otherwise, the above equation would entail the relation $(d/c)^2 = 847/27$ with $d/c \in \mathbb{Q}(\sqrt{-11})$, which is impossible. Since the only automorphisms of $B$ fixing the origin are the identity and the elliptic involution, it follows $\sigma(x) = x$ and $\sigma(y) = \pm y$. Thus, $\sigma(X) = X$ whereas $\sigma(Y)$ must be either $Y$ or $1 - Y$. The equations given for $X_{ns}(11)$ in Proposition 1 imply then $\sigma(T) = \pm T$. This proves the theorem.
References

[1] Baran, B.: Normalizers of non-split Cartan subgroups, modular curves, and the class number one problem, J. of Number Theory 130 (2010), 2753–2772.

[2] Chen, I.: The jacobians of non-split Cartan modular curves, Proc. London Math. Soc. 77 (1998), 1–38.

[3] Cremona, J.: Algorithms for modular elliptic curves, Cambridge University Press, Cambridge 1997.

[4] De Smit, B. and Edixhoven, B.: Sur un résultat d’Imin Chen, Mathematical Research Letters 7 (2000), 147–154.

[5] Dose, V.: Serre’s theorem on Galois representations attached to elliptic curves, Tesi di Laurea Specialistica in Matematica, Università degli Studi di Roma Tor Vergata, Roma 2010.

[6] Halberstadt, E.: Sur la courbe modulaire $X_{\text{ndep}}(11)$, Experiment. Math. 7 (1998), 163–174.

[7] Bröker, R., Howe, E., Lauter, K. and Stevenhagen, P.: Genus-2 curves and Jacobians with a given number of points, in preparation.

[8] Ligozat, G.: Courbes modulaires de niveau 11, 149–237 in: Modular functions of one variable, V (Proc. Second Internat. Conf. Univ. Bonn, Bonn, 1976), Lecture Notes in Math. 601, Springer-Verlag, Berlin 1977.

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

[10] Serre, J.-P.: Lectures on the Mordell-Weil Theorem, Aspects Math. E15, Springer Vieweg, Braunschweig/Wiesbaden 1989.

Valerio Dose
dose@mat.uniroma2.it
René Schoof
schoof@mat.uniroma2.it
Dipartimento di Matematica
Università degli Studi di Roma Tor Vergata
Via della Ricerca Scientifica 1
00133 Roma, Italy

Josep González
josepg@ma4.upc.edu
Julio Fernández
julio@ma4.upc.edu
Departament de Matemàtica Aplicada 4
Universitat Politècnica de Catalunya
EPSEVG, Avinguda Víctor Balaguer 1
08800 Vilanova i la Geltrú, Spain