Rational Points on Elliptic Curves over $\mathbb{Q}$ in Elementary Abelian 2-Extensions of $\mathbb{Q}$

by

Michael Laska and Martin Lorenz *)

SONDERFORSCHUNGSBEREICH 40

THEORETISCHE MATHEMATIK

UNIVERSITÄT BONN

UND

MAX-PLANCK-INSTITUT FÜR MATHEMATIK

BONN

Rational Points on Elliptic Curves over $\mathbb{Q}$ in Elementary Abelian 2-Extensions of $\mathbb{Q}$

by

Michael Laska and Martin Lorenz *)

Max-Planck-Institut für Mathematik
Gottfried-Claren-Straße 26
D - 5300 Bonn 3

MPI/SFB 84-21

*) Research supported by the Deutsche Forschungsgemeinschaft/ Heisenberg Programm (Lo 261/2-1).

Introduction.

Let E be an elliptic curve over $\mathbb{Q}$. In this note, we describe the possibilities for the torsion subgroup $E(F)_{tors}$ of the group $E(F)$ of F-rational points on E, where $F = \mathbb{Q}[\sqrt{z}\ ;\ z \in \mathbb{Z}]$ denotes the maximal elementary abelian 2-extension of $\mathbb{Q}$. Our main result is as follows.

Theorem. $E(F)_{tors}$ is isomorphic to one of the following 22 groups

$$\mathbb{Z}/2^a\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \qquad (a = 2,3,4,5)\ ,$$

$$\mathbb{Z}/2^a\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \qquad (a = 1,2,3,4)\ ,$$

$$\mathbb{Z}/2^a\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \qquad (a = 2,3)\ ,$$

$$\mathbb{Z}/2^a\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \qquad (a = 1,2)\ ,$$

$$\mathbb{Z}/2^a\mathbb{Z} \oplus \mathbb{Z}/2^a\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z} \qquad (a = 1,2)\ ,$$

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$$

or $\{0\}$, $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z}$, $\mathbb{Z}/7\mathbb{Z}$, $\mathbb{Z}/9\mathbb{Z}$, $\mathbb{Z}/15\mathbb{Z}$.

The finiteness of $E(F)_{tors}$ also follows from a very general theorem of Ribet [Ri] which we shall not need in the following. We do not know if all groups in the above list can actually be realized as $E(F)_{tors}$ for suitable curves E over $\mathbb{Q}$.

For quadratic number fields $K/\mathbb{Q}$ the group $E(K)_{tors}$ has been investigated in [La]. If E is defined over K, not necessarily over $\mathbb{Q}$, then there are several results proving the nonexistence of points of certain orders in $E(K)_{tors}$. Such results may be found e.g. in [Man], [Ke2] or [Kam].

Throughout this note we keep the following

Notations and Conventions. For any abelian group V, $\mathrm{rk}\, V = \dim_{\mathbb{Q}}(V \otimes_{\mathbb{Z}} \mathbb{Q})$ denotes the rank of V and V_{tors} will be the torsion subgroup of V. Furthermore, if n is a positive integer, then $V_n = \{v \in V \mid n \cdot v = 0\}$ is the group of n-division points of V, and $V_{(n)} = \bigcup_{i \geq 1} V_{n^i}$.

1. Some Technical Lemmas.

A) Decompositions.

Throughout this section, we will keep the following notation:

k will be a field,

K/k a finite Galois extension with group $G = \mathrm{Gal}(K/k)$, and

A will denote a simple abelian variety over k.

An abelian variety B over k is called a K/k-form of A if B is isomorphic to A over K. If $E(K/k,A)$ denotes the set of classes of K/k-forms of A under the equivalence relation defined by k-isomorphism, then there is a bijective correspondence

$$\Theta : E(K/k) \to H^1(G, \mathrm{Aut}_K A) .$$

Here $\mathrm{Aut}_K A$ denotes the group of K-automorphisms of A, with the usual G-operation. The map Θ is obtained as follows [Se; Chap.III,§ 1]: Let B be a K/k-form of A. Then G acts on the set of K-isomorphisms $f : B_K \to A_K$. If $s(f)$ denotes the image of f under $s \in G$, then the map $s \mapsto \phi_s := s(f) \cdot f^{-1}$ is a 1-cocycle of G with values in $\mathrm{Aut}_K A$. The class of (ϕ_s) in $H^1(G, \mathrm{Aut}_K A)$ is the image of the class of B in $E(K/k,A)$ under Θ. In particular, for any 1-cocycle $\gamma = (\gamma_s)$ of G with values in $\mathrm{Aut}_K A$, there

exists a K/k-form A^γ of A together with a K-isomorphism $f^\gamma : A^\gamma \to A$ such that

$$s(f^\gamma) = \gamma_s \circ f^\gamma \quad (s \in G) .$$

A^γ is called a <u>γ-twist of A</u> . For the operations of G on the K-points $A(K)$, resp. $A^\gamma(K)$, the above formula can be expressed as

$$s(f^\gamma(s^{-1}(a))) = (\gamma_s \circ f^\gamma)(a) \qquad (a \in A^\gamma(K),\ s \in G) .$$

Thus, in particular,

$$f^\gamma(A^\gamma(k)) = \{a \in A(K) \mid s(a) = \gamma_s(a) \text{ for all } s \in G\} .$$

<u>Lemma 1.1.</u> Suppose $G = \mathrm{Gal}(K/k)$ is abelian of order n and exponent e . If $\mathrm{Aut}_{\bar{k}}A$ contains a primitive e-th root of unity, then there exist K/k-forms A^i of A and K-isomorphisms $f^i : A^i \to A$ $(i = 1,2,\ldots,n)$ such that the kernel and cokernel of

$$\bigoplus_{i=1}^{n} A^i(k) \xrightarrow{\oplus f^i} A(K)$$

are annihilated by n .

<u>Proof.</u> Let $\omega \in \mathrm{Aut}_k A$ be a primitive e-th root of unity and set $R = \mathbb{Z}[\omega] \subseteq \mathrm{End}_k A$. Then R is a commutative domain, since A is simple, and the group ring $R[G]$ acts on $A(K)$. Moreover, there are n distinct homomorphisms $\chi_i : G \to \langle\omega\rangle \subseteq R$ $(i = 1,2,\ldots,n)$. Set

$$e_i := \sum_{s \in G} \chi_i(s^{-1})\, s \in R[G] .$$

and

$$A(K)^i := \{a \in A(K) \mid s(a) = \chi_i(s) \cdot a \text{ for all } s \in G\} .$$

Then we have $e_i \cdot A(K) \subseteq A(K)^i$. Furthermore, by the orthogonality relations ,

$\sum_{i=1}^{n} e_i = n \in R$, whence

$$n \cdot A(K) \subseteq \sum_{i=1}^{n} A(K)^i \quad .$$

The action of e_i on $A(K)^i$ is given by multiplication with $\sum_{s \in G} \chi_i(s^{-1})\, \chi_j(s) = n\, \delta_{ij}$ (δ_{ij} = Kronecker-δ) . Therefore, for all i we have

$$n\,(A(K)^i \cap \sum_{j \neq i} A(K)^j) = 0 \quad .$$

Finally, viewing χ_i as a 1-cocycle of G with values in $\mathrm{Aut}_K A$, we have an associated K/k-form A^i of A and a K-isomorphism $f^i : A^i \to A$ such that $f^i(A^i(k)) = A(K)^i$. This proves the lemma.

Remark 1.2. By construction, the image $f^i(A^i(k)) = A(K)^i$ is a G-invariant subgroup of $A(K)$. Moreover, if $\chi_i(G) \subseteq \{\pm 1\}$ (e.g., if $e = 2$) , then all subgroups of $A(K)^i$ are G-invariant.

Corollary 1.3. In the situation of Lemma 1.1, we have

(i) $\mathrm{rk}\, A(K) = \sum_{i=1}^{n} \mathrm{rk}\, A^i(k)$.

(ii) Let p be a rational prime and let n_p denote the p-part of n . Then n_p annihilates the kernel and cokernel of the map

$$\bigoplus_{i=1}^{n} A^i(k)_{(p)} \to A(K)_{(p)}$$

induced by $\oplus f_i$ on the p-primary components.

For our later applications to elliptic curves, we now briefly discuss the special case where G is an elementary abelian 2-group, say $G \cong C_2^m = C_2 \times \ldots \times C_2$ (m times) , and $\mathrm{char}\, k \neq 2$. Then there exists a k-basis $1 = \theta_1, \theta_2, \ldots, \theta_n$ ($n = 2^m$) of K such that $s(\theta_i) = \pm\theta_i$ holds for all $s \in G$ and all i . In particular, $\theta_i^2 =: z_i \in k$, and the characters

$\chi_i : G \to \{\pm 1\}$, $s \mapsto s(\theta_i)\theta_i^{-1}$ are all distinct. The corresponding K/k-forms A^i of A will also be denoted by $A^{(z_i)}$. So there are K-isomorphisms $f^i : A^{(z_i)} \to A$ with $s(f^i(a)) = \chi_i(s)\, f^i(a)$ $(s \in G\ ,\ a \in A^{(z_i)}(k))$.

Lemma 1.4. Assume that char $k \neq 2$ and $G = \mathrm{Gal}(K/k)$ is an elementary abelian 2-group. Then, with the above notations, we have

(i) If $A(K)_{(2)} \neq \{0\}$ then $A(k)_2 \neq \{0\}$.

(ii) For all $i \neq 1$, f^i yields an isomorphism of 2-division points $A^{(z_i)}(k)_2 \cong A(k)_2$ and the map $\mathrm{id} \oplus f^i : A(k) \oplus A^{(z_i)}(k) \to A(K)$ has kernel isomorphic to $A(k)_2$.

Proof. (i). If $A(K)_{(2)}$ is nonzero then $A(K)_2$ is a nonzero $\mathbb{F}_2[G]$-module. Since G is a 2-group, G acts trivially on the simple submodules of $A(K)_2$ so that these are contained in $A(k)_2$.

(ii). For each $a \in A^{(z_i)}(k)_2$, one has $f^i(a) = \chi_i(s)\, f^i(a) = s(f^i(a))$ and so $f^i(a) \in A(k)_2$. Similarly, the inverse of f^i maps $A(k)_2$ to $A^{(z_i)}(k)_2$. Finally, $(a, a_i) \in A(k) \oplus A^{(z_i)}(k)$ belongs to the kernel of $\mathrm{id} \oplus f^i$ if and only if $a + f^i(a_i) = 0 = s(a + f^i(a_i)) = a - f^i(a_i)$, where s is an element of G with $\chi_i(s) = -1$. Therefore, $\ker(\mathrm{id} \oplus f^i) = \{(a, (f^i)^{-1}a) \mid a \in A(k)_2\} \cong A(k)_2$.

In dealing with elliptic curves E over $\mathbb{Q}$ and elementary abelian 2-extensions $K/\mathbb{Q}$, one can always choose the basis $1 = \theta_1, \theta_2, \ldots, \theta_n$ of K over $\mathbb{Q}$ so that the elements $z_i = \theta_i^2$ belong to $\mathbb{Z}$. If E has Weierstrass equation

$$y^2 = x^3 + ax + b \qquad (a, b \in \mathbb{Z}) \ ,$$

then $E^{(z_i)}$ has Weierstrass equation

$$y^2 = x^3 + az_i^2 x + bz_i^3 \ ,$$

and an isomorphism $f^i : E^{(z_i)} \to E$ with $s(f^i(e)) = \chi_i(s)\, f^i(e)$ for all $s \in G$, $e \in E^{(z_i)}(k)$ is given by $f^i(x,y) = (z_i^{-1}x, \theta_i^{-1}z_i^{-1}y)$.

B) Automorphisms.

For later use in Section 2, we collect a few facts concerning the automorphism groups $\mathrm{Aut}(\mathbb{Z}/2^a\mathbb{Z} \oplus \mathbb{Z}/2^b\mathbb{Z})$. Consider, slightly more generally, any commutative ring R with a nilpotent maximal ideal M, say $M^a = \{0\}$, $M^{a-1} \neq \{0\}$. Let $I = M^b$, $0 < b < a$, be a non-trivial ideal of R. Then the automorphism ring of the (right) R-module $V = R \oplus R/I$ is isomorphic to a generalized matrix ring:

$$\mathrm{End}(V_R) \cong \begin{pmatrix} R & \mathrm{ann}_R I \\ R/I & R/I \end{pmatrix} .$$

Here, if $[r]$ denotes the class of $r \in R$ in R/I, then the matrix $\begin{pmatrix} r & j \\ [s] & [t] \end{pmatrix} \in \begin{pmatrix} R & \mathrm{ann}_R I \\ R/I & R/I \end{pmatrix}$ acts on $\begin{pmatrix} u \\ [v] \end{pmatrix} \in V$ via

$$\begin{pmatrix} r & j \\ [s] & [t] \end{pmatrix} \cdot \begin{pmatrix} u \\ [v] \end{pmatrix} = \begin{pmatrix} ru + jv \\ [su + tv] \end{pmatrix} .$$

Let Γ denote the group of R-automorphisms of V, viewed as the group of units of the above matrix ring. Then, with $U(.)$ denoting unit groups, we have

$$\Gamma = \begin{pmatrix} U(R) & \mathrm{ann}_R I \\ R/I & U(R/I) \end{pmatrix} .$$

In the following lemma, we apply this to the special case where $R = \mathbb{Z}/2^a\mathbb{Z}$ and $I = 2^bR$ $(0 < b < a)$. We use the above notation.

Lemma 1.5. Set $\Gamma_{a,b} = \mathrm{Aut}(\mathbb{Z}/2^a\mathbb{Z} \oplus \mathbb{Z}/2^b\mathbb{Z})$, where a and b are positive integers with $a > b$, and $R = \mathbb{Z}/2^a\mathbb{Z}$. Then $\Gamma_{a,b}$ has order 2^{a+3b-2}. In case $b = 1$, $\Gamma_{a,1}$ is a semidirect product, $\Gamma_{a,1} = N \rtimes U$, with

$N = \begin{pmatrix} 1+2R & 2^{a-1}R \\ [0] & [1] \end{pmatrix} \cong (1+2R,\cdot) \oplus (2^{a-1}R,+)$, the kernel of the reduction map modulo $2R$, and $U = \begin{pmatrix} 1 & 0 \\ R/2R & [1] \end{pmatrix} \cong \mathbb{Z}/2\mathbb{Z}$. All elementary abelian subgroups $A \subseteq \Gamma_{a,1}$ have order at most 8 (and at most 4 for $a = 2$) , and a subgroup of A of index ≤ 2 lies in the diagonal $D = \begin{pmatrix} 1+2R & 0 \\ [0] & [1] \end{pmatrix}$. If, in addition, $a = 2$ or 3 then A is either upper or lower triangular.

Proof. The formula for $\#\Gamma_{a,b}$ is clear from the explicit description of $\Gamma_{a,b}$ in terms of matrices.

Assume now that $b = 1$. The decomposition $\Gamma_{a,1} = N \rtimes U$, with N and U as above is easily verified. Also, U is generated by the matrix $u = \begin{pmatrix} 1 & 0 \\ [1] & [1] \end{pmatrix} \in \Gamma_{a,1}$. Its centralizer in N is the diagonal $D \cong (U(R),\cdot)$. Now let $A \subseteq \Gamma_{a,1}$ be elementary abelian. If $A \subseteq N$, then clearly A has order at most 8 (and at most 4 if $a = 2$) , since $U(R) = 1 + 2R \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2^{a-2}\mathbb{Z}$. Otherwise, A contains an element of the form $g = nu$, with the above matrix u and with a suitable $n \in N$, and $A = \langle N \cap A, g \rangle$. Now $N \cap A$ centralizes g and hence n , as N is commutative. Thus $N \cap A \subseteq D$ and, again, A has order at most 8 (at most 4 if $a = 2$). Also, in both cases, $[A : A \cap D] \leq 2$. Finally, we claim that for $a = 2$ or 3 , each element $g \in \Gamma$ of order 2 is either upper or lower triangular. To see this, suppose $g = \begin{pmatrix} 1+i & j \\ [1] & [1] \end{pmatrix}$, with $i \in 2R$ and $j \in 2^{a-1}R$, has order 2 . Then $(1+i)^2 + j = 1$ in R , and hence $i(i+2) + j = 0$. Now $i = 2i_1$ for some $i_1 \in R$ and so $i(i+2) = 4i_1(i_1+1) \in 8R$. Thus, if $a \leq 3$, then we must have $j = 0$ and g is lower triangular. ∎

2. Elementary Abelian 2-Extensions.

Let E be an elliptic curve over $\mathbb{Q}$ and let $F \supseteq \mathbb{Q}$ be the maximal elementary abelian 2-extension of $\mathbb{Q}$, i.e. $F = \mathbb{Q}[\sqrt{z} \; ; \; z \in \mathbb{Z}]$. In this section, we consider the possiblities for the torsion subgroup $E(F)_{tors}$ of $E(F)$. Our essential tool will be the following result due to MAZUR [Maz; Theorems 1 and 2] and KENKU who added the finishing touches to part (ii) [Ke3], [Ke4], [Ke5], [Ke6], [Ke7].

Theorem 2.1. Let E be an elliptic curve over $\mathbb{Q}$.

(i) $E(\mathbb{Q})_{tors}$ is isomorphic to one of the following fifteen groups:

$$\mathbb{Z}/m\mathbb{Z} \quad \text{with} \quad 1 \leq m \leq 10 \quad \text{or} \quad m = 12 \, ,$$

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z} \quad \text{with} \quad 1 \leq n \leq 4 \, .$$

(ii) If $E(\overline{\mathbb{Q}})_{tors}$ has a rational (i.e $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$-invariant) subgroup isomorphic to $\mathbb{Z}/n\mathbb{Z}$, then

$$n \leq 19 \quad \text{or} \quad n \in \{21,25,27,37,43,67,163\} \, .$$

The above notations will be kept throughout this section. So

E will be an elliptic curve over $\mathbb{Q}$, and

$F = \mathbb{Q}[\sqrt{z} \; ; \; z \in \mathbb{Z}]$.

We first describe the possibilities for the 2'-torsion subgroup of $E(F)$

Proposition 2.2. $E(F)_{2'} = \{e \in E(F) \mid ne = 0 \text{ for some odd } n\}$ is isomorphic to one of the following seven groups:

$$\mathbb{Z}/m\mathbb{Z} \text{ with } m \in \{1,3,5,7,9,15\} \text{, or}$$

$$\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \, .$$

Proof. It clearly suffices to show that for all finite subextensions $K/\mathbb{Q}$ with $K \subseteq F$, $E(K)_{2'}$ is isomorphic to one of the above seven groups. So fix $K/\mathbb{Q}$ with $G = \mathrm{Gal}(K/\mathbb{Q}) \simeq C_2^m$. Then, by Corollary 1.3(ii),

$$E(K)_{2'} \simeq E^{(z_1)}(\mathbb{Q})_{2'} \oplus \ldots \oplus E^{(z_n)}(\mathbb{Q})_{2'}$$

for suitable integers $z_i \in \mathbb{Z}$; $i = 1,2,\ldots,n = 2^m$. Furthermore, by Theorem 2.1(i). each summand $C_i := E^{(z_i)}(\mathbb{Q})_{2'}$ is isomorphic to one of the groups $\mathbb{Z}/m\mathbb{Z}$ with $m \in \{1,3,5,7,9\}$. Note also that each C_i corresponds to a rational subgroup of $E(K)_{2'}$. For, by Remark 1.2, the image of $E^{(z_i)}(\mathbb{Q})$ in $E(K)$ is rational, and hence so is the image of C_i, since $C_i = E^{(z_i)}(\mathbb{Q})_{2'}$ is characteristic in $E^{(z_i)}(\mathbb{Q})$. Next, observe that, by duality, each of the groups $\mathbb{Z}/m\mathbb{Z}$ with $m \in \{5,7,9\}$ can occur at most once among the C_i, for otherwise K would contain the m-division field of E and hence a primitive m-th root of unity ζ_m [Shi; Proposition 4.2]. But this is impossible for $m \in \{5,7,9\}$, since $G = \mathrm{Gal}(K/\mathbb{Q})$ has exponent 2. Moreover, of course, at most two of the $E^{(z_i)}(\mathbb{Q})_{2'}$ can contain a copy of $\mathbb{Z}/3\mathbb{Z}$. Using the fact that the image of each C_i in $E(K)$ is a rational cycle in $E(K)$, we conclude that $\mathbb{Z}/5\mathbb{Z}$ and $\mathbb{Z}/7\mathbb{Z}$ cannot occur simultaneously among the C_i, for otherwise $E(K)$ would contain a rational subgroup isomorphic to $\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/7\mathbb{Z} \simeq \mathbb{Z}/35\mathbb{Z}$, contradicting Theorem 2.1(ii). Similarly, $\mathbb{Z}/5\mathbb{Z}$ and $\mathbb{Z}/9\mathbb{Z}$ cannot occur together, and the same holds for $\mathbb{Z}/7\mathbb{Z}$ and $\mathbb{Z}/9\mathbb{Z}$.

We claim that the combination $\mathbb{Z}/9\mathbb{Z}$ with $\mathbb{Z}/3\mathbb{Z}$ is impossible. Indeed, if $E^{(z_i)}(\mathbb{Q})_{2'} \simeq \mathbb{Z}/9\mathbb{Z}$ and $E^{(z_j)}(\mathbb{Q})_{2'} \simeq \mathbb{Z}/3\mathbb{Z}$, say, then replacing E by $E^{(z_i)}$ if necessary, we can assume that $E(\mathbb{Q})_{2'} \simeq \mathbb{Z}/9\mathbb{Z}$ and $E^{(z_iz_j)}(\mathbb{Q})_{2'} \simeq \mathbb{Z}/3\mathbb{Z}$. In particular, E has a rational point of order 9 and an additional rational 3-cycle. But this contradicts [Ku; Lemma III.2.2].

It remains to discard the possibilities of $\mathbb{Z}/3\mathbb{Z}$ and $\mathbb{Z}/7\mathbb{Z}$ occuring together. In this case, these two groups would generate a rational 21-cycle in $E(\overline{\mathbb{Q}})$. Nox $X_0(21)$ has exactly four rational points which are not cusps,

and to each of these points there corresponds an elliptic curve over $\mathbb{Q}$ with conductor of the form $2^a 3^b$ [Modular Functions of One Variable IV, Springer LN 476(1975)*); p. 80 and 123]. Therefore, after replacing E (and correspondingly the two twists of E with rational 2'-torsion $\simeq \mathbb{Z}/3\mathbb{Z}$, resp. $\simeq \mathbb{Z}/7\mathbb{Z}$) by a quadratic twist, we can assume that E has good reduction at 5, and that $E^{(t_1)}(\mathbb{Q})_{2'} \simeq \mathbb{Z}/3\mathbb{Z}$ and $E^{(t_2)}(\mathbb{Q})_{2'} \simeq \mathbb{Z}/7\mathbb{Z}$ for suitable $t_i \in \mathbb{Z}$. Letting $\tilde{E}$ denote the reduction of E modulo 5, we claim that $N_{25} := \#\tilde{E}(\mathbb{F}_{25}) = 21$. To see this, let $K_i = \mathbb{Q}(\sqrt{t_i})$, let $\mathfrak{p}_i$ be a prime of K_i over 5, and let $F_{\mathfrak{p}_i} = \mathcal{O}_{K_i}/\mathfrak{p}_i$ be the corresponding residue field. Then reduction mod $\mathfrak{p}_i$ defines an injective map $E(K_i)_{tors} \hookrightarrow \tilde{E}(F_{\mathfrak{p}_i}) \subseteq \tilde{E}(\mathbb{F}_{25})$ (see[Kat; Appendix]). We conclude that $3 \mid N_{25}$ and $7 \mid N_{25}$. On the other hand, by the "Riemann hypothesis", $N_{25} = 26 - a_{25}$, where $a_{25} = \pi^2 + \bar{\pi}^2$ for some $\pi \in \mathbb{C}$ with $\pi \cdot \bar{\pi} = 5$ and $a_5 = \pi + \bar{\pi} \in \mathbb{Z}$. In particular, $N_{25} \leq (5+1)^2 = 36$ whence $N_{25} = 21$, as claimed. But then we deduce that $5 = a_{25} = a_5^2 - 10$ so that $a_5^2 = 15$, contradiction. This completes the proof of the proposition. ∎

Remarks 2.3. a) Let $K_{2'} \supseteq \mathbb{Q}$ denote the field extension of $\mathbb{Q}$ generated by $E(F)_{2'}$. If $E(F)_{2'} = \{0\}$ then, of course, $K_{2'} = \mathbb{Q}$. In the case $E(F)_{2'} \simeq \mathbb{Z}/m\mathbb{Z}$, for $m = 3,5,7$ or 9, $K_{2'}$ has degree 0 or 2 over $\mathbb{Q}$. This follows from the fact that the automorphism group of $\mathbb{Z}/m\mathbb{Z}$ is cyclic for the above values of m (of order 2,4,6, and 6, respectively). So $\mathrm{Gal}(F/\mathbb{Q})$ acts on $E(F)_{2'} \simeq \mathbb{Z}/m\mathbb{Z}$ through a cyclic quotient which must be of order 1 or 2. Finally, in the cases where $E(F)_{2'} \simeq \mathbb{Z}/15\mathbb{Z}$ or $\simeq \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$, the elementary abelian 2-groups of $\mathrm{Aut}(E(F)_{2'})$ have rank at most 2. Since $\mathrm{Gal}(F/\mathbb{Q})$ cannot act trivially on $E(F)_{2'}$ in these cases (Theorem 2.1(i)), $K_{2'}$ is of degree 2 or 4 over $\mathbb{Q}$.

b) If $E(F)_{2'} \simeq \mathbb{Z}/m\mathbb{Z}$ with $m = 7,9$ or 15, then $E(F)_{(2)} = \{0\}$ and

---

*) In the following quoted as "MF IV".

so $E(F)_{tors} \simeq \mathbb{Z}/m\mathbb{Z}$. To see this, note that, by Lemma 1.4, $E(F)_{(2)} \neq \{0\}$ implies that $E^{(z)}(\mathbb{Q})_2 \neq \{0\}$ for all quadratic twists $E^{(z)}$ of E . In the case where $m = 15$ we would deduce the existence of a rational 30-cycle, which is impossible, by Theorem 2.1(ii). If $E(F)_{2'} \simeq \mathbb{Z}/m\mathbb{Z}$ with $m = 7$ or 9 , then $E^{(z)}(\mathbb{Q}) \simeq \mathbb{Z}/m\mathbb{Z}$ for a suitable z and so, again, $E(F)_{(2)} = \{0\}$.

Proposition 2.4. $E(F)$ does not contain a rational subgroup isomorphic to one of the following groups:

$$\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \quad , \quad \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z} \quad ,$$
$$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \quad , \quad \mathbb{Z}/32\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \; .$$

Proof. Suppose, by way of contradiction, that $V \subseteq E(F)$ is rational and isomorphic to one of the above groups. Write $V_{(2)} = L \oplus S$ with $S \simeq \mathbb{Z}/2\mathbb{Z}$ and L the long 2-cycle, i.e. $L \simeq \mathbb{Z}/2^a\mathbb{Z}$, $a = 2,3$, or 5 . Let A denote the subgroup of $\mathrm{Aut}(V_2) = \Gamma_{a,1}$ given by the action of $\mathrm{Gal}(F/\mathbb{Q})$ on V_2 . In all cases, it is easy to see that A does not stabilize the long cycle L : If $V \simeq \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$, or $\mathbb{Z}/32\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, one would have rational cycles of order 24 , 20 , or 32 , respectively, which contradicts Theorem 2.1(ii). In case $V \simeq \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$, two 3-cycles in V are rational, hence a curve E' 3-isogenous to E over $\mathbb{Q}$ has a rational 9-cycle as well as a rational 4-cycle, contradicting Theorem 2.1(ii).

We now first discard the three cases with $a = 2$ or 3 . By Lemma 1.5, A is lower triangular and therefore stabilizes the short cycle $S \simeq \mathbb{Z}/2\mathbb{Z}$. In addition $2V_2 = 2L$ is a rational cycle contained in L . Let $\phi : E \to E' = E/S$ denote the isogeny associated with S and let $\phi' : E' \to E$ be the dual isogeny, both defined over $\mathbb{Q}$. Then $L_1 := (\phi')^{-1}(2V_2) \subseteq E'(\overline{\mathbb{Q}})$ is rational and cyclic of order $2^a = \#L$. Arguing as in the first paragraph

of the proof we derive a contradiction.

Thus in the following suppose that $V \simeq \mathbb{Z}/32\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. By Lemma 1.5, A has a subgroup A_o of index 2 which is diagonal, and hence stabilizes S and L . In particular, the above isogeny $\phi : E \to E' = E/S$ is A_o-invariant. Also, $L' = (\phi')^{-1}(L) \subseteq E'(\overline{\mathbb{Q}})$ is stabilized by A_o and L' is cyclic of order 64 . Therefore, the pair (E',L') belongs to a point of $X_0(64)$ of degree 2 which is not a cusp. By [Ke1; Lemma 1], the j-invariant $j(E')$ is integral (in fact, $j(E') = -3^3 \cdot 5^3$ or $3^3 \cdot 5^3 \cdot 17^3$). Now let $K \subseteq F$ be the field generated by $\phi(L) \subseteq E'(F)$. Let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$ over 3 and note that $F_{\mathfrak{p}} = \mathcal{O}_K/\mathfrak{p}$ is of degree ≤ 2 over $\mathbb{F}_3$ (for, $\mathrm{Gal}(F_{\mathfrak{p}}/\mathbb{F}_3)$ is a cyclic subquotient of $\mathrm{Gal}(K/\mathbb{Q})$ which is an elementary abelian 2-group). We consider reduction of E' modulo $\mathfrak{p}$ and denote the reduced curve by $\tilde{E}'$. As $j(E')$ is integral, reduction at $\mathfrak{p}$ is either good or additive. In case of good reduction, one has $\#\tilde{E}'(\mathbb{F}_9) \leq 16$, which is impossible, since $\mathbb{Z}/32\mathbb{Z} \simeq \phi(L) \subseteq E'(K)_{(2)}$ and reduction modulo $\mathfrak{p}$ is injective on $E'(K)_{(2)}$. In case of additive reduction, let $E'_o(K)_{(2)}$ denote the subgroup of $E'(K)_{(2)}$ consisting of those points which are mapped to nonsingular points of $\tilde{E}'(F_{\mathfrak{p}})$. One has $[E'(K)_{(2)} : E'_o(K)_{(2)}] \leq 4$ (cf. [Ta; §6]) and so $\#E'_o(K)_{(2)} \geq 8$. On the other hand, $E'_o(K)_{(2)} \subseteq \tilde{E}'_{ns}(\mathbb{F}_9) \simeq \mathbb{F}_9^+$, a contradiction. Thus $V \simeq \mathbb{Z}/32\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ is impossible, and the proposition is proved. ∎

Theorem 2.5. Let E be an elliptic curve over $\mathbb{Q}$ and let $F = \mathbb{Q}[\sqrt{z}\ ;\ z \in \mathbb{Z}]$. Then the torsion subgroup $E(F)_{tors}$ is isomorphic to one of the following 22 groups:

$$\mathbb{Z}/2^a\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \qquad (a = 2,3,4,5),$$

$$\mathbb{Z}/2^a\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \qquad (a = 1,2,3,4),$$

$$\mathbb{Z}/2^a\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \qquad (a = 2,3),$$

$$\mathbb{Z}/2^a\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \qquad (a = 1,2),$$

$$\mathbb{Z}/2^a\mathbb{Z} \oplus \mathbb{Z}/2^a\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z} \qquad (a = 1,2),$$

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$$

or $\{0\}$, $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z}$, $\mathbb{Z}/7\mathbb{Z}$, $\mathbb{Z}/9\mathbb{Z}$, $\mathbb{Z}/15\mathbb{Z}$.

Proof. We first describe the possibilities for the 2-primary component $E(F)_{(2)}$. If $E(F)_{(2)} \neq \{0\}$ then, by Lemma 1.4(i), we must have $E(\mathbb{Q})_2 \neq \{0\}$ and so the 2-division field of E is quadratic over $\mathbb{Q}$ and thus contained in F. On the other hand, the 8-division field of E is not contained in F, as F does not contain a primitive 8th root of unity. Therefore, if $E(F)_{(2)} \neq \{0\}$ then it must be of the form $E(F)_{(2)} \simeq \mathbb{Z}/2^a\mathbb{Z} \oplus \mathbb{Z}/2^b\mathbb{Z}$ with $a \geq b$ and $b = 1$ or 2. Moreover, $a - b \leq 4$ for otherwise $2^b \cdot E(F)_{(2)}$ would be a rational cycle of E of order divisible by 32, which is impossible by Theorem 2.1(ii). Finally, since $E(F)$ does not contain a rational subgroup isomorphic to $\mathbb{Z}/32\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, by Proposition 2.4, the groups $\mathbb{Z}/64\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/32\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ are ruled out, and we are left with nine possibilities: $\{0\}$, $\mathbb{Z}/2^a\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ $(a = 1,2,3,4)$, and $\mathbb{Z}/2^a\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ $(a = 2,3,4,5)$.

It remains to check the possible combinations of these groups with the choices for $E(F)_2$, as described in Proposition 2.2. First, by Remark 2.3 b), $E(F)_2 \simeq \mathbb{Z}/m\mathbb{Z}$ with $m = 7,9$ or 15 entails $E(F)_{(2)} = \{0\}$. Also, if

$E(F)_{2'} \neq \{0\}$, then it contains a rational cycle of order 3, 5 or 7 . Therefore, by Theorem 2.1(ii), E cannot have an additional rational 8-cycle, which rules out the possibilities $E(F)_{(2)} \simeq \mathbb{Z}/32\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ or $\simeq \mathbb{Z}/16\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Similarly, if $E(F)$ has 5- or 7-torsion then E cannot have a rational 4-cycle and so $E(F)_{(2)} \simeq \mathbb{Z}/16\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ or $\simeq \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ are impossible. By Proposition 2.4, the latter two cases also don't combine with a rational 3-cycle and so we have shown that in the four cases where $E(F)_{(2)} \simeq \mathbb{Z}/32\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/16\mathbb{Z} \oplus \mathbb{Z}/2^b\mathbb{Z}$ $(b = 1,2)$ or $\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ we must have $E(F)_{2'} = \{0\}$.

Now assume that $E(F)_{(2)} \simeq \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Then $E(F)_{(2)}$ contains a rational subgroup isomorphic to $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ and so, by Proposition 2.4, $E(F)_{2'}$ cannot be isomorphic to $\mathbb{Z}/5\mathbb{Z}$ or to $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$. This leaves $E(F)_{2'} \simeq \{0\}$ or $\mathbb{Z}/3\mathbb{Z}$ as the only possibilities. Finally, if $E(F)_{(2)} \simeq \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$, then $E(F)_{2'}$ cannot be isomorphic to $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$, for otherwise F would contain the 12-division field of E and hence a primitive 12th root of unity. This complete the proof of the theorem. ∎

Remarks 2.6. (a) The curves E over $\mathbb{Q}$ with $E(F)_{tors} \simeq \mathbb{Z}/15\mathbb{Z}$ are exactly the quadratic twists of the curves 50A and 50B in [MF IV, p. 86]. Indeed, the curve 50A satisfies $(50A)(\mathbb{Q})_{tors} \simeq \mathbb{Z}/5\mathbb{Z}$ and $(50A)^{(5)}(\mathbb{Q})_{tors} \simeq (50G)(\mathbb{Q})_{tors} \simeq \mathbb{Z}/3\mathbb{Z}$, and for 50B one has $(50B)(\mathbb{Q})_{tors} \simeq \mathbb{Z}/5\mathbb{Z}$ and $(50B)^{(-15)}(\mathbb{Q})_{tors} \simeq \mathbb{Z}/3\mathbb{Z}$. Therefore, if E = 50A , 50B , or a quadratic twist thereof, then $E(F)_{tors} \simeq \mathbb{Z}/15\mathbb{Z}$. Conversely, any elliptic curve E over $\mathbb{Q}$ with $E(F)_{tors} \simeq \mathbb{Z}/15\mathbb{Z}$ belongs to a rational non-cusp of $X_0(15)$. By [MF IV, p. 80] there are exactly four such points and these are accounted for by the curves 50ABCD . Direct computation shows that no quadratic twist of 50C or 50D has a rational 5-division point so that 50C and 50D , or quadratic twists

thereof, cannot have $E(F)_{tors} \simeq \mathbb{Z}/15\mathbb{Z}$.

(b) If E is an elliptic curve over $\mathbb{Q}$ with $E(\mathbb{Q})_{tors} \simeq \mathbb{Z}/9\mathbb{Z}$ or $\mathbb{Z}/7\mathbb{Z}$, then Theorem 2.5 implies that $E(F)_{tors} \simeq \mathbb{Z}/9\mathbb{Z}$ or $\mathbb{Z}/7\mathbb{Z}$, respectively. Also, if E satisfies $E(\mathbb{Q})_{tors} \simeq \mathbb{Z}/5\mathbb{Z}$ and E is not a quadratic twist of 50A or 50B (Remark (a)), then we must have $E(F)_{tors} \simeq \mathbb{Z}/5\mathbb{Z}$.

(c) To get an example with $E(F)_{tors} \simeq \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ take any elliptic curve E_1 over $\mathbb{Q}$ with $E_1(\mathbb{Q})_{tors} = \langle a \rangle \simeq \mathbb{Z}/9\mathbb{Z}$ and set $E = E_1/\langle 3a \rangle$. The curve E given by the Weierstrass equation $Y^2 = X^3 + 5805\,X - 285714$ (= 14C in [MF IV]) satisfies $E(F)_{tors} = \langle (39,0) \rangle \oplus \langle (-\frac{39}{2}+\frac{189}{2}\sqrt{-7}\,,\,0) \rangle \oplus \langle (75,756) \rangle \oplus \langle (-9,336\sqrt{-3}) \rangle \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$.

(d) Curves E over $\mathbb{Q}$ with a point of order 16 in a quadratic extension of $\mathbb{Q}$ can be obtained as follows. Take any elliptic curve E_1 over $\mathbb{Q}$ with $E_1(\mathbb{Q})_{tors} \simeq \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ and consider the $\mathbb{Q}$-isogeny $\phi : E_1 \to E = E_1/(\mathbb{Z}/2\mathbb{Z})$ and its dual ϕ' . Then $(\phi')^{-1}(\mathbb{Z}/8\mathbb{Z}) =: U \subseteq E(\overline{\mathbb{Q}})$ is cyclic of order 16 . Moreover, if $\sigma \in Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ and $e \in U$, then $\sigma(e)-e =: t_\sigma \in \ker \phi'$. Since $\ker \phi' \simeq \mathbb{Z}/2\mathbb{Z}$, $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ operates trivially on $\ker \phi'$ and the map $t : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{Z}/2\mathbb{Z}$, $\sigma \mapsto t_\sigma$ is a group homomorphism. The kernel N of t has index 2 in $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ and operates trivially on U . Therefore, $U \subseteq E(K)$ where $K = Fix_{\overline{\mathbb{Q}}}(N)$ is quadratic over $\mathbb{Q}$.

References

[Kam] S. Kamienny, Points of order p on elliptic curves over $\mathbb{Q}(\sqrt{p})$. Math. Ann. 261 (1982), 413-424.

[Kat] N.M. Katz, Galois properties of torsion points on abelian varieties. Inv. Math. 62 (1981), 481-502.

[Ke1] M.A. Kenku, Rational 2^n-torsion points on elliptic curves defined over quadratic fields. J. London Math. Soc. (2), 11 (1975), 93-98.

[Ke2] M.A. Kenku, Certain torsion points on elliptic curves defined over quadratic fields. J. London Math. Soc. (2), 19 (1979), 233-240.

[Ke3] M.A. Kenku, The modular curve $X_0(39)$ and rational isogeny. Math. Proc. Cambridge Philos. Soc. 85 (1979), no. 1, 21-23.

[Ke4] M.A. Kenku, The modular curve $X_0(169)$ and rational isogeny. J. London Math. Soc. (2), 22 (1980), 239-244.

[Ke5] M.A. Kenku, The modular curves $X_0(65)$ and $X_0(91)$ and rational isogeny. Math. Proc. Cambridge Philos. Soc. 87 (1980), no. 1, 15-20.

[Ke6] M.A. Kenku, Corrigendum: "The modular curve $X_0(169)$ and rational isogeny" [J. London Math. Soc. (2), 22 (1980), 239-244]. J. London Math. Soc. (2), 23 (1981), 428.

[Ke7] M.A. Kenku, On the modular curves $X_0(125)$, $X_1(25)$ and $X_1(49)$. J. London Math. Soc. (2), 23 (1981), 415-427.

[Ku] S.D. Kubert, Universal bounds on the torsion of elliptic curves. Proc. London Math. Soc. (3), 33 (1976), 193-237.

[La] M. Laska, Punkte auf elliptischen Kurven über $\mathbb{Q}$ in quadratischen Zahlkörpern. Max-Planck-Institut für Mathematik, Bonn, MPI/SFB 83-13.

[Man] J. Manin, The p-torsion of elliptic curves is uniformly bounded. Izv. Akad. Nauk SSSR, Ser. Mat. 33 (1969), 459-465.

[Maz] B. Mazur, Rational isogenies of prime degree. Inv. Math. 44 (1978), 129-162.

[Ri] K.A. Ribet. Torsion points of abelian varieties in cyclotomic extensions (Appendix to N.M. Katz and S. Lang, Finiteness theorems in geometric classfield theory), L'Enseignement Math. 27 (1981), 315-319.

[Se] J.P. Serre, Cohomologie Galoisienne. Lecture Notes in Math. 5 (1973), Springer Verlag.

[Shi] G. Shimura, Introduction to the Arithmetic Theory of Automorphic Functions. Publ. Math. Soc. Japan 11, Iwanomi Shoten Publishers and Princeton Univ. Press, 1971.

[Ta] J. Tate, The arithmetic of elliptic curves. Inv. Math. 23 (1974), 179-206.