

ON THE MODULAR CURVES $Y_E(7)$

EMMANUEL HALBERSTADT AND ALAIN KRAUS

ABSTRACT. Let E denote an elliptic curve over \mathbf{Q} and $Y_E(7)$ the modular curve classifying the elliptic curves E' over \mathbf{Q} such that the representations of $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ in the 7-torsion points of E and of E' are symplectically isomorphic. In case E is given by a Weierstraß equation such that the c_4 invariant is a square, we exhibit here nontrivial points of $Y_E(7)(\mathbf{Q})$. From this we deduce an infinite family of curves E for which $Y_E(7)(\mathbf{Q})$ has at least four nontrivial points.

INTRODUCTION

If K is a field of characteristic 0 and E is an elliptic curve over K , we denote by $E[7]$ the K -group scheme kernel of the multiplication-by-7 map on E . The Weil pairing on $E[7]$ is a nondegenerate alternating bilinear form, taking its values in μ_7 , the K -group scheme of 7th roots of unity. Moreover, let \overline{K} be an algebraic closure of K . The natural representation of $\text{Gal}(\overline{K}/K)$ in $E[7]$ will be called simply the representation associated to E (whenever it is clear what K and \overline{K} are). Suppose now that E is a given elliptic curve over \mathbf{Q} . It is known (cf. [4]) that there is a smooth affine algebraic curve $Y_E(7)$, defined over \mathbf{Q} and absolutely irreducible, which has the following property. For every field K of characteristic 0, the points of $Y_E(K)$ correspond, by a canonical bijection, to the isomorphism classes of pairs (E', Ψ') , where E' is an elliptic curve over K and Ψ' is a symplectic isomorphism of K -group schemes from $E[7]$ onto $E'[7]$. Two such pairs (E', Ψ') and (E'', Ψ'') are isomorphic if there is an isomorphism u of E' onto E'' defined over K and such that $\Psi'' = u \circ \Psi'$. Denote by $X_E(7)$ the smooth compactification of $Y_E(7)$. From now on, Y_E (resp. X_E) will stand for $Y_E(7)$ (resp. $X_E(7)$). The curve X_E is a Galois twist of the modular curve $X(7)$ which is, as one knows, isomorphic (over \mathbf{Q}) to the Klein quartic. In particular, X_E has genus 3, and so, over every number field, the number of its rational points is finite by Falting's theorem. The curve Y_E always has trivial points rational over \mathbf{Q} . We say that a point of $Y_E(\mathbf{Q})$ is trivial if it corresponds to a pair (E', Ψ') , as above, where E' is an elliptic curve over \mathbf{Q} isogenous over \mathbf{Q} to E . The problem of the existence, on the curves Y_E , of *nontrivial* points rational over \mathbf{Q} has been raised by B. Mazur (cf. [7], p. 133). The first examples of such points have been given in [4].

Given an equation for E , it is not easy to get explicit equations for Y_E (if the prime number 7 is replaced by 3 or 5, the corresponding explicit calculations have been done in [8], but the curves $Y_E(3)$ and $Y_E(5)$ have genus 0). As an example,

Received by the editor August 8, 1997 and, in revised form, July 24, 1998.
1991 *Mathematics Subject Classification*. Primary 11Gxx.

let E be the elliptic curve given by

$$(1) \quad y^2 + y = x^3 - x^2.$$

This elliptic curve has conductor 11, it is the curve 11A3 in the tables of [2]. As we know, E is isomorphic (over \mathbf{Q}) to the modular curve $X_1(11)$. The associated curve Y_E has a nontrivial point rational over \mathbf{Q} (we will explain later how we found this point), corresponding to the elliptic curve E' given by

$$(2) \quad y^2 + y = x^3 - x^2 - 8\,526\,286x + 140\,410\,525\,642.$$

E' has conductor $20\,185 = 5 \times 11 \times 367$. The representations associated to the curves E, E' are symplectically isomorphic, but E and E' are not isogenous (over $\overline{\mathbf{Q}}$).

The c_4 invariant associated to equation (1) is 16. More generally, let E be an elliptic curve over a field of characteristic 0, with modular invariant $j = j(E)$ different from 0 and 1728. As the equality

$$j(j - 1728) = \frac{c_4^3 c_6^2}{\Delta^2}$$

shows, E has a Weierstraß model for which the c_4 invariant is a square if and only if $j(j - 1728)$ is a square. Among other things, we prove in this work that if E is defined over \mathbf{Q} and satisfies the above condition, and if one excludes a finite number of values for $j(E)$, then the associated curve Y_E has at least two (explicit) nontrivial points rational over \mathbf{Q} (cf. Corollary 1). Therefore, if E is an *arbitrary* elliptic curve over \mathbf{Q} , the curve Y_E has at least nontrivial points rational over a suitable quadratic field: just adjoin to \mathbf{Q} a square root of $j(E)(j(E) - 1728)$; here again, there are a finite number of exceptional values for $j(E)$. In order to prove Corollary 1 we will exhibit, over the field $\mathbf{Q}(T)$, three elliptic curves E, E', E'' whose associated representations are symplectically isomorphic, these representations being onto and the curves E, E', E'' being pairwise nonisogenous (cf. Theorem 1). The elliptic curve E has the following property: if $j = j(E)$ is its modular invariant, then $j(j - 1728)$ is a square in $\mathbf{Q}(T)$, and E is, in a sense, universal for this property. Finally, Theorem 2 gives an infinite family of elliptic curves A over \mathbf{Q} for which the curve Y_A has at least four nontrivial points rational over \mathbf{Q} (see the details in §5).

1. THE ELLIPTIC CURVES E, E', E''

Let T be an indeterminate. Denote by E, E', E'' the elliptic curves over $\mathbf{Q}(T)$ given respectively by equations (3), (4), (5) below; these equations are minimal over $\mathbf{Q}[T]$:

$$(3) \quad y^2 = x^3 + 7x^2 + 28T,$$

$$(4) \quad y^2 = x^3 + x^2 + a_4(E')x + a_6(E'),$$

$$(5) \quad y^2 = x^3 + x^2 + a_4(E'')x + a_6(E''),$$

the coefficients in (4) and (5) being

$$\begin{cases} a_4(E') = 7T^3 + 7T^2 - 19T - 16, \\ a_6(E') = -T^5 + 14T^4 + 63T^3 + 77T^2 + 38T + 20, \end{cases}$$

$$\begin{cases} a_4(E'') = -(45\,927T^3 + 204\,120T^2 + 162\,432T + 4\,181), \\ a_6(E'') = -(531\,441T^5 + 12\,262\,509T^4 + 39\,287\,997T^3 \\ \qquad \qquad \qquad + 43\,008\,840T^2 + 8\,670\,080T - 102\,675). \end{cases}$$

The corresponding standard invariants are:

$$\begin{cases} c_4(E) = 2^4 \times 7^2, \\ c_6(E) = -2^6 \times 7 \times (54T + 49), \\ \Delta(E) = -2^8 \times 7^2 \times T(27T + 49), \\ j(E) = \frac{-2^4 \times 7^4}{T(27T+49)}, \end{cases}$$

$$\begin{cases} c_4(E') = -2^4(21T^3 + 21T^2 - 57T - 49), \\ c_6(E') = 2^5(27T^5 - 378T^4 - 1638T^3 - 2016T^2 - 1197T - 686), \\ \Delta(E') = -2^4T^2(27T + 49)(T + 3)^7, \\ j(E') = \frac{2^8(21T^3+21T^2-57T-49)^3}{T^2(27T+49)(T+3)^7}, \end{cases}$$

$$\begin{cases} c_4(E'') = 2^4[137\,781T^3 + 612\,360T^2 + 487\,296T + 12\,544], \\ c_6(E'') = 2^5[14\,348\,907T^5 + 331\,087\,743T^4 + 1\,060\,362\,576T^3 \\ \qquad \qquad \qquad + 1\,159\,401\,600T^2 + 232\,630\,272T - 2\,809\,856], \\ \Delta(E'') = -2^4T(27T + 49)^2(27T - 32)^7, \\ j(E'') = \frac{-2^8(137\,781T^3+612\,360T^2+487\,296T+12\,544)^3}{T(27T+49)^2(27T-32)^7}. \end{cases}$$

Let K be an extension of \mathbf{Q} and t an element of K . Whenever we have

$$(6) \qquad t \neq 0, -3, \frac{-49}{27}, \frac{32}{27},$$

we denote by E_t, E'_t, E''_t the elliptic curves over K obtained from E, E', E'' respectively, by specializing T to t .

2. STATEMENT OF THE RESULTS

Denote by Ω an algebraic closure of $\mathbf{Q}(T)$ and by $\overline{\mathbf{Q}}$ the algebraic closure of \mathbf{Q} in Ω . Here is the essential result of this work.

Theorem 1. *Consider the elliptic curves E, E', E'' over $\mathbf{Q}(T)$ given by equations (3), (4) and (5), respectively. Then:*

- (a) *the representations of $\text{Gal}(\Omega/\mathbf{Q}(T))$ on the 7-torsion points of the elliptic curves E, E', E'' are onto;*
- (b) *these three representations are pairwise symplectically isomorphic;*
- (c) *the elliptic curves E, E', E'' are pairwise nonisogenous over Ω .*

By specializing, we will obtain the corollary below, which exhibits a class of elliptic curves A over \mathbf{Q} for which $Y_A(\mathbf{Q})$ has at least two nontrivial points.

Corollary 1. *There is a finite subset S of \mathbf{Q} , containing 0 and 1728 and having the following property: for every elliptic curve A over \mathbf{Q} whose modular invariant j does not belong to S , and which satisfies the condition*

$$(*) \qquad j(j - 1728) \text{ is a square in } \mathbf{Q},$$

$Y_A(\mathbf{Q})$ has at least two nontrivial points.

We do not have such a subset S explicitly. On the other hand, the following explicit result makes Corollary 1 more precise, as we shall see. An analogous result has been obtained already in [5], but the corresponding representations were not onto.

Corollary 2. *Let u be a nonzero integer divisible by 6. Set*

$$(7) \quad t = \frac{49}{54}(u - 1),$$

and consider the elliptic curves E_t, E'_t, E''_t . Then:

- (a) *the representations associated to the elliptic curves E_t, E'_t, E''_t , respectively, are onto;*
- (b) *these three representations are pairwise symplectically isomorphic;*
- (c) *the elliptic curves E_t, E'_t, E''_t are pairwise nonisogeneous over $\overline{\mathbf{Q}}$.*

In this direction, there is an obvious question: What are the integers $m > 1$ for which there exist m elliptic curves over \mathbf{Q} , pairwise nonisogenous over \mathbf{Q} , such that the m associated representations are symplectically isomorphic? Let k be the least upper bound for the set of such integers m . What can be said about k ? In particular is it finite? Obviously the answer is yes if the Uniform Conjecture (cf. [1]) is taken for granted. A variant of this question is to find the least upper bound k' for the set of integers $m > 1$ for which there exist an *infinity* of m -tuples of elliptic curves over \mathbf{Q} , pairwise nonisogenous over \mathbf{Q} , such that the m associated representations are symplectically isomorphic. The following theorem shows that $k' \geq 5$.

Theorem 2. *There is an infinite family (explicitly given in §5) of quintuples $(\mathcal{E}_1, \mathcal{E}_2, \mathcal{E}_3, \mathcal{E}_4, \mathcal{E}_5)$ of elliptic curves over \mathbf{Q} with the following properties:*

- (a) *for $i = 1, \dots, 5$, the representation associated to the elliptic curve \mathcal{E}_i is onto;*
- (b) *the representations in (a) are pairwise symplectically isomorphic;*
- (c) *the elliptic curves \mathcal{E}_i ($i = 1, \dots, 5$) are pairwise nonisogenous over $\overline{\mathbf{Q}}$.*

The above family of quintuples is parametrized by (almost all) the rational points of a certain elliptic curve \mathcal{F} over \mathbf{Q} ; the group $\mathcal{F}(\mathbf{Q})$ has rank 2.

3. PROOF OF THEOREM 1

3.1. Some preliminaries. To begin with, consider a field K of characteristic 0, an algebraic closure \overline{K} of K and a continuous quadratic character χ of $\text{Gal}(\overline{K}/K)$. Then denote by A an elliptic curve over K , by A' the twist of A by χ , and by ρ and ρ' the representations associated to A and A' , respectively. Since ρ' is symplectically isomorphic to $\chi \otimes \rho$, one easily sees that ρ' is onto if and only if ρ is onto. Similarly, let A_1 be another elliptic curve over K , let A'_1 be the twist of A_1 by χ , and let ρ_1 and ρ'_1 be the corresponding representations. The representations ρ and ρ_1 are symplectically isomorphic if and only if the representations ρ' and ρ'_1 are.

The following lemmas will be useful in the various proofs.

Lemma 1. *Denote by A and A' two elliptic curves over K . Suppose A is without complex multiplication. If A and A' are isogenous over \overline{K} , then A' is isogenous over K either to A or to a quadratic twist of A .*

Lemma 2. *Let A be an elliptic curve over $\mathbf{Q}(T)$, given by a Weierstraß equation*

$$y^2 + a_1(T)xy + a_3(T)y = x^3 + a_2(T)x^2 + a_4(T)x + a_6(T),$$

and let $\Delta(T)$ be the corresponding discriminant. Then:

(a) *Let t be a rational number. Suppose that $\Delta(t)$ is nonzero and that t is not a pole of a_1, a_2, a_3, a_4 or a_6 . Let A_t be the elliptic curve over \mathbf{Q} obtained from A by specializing T to t . If the representation associated to A_t is onto, so is the representation to A .*

(b) *Let A' be another elliptic curve over $\mathbf{Q}(T)$, given by a Weierstraß equation as above. Suppose that the representations associated to A and A' are symplectically isomorphic. Let t be a rational number. With obvious notation, suppose that $\Delta(t)\Delta'(t)$ is nonzero and that t is not a pole of a_i or a'_i , for $i = 1, 2, 3, 4, 6$. Then the representations associated to A_t and A'_t are symplectically isomorphic.*

Lemma 3. *Denote by A_1 and A_2 two elliptic curves over a number field K . Suppose that A_1 and A_2 are not isogenous over $\overline{\mathbf{Q}}$. Let Z be a smooth projective algebraic curve, defined over K and absolutely irreducible. For $i = 1, 2$, let f_i be a nonconstant morphism from A_i to Z defined over K . Under these assumptions, the pairs $(P_1, P_2) \in A_1(K) \times A_2(K)$ such that $f_1(P_1) = f_2(P_2)$ form a finite set.*

Let us sketch the proofs of these lemmata. For Lemma 1, let f be an isogeny of degree n from A to A' , and f^0 the dual isogeny. For each element s of $\text{Gal}(\overline{K}/K)$, denote by ${}^s f$ the transform of f by s . Since A is without complex multiplication, one has $f^0 \circ {}^s f = \pm[n]$, and so ${}^s f = \pm f$. The conclusion of Lemma 1 follows immediately. Lemma 2 comes essentially from [9], Lemma 2, p. 495. As for Lemma 3, one shows first that each irreducible component S (over $\overline{\mathbf{Q}}$) of the fibered product $A_1 \times_Z A_2$ is a projective curve because Z is smooth, and so the projections from S to A_1 and A_2 are onto (the precise argument is due to M. Lazarus). Therefore S has genus ≥ 2 , because of the assumptions made. The conclusion follows from Faltings' theorem.

3.2. The elliptic curves W, W', W'' . First, let A be an elliptic curve over a field K of characteristic 0. Suppose that the modular invariant j of A is different from 0 and 1728. Then $j(j - 1728)$ is a square in K if and only if, A being replaced by one of its quadratic twists if necessary, A has a model for which $c_4 = 12^2$. Given such a model, set

$$(8) \quad u = \frac{-c_6}{1728}.$$

We have $u \neq 1, -1$. Therefore A has the following model:

$$(9) \quad y^2 = x^3 - 3x + 2u.$$

More generally, if $u \neq 1, -1$, denote by W_u the plane projective cubic given by equation (9). The corresponding standard invariants are

$$\begin{cases} c_4(W_u) = 12^2, \\ c_6(W_u) = -12^3 u, \\ \Delta(W_u) = 1728(1 - u^2), \\ j(W_u) = \frac{1728}{1 - u^2}. \end{cases}$$

The considerations above show that if A is an elliptic curve over K whose modular invariant j is different from 0 and 1728, and if $j(j - 1728)$ is a square in K , then

there is an element u of K such that A is isomorphic over K either to W_u or to a quadratic twist of W_u . Now let U be defined by the relation

$$(10) \quad T = \frac{49}{54}(U - 1).$$

The elliptic curve W_U over $\mathbf{Q}(T) = \mathbf{Q}(U)$ will be denoted simply by W . Then W is isomorphic to the curve E (defined by equation (3)) twisted by $\sqrt{21}$. Let us now twist the elliptic curves E' and E'' (equations (4) and (5)) by $\sqrt{21}$ and denote by W' and W'' the elliptic curves over $\mathbf{Q}(T)$ thus obtained. The point in choosing the curves E', E'' rather than W', W'' is that the latter give more complicated invariants. On the other hand, note that W'' can be obtained from W' as follows:

- (i) one substitutes $-U$ for U in an equation for W' ;
- (ii) the elliptic curve thus obtained is twisted by $\sqrt{-1}$.

Note also that if operations (i) and (ii) are performed on W , the resulting curve is W itself. For instance, taking the remarks in 3.1 into account, if one wants to prove that the representation associated to E'' is onto, it will be enough to show that the representation associated to W' is onto. Denote now by K a field of characteristic 0 and by u an element of K . Define t in terms of u by equation (7). Let W'_u, W''_u be the curves deduced from W', W'' , respectively, by specializing U to u . These elliptic curves are twists of E'_t, E''_t , respectively, by $\sqrt{21}$. The elliptic curve W'_u (resp. W''_u) is defined as soon as u is different from 1, -1 and $\frac{-113}{49}$ (resp. $\frac{113}{49}$).

3.3. Proof of assertion (a) in Theorem 1. Let ρ, ρ', ρ'' be the representations associated to the elliptic curves E, E', E'' , respectively. Let us prove that ρ is onto. By Lemma 2, it is enough to find a rational number t satisfying (6) and such that the representation associated to E_t is onto. Take $t = 1$. An equation for the curve E_1 is

$$y^2 = x^3 + 7x^2 + 28.$$

It is the curve denoted by E in the theorem of [4], p. 266. By Lemma 3 in *loc. cit.*, the representation associated to E_1 is onto. Likewise, an equation for E'_1 is

$$y^2 = x^3 + x^2 - 21x + 211,$$

a minimal model being given by

$$y^2 = x^3 + x^2 - x + 3.$$

This is the curve denoted by E' in the theorem of [4], and the same argument shows that the representation associated to E'_1 is onto. Therefore the representations ρ' and ρ'' are onto, as noted above.

3.4. Proof of assertion (b) in Theorem 1. It is enough to show that ρ and ρ' are symplectically isomorphic. We follow (*mutatis mutandis*) the arguments used in the proof of the theorem in [4]. Consider the following polynomials over $\mathbf{Q}(T)$:

$$P = (X^2 + 5X + 1)^3(X^2 + 13X + 49) - j(E)X,$$

$$Q = (X^2 + 5X + 1)^3(X^2 + 13X + 49) - j(E')X.$$

They are irreducible over $\mathbf{Q}(T)$ (cf. Lemma 4 in *loc. cit.*). Let x (resp. y) be a root of P (resp. Q) in Ω . Let us prove that the fields $\mathbf{Q}(T)(x)$ and $\mathbf{Q}(T)(y)$ are conjugate over $\mathbf{Q}(T)$. This means that there is a polynomial

$$R = \beta_7 X^7 + \beta_6 X^6 + \dots + \beta_0 \in \mathbf{Q}(T)[X]$$

such that $R(x)$ is a root of Q ; i.e., it means that the following congruence is satisfied:

$$(11) \quad Q(R) \equiv 0 \pmod{P}.$$

With the help of the Pari software, one actually find rational fractions β_i , $i = 0, \dots, 7$, for which the congruence (11) is satisfied. For $i = 0, \dots, 7$, one has

$$\beta_i = \frac{\alpha_i}{2 \times 7^3(T + 3)(54T + 49)},$$

the α_i being given by:

$$\begin{cases} \alpha_0 = 49T(27T + 49)(69T - 7), \\ \alpha_1 = 2[478\,467T^3 + 1\,648\,710T^2 + 1\,336\,671T - 134\,456], \\ \alpha_2 = (27T + 49)(107\,871T^2 + 155\,799T - 686), \\ \alpha_3 = T(27T + 49)(80\,529T + 112\,259), \\ \alpha_4 = 69T(27T + 49)(391T + 539), \\ \alpha_5 = 3T(27T + 49)(1559T + 2149), \\ \alpha_6 = 2T(27T + 49)(207T + 287), \\ \alpha_7 = 3T(27T + 49)(5T + 7). \end{cases}$$

We will explain in §6 how these coefficients and the curves E, E', E'' were found.

Now apply Lemma 5 of [4], *mutatis mutandis*. Since the fields $\mathbf{Q}(T)(x)$ and $\mathbf{Q}(T)(y)$ are conjugate over $\mathbf{Q}(T)$, this lemma shows that there is a continuous character ε of $\text{Gal}(\Omega/\mathbf{Q}(T))$ into $\{1, -1\}$ such that ρ' is isomorphic to $\varepsilon \otimes \rho$. Let us show that ε is trivial. Suppose it is not, and let $L/\mathbf{Q}(T)$ be the corresponding quadratic extension; one has $L = \mathbf{Q}(T)(\sqrt{D})$, for some $D \in \mathbf{Q}(T)^*$. Looking at the places of bad reduction for E and E' , then applying the Néron-Ogg-Shafarevitch criterion, one can suppose that D is given by

$$D = dT^a(27T + 49)^b(T + 3)^c,$$

where a, b, c are 0 or 1 and d is a squarefree integer. The curve E' has multiplicative reduction at $T + 3$, and the exponent of $T + 3$ and its discriminant is divisible by 7. Therefore, by Tate's theory, ρ' is unramified at $T + 3$, so that $c = 0$. Let us specialize T to a rational number t satisfying (6). Let ρ_t, ρ'_t be the representations associated to E_t, E'_t , respectively. The representation ρ'_t is isomorphic to $\varepsilon_t \otimes \rho_t$, where, setting $D_t = D(t)$, ε_t is the character of $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ corresponding to the extension $\mathbf{Q}(\sqrt{D_t})/\mathbf{Q}$. Therefore, if p is a prime number not dividing D_t , and if E_t and E'_t have good reduction at p , one must have

$$a_p(E'_t) \equiv \left(\frac{D_t}{p}\right) a_p(E_t) \pmod{7},$$

the a_p being the coefficients of the Hasse-Weil L -functions of the elliptic curves considered. By choosing for t the values 1, 2 and 5, and by applying the above congruence with suitable primes p , one sees easily and successively that $b = 0$, then $a = 0$, and finally $d = 1$. Thus $D = 1$, a contradiction.

One still has to show that ρ and ρ' are symplectically isomorphic. Apply Proposition 2 of [4], replacing in it \mathbf{Q} by $\mathbf{Q}(T)$, the prime number p by 7, and the prime number ℓ by the place of $\mathbf{Q}(T)$ associated to T . At this place the curves E and E' have multiplicative reduction, and the exponents of T in $\Delta(E)$ and $\Delta(E')$ are 1 and 2, respectively. Since 2 is a square modulo 7, we have the desired conclusion.

3.5. **End of the proof.** Suppose that two of the curves E, E', E'' are isogenous over Ω , and denote them by A_1 and A_2 . Clearly A_1 and A_2 are not isogenous over $\mathbf{Q}(T)$, because their places of bad reduction are not the same. These curves have no complex multiplication, so Lemma 1 shows that A_2 is isogenous over $\mathbf{Q}(T)$ to a quadratic twist of A_1 . For $i = 1, 2$, let r_i be the representation associated to A_i . The representations r_1 and r_2 are isomorphic by assertion (b); therefore, this assertion shows that there is an automorphism θ of $A_1[7]$ and a quadratic character ε of $\text{Gal}(\Omega/\mathbf{Q}(T))$ such that, for every element s of $\text{Gal}(\Omega/\mathbf{Q}(T))$, one has

$$r_1(s)\theta = \varepsilon(s)\theta r_1(s).$$

Since r_1 is onto, one sees at once that ε is trivial, a contradiction. The proof of Theorem 1 is now complete.

Let us look again for a moment at the elliptic curves E and E' defined in the introduction by equations (1) and (2), respectively. The standard invariants of E are

$$c_4 = 16, \quad c_6 = -152, \quad j = \frac{-4096}{11}.$$

One checks that E is the twist of the curve W_u , corresponding to the parameter $u = \frac{19}{8}$, by $\sqrt{3}$; the corresponding value of t is $t = \frac{539}{432}$. So E is the twist of E_t by $\sqrt{7}$, and one sees that E' is the twist of E'_t by $\sqrt{7}$. Therefore, by Theorem 1 and Lemma 2, the representations associated to E and E' are symplectically isomorphic. The curves E and E' are not isogenous over $\overline{\mathbf{Q}}$: at 5 the curve E has good reduction and the curve E' has multiplicative reduction. On the other hand, if we denote here by E'' the twist of E''_t by $\sqrt{7}$, one sees that E'' is isogenous to E over \mathbf{Q} and that E'' is the curve denoted by 11A2 in the tables in [2].

4. PROOF OF THE COROLLARIES

4.1. **Proof of Corollary 1.** Let t be a rational number satisfying condition (6). From Theorem 1 and assertion (b) of Lemma 2, we know that the representations associated to E_t, E'_t and E''_t are symplectically isomorphic. Therefore, Corollary 1 will be proven if we show that the elliptic curves E_t, E'_t and E''_t are pairwise non-isogenous over $\overline{\mathbf{Q}}$, with a finite number of exceptions for t . To this end, consider, for every integer $n > 1$, the modular polynomial $\Phi_n \in \mathbf{Z}[X, Y]$. One knows (cf. [6], pp. 55 and 59) that, if k is an algebraically closed field of characteristic 0 and if A and A' are elliptic curves over k , there is an isogeny of degree n from A onto A' with cyclic kernel if and only if

$$\Phi_n(j(A), j(A')) = 0.$$

Now let A and A' be two elliptic curves over \mathbf{Q} . If these curves are isogenous over \mathbf{Q} , there is an isogeny λ from A onto A' , defined over \mathbf{Q} and having a cyclic kernel, say of order n . This kernel is a cyclic subgroup of order n of $A[n]$, defined over \mathbf{Q} . Therefore the modular curve $Y_0(n)$ has a point rational over \mathbf{Q} . Now the integers n for which $Y_0(n)(\mathbf{Q})$ is not empty constitute a finite set (cf. [11] and later results of Mestre and Kenku). Consider then the polynomial

$$\Phi = (X - Y) \prod_n \Phi_n.$$

In this product, n describes the finite set of integers just mentioned. If A and A' have no complex multiplication, Lemma 1 shows that A and A' are isogenous over

$\overline{\mathbf{Q}}$ if and only if $\Phi(j(A), j(A')) = 0$. Set

$$F = \Phi(j(E), j(E'))\Phi(j(E), j(E''))\Phi(j(E'), j(E'')).$$

This is a nonzero element of $\mathbf{Q}(T)$, since the elliptic curves E, E', E'' are pairwise nonisogenous over Ω (Theorem 1). Let t be a rational number satisfying condition (6) and such that

- 1) $F(t)$ is nonzero, and
- 2) the modular invariants $j(E_t), j(E'_t), j(E''_t)$ are not singular j -invariants.

For such a t , the elliptic curves E_t, E'_t and E''_t are clearly pairwise nonisogenous over $\overline{\mathbf{Q}}$. Corollary 1 follows, since conditions 1) and 2) leave out only a finite number of values for t .

4.2. The image of the representation associated to E_t . Let t, u be two rational numbers satisfying conditions (6) and (7). What can be said about the image of the representation ρ_t associated to E_t ? In this subsection we show that generally ρ_t is onto, and we study the exceptional cases. From [10] we know that if ρ_t is not onto, its image is contained either in the normalizer of a Cartan subgroup or in a Borel subgroup of $\text{GL}(E_t[7])$ (if A is an elliptic curve over \mathbf{Q} and ρ is the associated representation, the projection of $\text{Im}(\rho)$ in $\text{PGL}(A[7])$ cannot be isomorphic to $\mathfrak{A}_4, \mathfrak{A}_5$ or \mathfrak{S}_4). Let us look at these exceptional cases. Let $X_{\text{non-split}}(7)$ (resp. $X_{\text{split}}(7)$) be the modular curve which classifies the elliptic curves E whose associated representation has its image contained in the normalizer of a nonsplit (resp. split) Cartan subgroup of $\text{GL}(E[7])$.

There is an isomorphism between $X_{\text{non-split}}(7)$ and $\mathbf{P}^1(\mathbf{Q})$. If such an isomorphism is suitably chosen, the j -function on $X_{\text{non-split}}(7)$ gives on $\mathbf{P}^1(\mathbf{Q})$ the following rational function:

$$(12) \quad J_1(x) = \frac{\{(3x + 1)(x^2 + 10x + 4)(x^2 + 3x + 4)(4x^2 + 5x + 2)\}^3}{\{(x^3 + x^2 - 2x - 1)\}^7}.$$

The image of ρ_t is contained in the normalizer of a nonsplit Cartan subgroup of $\text{GL}(E_t[7])$ if and only if there is a rational number x such that $J_1(x) = j(E_t)$. For such an x , $J_1(x)(J_1(x) - 1728)$ must be a square. As a little calculation shows, this is the same as saying that there is a rational number y such that

$$y^2 = (3x + 1)(x^2 + 10x + 4)(x^2 + 3x + 4)(4x^2 + 5x + 2) \times (16x^4 + 68x^3 + 111x^2 + 62x + 11).$$

We have here an equation for a hyperelliptic curve having genus 5. Therefore the number of t for which the image of ρ_t is contained in the normalizer of a nonsplit Cartan subgroup of $\text{GL}(E_t[7])$ is finite because of Faltings' theorem.

The same argument works in the split case: just replace $X_{\text{non-split}}(7)$ by $X_{\text{split}}(7)$ and J_1 by

$$(13) \quad J_2(x) = \frac{(1 - x)\{(x - 2)(x^2 + 3x + 4)(x^2 + 3x - 3)(x^4 + x^3 - x^2 + 2x + 4)\}^3}{\{(x^3 + x^2 - 2x - 1)\}^7}.$$

We have here a hyperelliptic curve having genus 6, given by the equation

$$y^2 = (x - 1)(x - 2)(x^2 + 3x + 4)(x^2 + 3x - 3) \times (x^4 + x^3 - x^2 + 2x + 4)(x^4 + 6x^3 + 3x^2 - 18x - 19).$$

Again the number of t for which the image of ρ_t is contained in the normalizer of a split Cartan subgroup of $\text{GL}(E_t[7])$ is finite because of Faltings' theorem.

The case of Borel subgroups is different, as we show now. If an isomorphism of the modular curve $X_0(7)$ onto $\mathbf{P}^1(\mathbf{Q})$ is suitably chosen, the j -function on $X_0(7)$ gives on $\mathbf{P}^1(\mathbf{Q})$ the following rational function (cf. [4], Appendix I):

$$(14) \quad J_3(x) = \frac{(x^2 + 5x + 1)^3(x^2 + 13x + 49)}{x}.$$

Now take an $x \in \mathbf{Q}^*$ and set $j = J_3(x)$. Then $j(j - 1728)$ is a square if and only if there is a rational number y such that

$$(15) \quad y^2 = (x^2 + 5x + 1)(x^2 + 13x + 49).$$

If so, we have

$$(16) \quad \begin{cases} j = \frac{1728}{1 - u^2} & \text{by setting} \\ u = \frac{x^4 + 14x^3 + 63x^2 + 70x - 7}{y(x^2 + 5x + 1)}. \end{cases}$$

So let t, u be two rational numbers satisfying conditions (6) and (7). The image of ρ_t is contained in a Borel subgroup of $\text{GL}(E_t[7])$ if and only if there are two rational numbers x, y satisfying conditions (15) and (16), with $j = j(E_t)$. Consider then the plane quartic curve \mathcal{Q} which is the projective completion of the curve given by equation (15). The normalization of \mathcal{Q} is the elliptic curve \mathcal{C} given by

$$(17) \quad Y^2 + XY + Y = X^3 + 2X + 32.$$

Denote by π a birational morphism from \mathcal{C} onto \mathcal{Q} (defined over \mathbf{Q}). The elliptic curve \mathcal{C} is the curve 294G1 in the tables of [2]. The group $\mathcal{C}(\mathbf{Q})$ has rank 1; it is generated by the points $P_0 = (-3, 1)$ (of order 2) and $P = (1, -7)$ (of infinite order).

In conclusion, there is an infinity of pairs of rational numbers (t, u) satisfying (6) and (7) and such that the image of ρ_t is contained in a Borel subgroup of $\text{GL}(E_t[7])$. All these pairs are obtained as follows: start with a point $M = (X, Y)$ of $\mathcal{C}(\mathbf{Q})$, different from $0, 3P, 4P, 7P$, set $\pi(M) = (x, y)$, and then define u by (16) and t by (7).

4.3. Proof of Corollary 2. Assertion (b) of this corollary results from Theorem 1 and Lemma 2. Let t and u satisfy the hypotheses of Corollary 2. For assertion (a), it is enough to show that the representation r_u associated to W_u is onto. It is easily seen that $1 - u^2$ is not a 7th power. So let p be a prime factor of $1 - u^2$ such that 7 does not divide $v_p(1 - u^2)$. The hypotheses show that p is different from 2 and 3. Moreover, equation (9) is minimal, and W_u has at p multiplicative reduction. Since the exponent of p in $\Delta(W_u)$ is not divisible by 7, Tate's theory implies that 7 divides the order of the image of r_u . It suffices then to prove that this image is not contained in a Borel subgroup of $\text{GL}(W_u[7])$. Suppose it is. As we said in 4.2, there is an $x \in \mathbf{Q}^*$ such that

$$\frac{1728}{1 - u^2} = J_3(x).$$

By formula (14), one has $v_2(J_3(x)) \leq 0$; a contradiction follows, since u is an even integer.

For assertion (c), it is enough to show that E'_t cannot be isogenous over \mathbf{Q} either to E_t or to E''_t (by the same argument as in 3.5). From (7), one has

$$t + 3 = \frac{49u + 113}{54}, \quad 27t - 32 = \frac{49u - 113}{2}.$$

Consider a prime factor p of $49u + 113$; p is different from 2, 3 and 7. The formulas in §1 show that at p the curve E_t has good reduction and the curve E'_t has multiplicative reduction. Therefore E_t and E'_t are not isogenous over $\overline{\mathbf{Q}}$. If p is different from 113, the curve E''_t has good reduction at p , so E'_t and E''_t are not isogenous over $\overline{\mathbf{Q}}$. We have the same conclusion if 113 is the only prime factor of $49u + 113$: just take a prime factor of $49u - 113$ different from 113. The proof of Corollary 2 is now complete.

5. PROOF OF THEOREM 2

The idea behind the construction of the quintuples in question is simple: consider two rational numbers t, u satisfying (6) and (7), and the corresponding elliptic curves E_t, E'_t, E''_t . One has

$$c_4(E'_t) = -2^4(21t^3 + 21t^2 - 57t - 49).$$

We want the pair (t, u) to satisfy the following condition:

$$(**) \quad c_4(E'_t) \text{ is a square;}$$

i.e., there is a rational number z satisfying

$$(18) \quad z^2 = -2^4(21t^3 + 21t^2 - 57t - 49).$$

Set

$$(19) \quad v = \frac{-c_6(E'_t)}{z^3}$$

and

$$(20) \quad s = \frac{49}{54}(v - 1).$$

One checks that s is different from $0, -3, \frac{-49}{27}$ and $\frac{32}{27}$, so we can associate to s the elliptic curves E_s, E'_s, E''_s . As seen in 3.2, E_s is the twist of E'_t by $\sqrt{7z}$. Consider now the following five elliptic curves:

$$\mathcal{E}_1 = E_t, \quad \mathcal{E}_2 = E'_t, \quad \mathcal{E}_3 = E''_t,$$

$$\mathcal{E}_4, \text{ twist of } E'_s \text{ by } \sqrt{7z}, \quad \mathcal{E}_5, \text{ twist of } E''_s \text{ by } \sqrt{7z}.$$

By Theorem 1 and Lemma 2, the representations associated to the $\mathcal{E}_i, i = 1, \dots, 5$, are symplectically isomorphic.

Consider now condition (**). The substitution

$$(21) \quad t = \frac{-(4x + 7)}{21}, \quad z = \frac{32y}{21}, \quad x = \frac{-7}{4}(3t + 1), \quad y = \frac{21z}{32},$$

transforms equation (18) into the following:

$$(22) \quad y^2 = x^3 - 84x + 196.$$

This is a minimal equation for an elliptic curve denoted by \mathcal{F} . The conductor of \mathcal{F} is $10\,584 = 2^3 \times 3^3 \times 7^2$. The Mordell-Weil group $\mathcal{F}(\mathbf{Q})$ has rank 2; a basis for this group is (A, B) , where

$$A = (14, 42), \quad B = (0, 14).$$

Let $M = (x, y)$ be a point of $\mathcal{F}(\mathbf{Q})$ such that

$$(23) \quad M \neq 0, \pm A, \pm(2A + B), \pm(3A - 2B).$$

To the point M we associate first, by (21), a pair (t, z) satisfying (18), then the number u given by (7), and finally the pair (v, s) given by (19), (20). The condition (23) guarantees that s and t are different from $0, -3, \frac{-49}{27}$ and $\frac{32}{27}$. The pair (t, u) satisfies (6), (7) and (**), and so, to every point $M = (x, y)$ of $\mathcal{F}(\mathbf{Q})$ satisfying (23), one associates a quintuple $(\mathcal{E}_1, \mathcal{E}_2, \mathcal{E}_3, \mathcal{E}_4, \mathcal{E}_5)$ of elliptic curves over \mathbf{Q} , for which the five associated representations are symplectically isomorphic.

Here is a numerical example. Take $M = 2A = (8, -6)$, so that $t = \frac{-13}{7}$ and $s = \frac{-169}{108}$. The corresponding five elliptic curves \mathcal{E}_i have the following minimal equations:

$$\begin{aligned} \mathcal{E}_1: y^2 &= x^3 + x^2 - 16x - 32, \\ \mathcal{E}_2: y^2 &= x^3 + x^2 - 16x + 13, \\ \mathcal{E}_3: y^2 &= x^3 + x^2 - 269\,761\,480x - 1\,714\,632\,766\,400, \\ \mathcal{E}_4: y^2 &= x^3 + x^2 + 6\,243\,015x + 577\,597\,883, \\ \mathcal{E}_5: y^2 &= x^3 + x^2 - 2\,881x + 73\,171. \end{aligned}$$

The conductors $N_i = N(\mathcal{E}_i)$ are the following:

$$\begin{aligned} N_1 &= 104 = 2^3 \times 13, \\ N_2 &= 5\,096 = 2^3 \times 7^2 \times 13, \\ N_3 &= 586\,040 = 2^3 \times 5 \times 7^2 \times 13 \times 23, \\ N_4 &= 16\,120 = 2^3 \times 5 \times 13 \times 31, \\ N_5 &= 1\,144 = 2^3 \times 11 \times 13. \end{aligned}$$

As one can check, the representations associated to the \mathcal{E}_i are onto, and the \mathcal{E}_i are pairwise nonisogenous over $\overline{\mathbf{Q}}$. Now Theorem 2 is a consequence of the following more precise result:

Proposition 1. *To every point $M = (x, y)$ of $\mathcal{F}(\mathbf{Q})$ satisfying (23), let us associate the quintuple $(\mathcal{E}_1, \mathcal{E}_2, \mathcal{E}_3, \mathcal{E}_4, \mathcal{E}_5)$ as above. Then, except for a finite number of such points M ,*

- (a) *the representations associated to the \mathcal{E}_i are onto, and*
- (b) *the \mathcal{E}_i are pairwise nonisogenous over $\overline{\mathbf{Q}}$.*

Proof. The formulas (21), (7), (19), (20) define nonconstant elements t, z, u, v, s of the function field $\mathbf{Q}(\mathcal{F})$. By 4.2, the number of points M such that the image of the representation ρ_t associated to E_t is contained in the normalizer of a Cartan subgroup of $\mathrm{GL}(E_u[7])$ is finite. To prove assertion (a) (for almost all M), it remains to show that the number of points M such that the image of the representation ρ_t associated to E_t is contained in a Borel subgroup of $\mathrm{GL}(E_t[7])$ is also finite. Consider such a point M . One has $j(E_t) = f(M)$, for a suitable nonconstant function $f \in \mathbf{Q}(\mathcal{F})$. On the other hand, 4.2 shows that there is a point $M' = (X, Y)$ of $\mathcal{C}(\mathbf{Q})$ such that $j(E_t) = g(M')$, for some nonconstant function $g \in \mathbf{Q}(\mathcal{C})$. The conclusion now comes from Lemma 3, since the elliptic curves \mathcal{F} are \mathcal{C} are not isogenous over $\overline{\mathbf{Q}}$; indeed we can apply Lemma 1, noting that \mathcal{C} has no complex multiplication and that one has, for instance, $a_{11}(\mathcal{C}) = -4$, whereas $a_{11}(\mathcal{F}) = -6$.

Now let us prove assertion (b). For $i = 1, \dots, 5$, there is a nonconstant function $f_i \in \mathbf{Q}(\mathcal{F})$ such that, for every point M satisfying (23),

$$j(\mathcal{E}_i) = f_i(M).$$

Consider then the following function $\Psi \in \mathbf{Q}(\mathcal{C})$:

$$\Psi = \prod_{1 \leq i < l \leq 5} \Phi(f_i, f_l),$$

where Φ is the polynomial defined in 4.1. First Ψ is nonzero, because we saw that the elliptic curves \mathcal{E}_i associated to the point $M = 2A$ were pairwise nonisogenous over $\overline{\mathbf{Q}}$. If now M is a point of $\mathcal{F}(\mathbf{Q})$ satisfying (23), and if from one side the representation ρ_t associated to E_t is onto and from another side $\Psi(M) \neq 0$, then the point M satisfies conditions (a) and (b) of the proposition.

6. SOME REMARKS

Let us first explain briefly how we found the elliptic curves E, E', E'' . By the method of §6 of [4], we obtained a lot of pairs (A, A') of nonisogenous elliptic curves over \mathbf{Q} giving symplectically isomorphic representations, $j(A)(j(A) - 1728)$ being a square. To this end, use was made of the tables of J. Cremona giving the list, up to isogeny, of Weil curves having conductor ≤ 5077 ; these tables are accessible by ftp. One could then guess the existence of a pair (E, E') having the properties listed in Theorem 1. The curve E was known; as to E' , we just had to find $j(E')$. In this fraction, the denominator was essentially known, and the numerator was obtained by Lagrange interpolation. Similarly, for each pair (A, A') as above, corresponding to the parameter t , the values of the polynomials α_i (considered in 3.4) at t were found with the help of the LLL algorithm (cf. the proof of Lemma 4 of [4]). Lagrange interpolation then gave the α_i themselves. Of course, the congruence (11) still had to be checked, which was done, using Pari once more.

Also, the following question arises naturally. For an elliptic curve A , consider the condition (*) in Corollary 1, which amounts to saying that A may be defined by a Weierstraß equation for which the c_4 invariant is a square (in the base field). Is there some reasonable (probably not modular) interpretation of this condition?

Let us recall finally why one could suspect the existence of pairs similar to the pair (E, E') in Theorem 1, as mentioned in [3]. In *loc. cit.* one introduces a certain surface $Z = Z_{7,1}$, which is normal, projective, and defined over \mathbf{Q} , as well as its desingularization \tilde{Z} . The surface Z essentially classifies the isomorphism classes of triples (E, E', φ) consisting of two elliptic curves E, E' and a symplectic isomorphism φ from $E[7]$ onto $E'[7]$ compatible with the action of Galois. In *loc. cit.*, it is shown that the surface \tilde{Z} is *rational*, which gives a possible explanation. Note that in some of the proofs above one could also use the surface Z . As an example, the classes of triples (E, E', φ) , where E, E' are defined over \mathbf{Q} and isogenous over $\overline{\mathbf{Q}}$, belong to a finite number of curves on Z . These curves have to be removed if one is interested in the nontrivial points of Z rational over \mathbf{Q} .

REFERENCES

- [1] L. Caporaso, J. Harris, and B. Mazur, *Uniformity of rational points*, J. Amer. Math. Soc. **10** (1995), 1–35. MR **97d**:14033
- [2] J. E. Cremona, *Algorithms for modular elliptic curves*, Cambridge Univ. Press, 1992. MR **93m**:11053

- [3] E. Kani, and W. Schanz, *Diagonal quotient surfaces*, Manuscripta Math. **93** (1997), 67–108. MR **98d**:14048
- [4] A. Kraus and J. Oesterlé, *Sur une question de B. Mazur*, Math. Ann. **293** (1992), 259–275. MR **93e**:11074
- [5] A. Kraus, *Sur les modules des points de 7-torsion d'une famille de courbes elliptiques*, Ann. Inst. Fourier (Grenoble) **46** (1996), 899–907. MR **97i**:11060
- [6] S. Lang, *Elliptic functions*, 2nd ed., Springer-Verlag, 1987. MR **88c**:11028
- [7] B. Mazur, *Rational isogenies of prime degree*, Invent. Math. **44** (1978), 129–162. MR **80h**:14022
- [8] K. Rubin and A. Silverberg, *Families of elliptic curves with constant mod p representations*, in Elliptic Curves, Modular Forms and Fermat's Last Theorem, International Press, 1995, pp. 148–161. MR **96j**:11078
- [9] J.-P. Serre and J. Tate, *Good reduction of abelian varieties*, Ann. of Math. **68** (1968), 492–517. MR **38**:4488
- [10] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259–331. MR **52**:8126
- [11] J.-P. Serre, *Points rationnels des courbes modulaires $X_0(N)$* , Sémin. Bourbaki, Exposé **511** (1977), Lecture Notes in Math., vol. 710, Springer-Verlag, 1979, pp. 89–100. MR **82c**:14049

UNIVERSITÉ PARIS VI, LABORATOIRE DE MATHÉMATIQUES FONDAMENTALES, UFR 921,
4, PLACE JUSSIEU, 75252 PARIS CEDEX 05, FRANCE

E-mail address: halberst@math.jussieu.fr

UNIVERSITÉ PARIS VI, INSTITUT DE MATHÉMATIQUES, CASE 247, 4, PLACE JUSSIEU, 75252
PARIS CEDEX 05, FRANCE

E-mail address: kraus@math.jussieu.fr