TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 344, Number 1, July 1994

MINIMAL TORSION IN ISOGENY CLASSES OF ELLIPTIC CURVES

RAYMOND ROSS

Abstract. Let K be a field finitely generated over its prime field, and let $w(K)$ denote the number of roots of unity in K. If K is of characteristic 0, then there is an integer D, divisible only by those primes dividing $w(K)$, such that for any elliptic curve E/K without complex multiplication over K, there is an elliptic curve E'/K isogenous to E such that $E'(K)_{\text{tors}}$ is of order dividing D. In case K admits a real embedding, we show $D = 2$, and a nonuniform result is proved in positive characteristic.

1. Introduction and summary of results

Let K be a number field, and E an elliptic curve defined over K. The uniform boundedness conjecture, in its strong form, asserts that there is a constant C, depending only upon $[K:\mathbf{Q}]$, such that $|E(K)_{\text{tors}}|$ divides C. This result is known in case $K = \mathbf{Q}$ [8] or $[K:\mathbf{Q}] \leq 8$ [2, 3].

It is interesting and amusing to reconsider this conjecture, not for isomorphism classes over K, but instead for isogeny classes over K. A result of Katz [4, Theorem 2(bis)] provides a description of $\sup|E(K)_{\text{tors}}|$, where the supremum is taken over the (finitely many) K-isomorphism classes E/K in a fixed K-isogeny class. This description depends a priori upon the isogeny class under consideration, although of course one expects that the actual values obtained as the isogeny class varies are bounded.

Instead of investigating the existence of an upper bound for these suprema, one can ask the following easier questions: Does there exist a constant D, depending only upon K (or perhaps $[K:\mathbf{Q}]$) such that within each K-isogeny class there exists an E/K such that $|E(K)_{\text{tors}}|$ divides D? In addition, if such a D exists, what is the optimal such constant?

Let K be a field which is finitely generated over its prime field. Recall that the Mordell-Weil theorem is true for abelian varietes defined over K [9]. In particular, $E(K)_{\text{tors}}$ is finite for any elliptic curve E/K. Also, we will need the fact that, for $\operatorname{char} K \neq 2$, given an elliptic curve E/K, there are up to isomorphism over K only finitely many elliptic curves E'/K such that there is an isogeny $\psi: E \to E'$ (if $\operatorname{char} K \neq 0$, we must also require that $\operatorname{char} K$ does not divide $\deg \psi$); see [6, p. 223], for the case $\operatorname{char} K = 0$ and [11] for the case

Received by the editors January 11, 1993.

1991 *Mathematics Subject Classification*. Primary 11G05.

Resarch partially supported by NSF grant DMS-9102786.

char $K \neq 0$. For any field L, let $w(L)$ denote the number of roots of unity in L. Our main result is the following.

Theorem 1. *Suppose that K is of characteristic 0. Then there is an integer D, divisible only by those primes dividing $w(K)$, such that for any elliptic curve E/K with $\mathrm{End}_K(E) \cong \mathbf{Z}$ there is an elliptic curve E'/K isogenous to E over K such that $|E'(K)_{\mathrm{tors}}|$ divides D.*

In a special case, we can sharpen Theorem 1.

Theorem 2. *Suppose that K has a real embedding, and let E/K be an elliptic curve. Then E is isogenous over K to an elliptic curve E'/K such that $|E'(K)_{\mathrm{tors}}|$ divides* 2.

Finally, we also give a result which provides a nonuniform bound on the minimal torsion which can occur in a given isogeny class:

Theorem 3. *Let E/K be an elliptic curve, and suppose that v is a discrete valuation of K such that $v(j(E)) < 0$. Then E is isogenous over K to an elliptic curve E'/K such that $E'(K)_{\mathrm{tors}}$ is cyclic, of order dividing $\prod_{p|w(K)} p^{\mathrm{ord}_p w(K_v)}$, where K_v is the completion of K at v.*

It seems likely that one can give a unified proof of these results by using Theorem 6.7.15 of [5]; such a proof probably requires most, if not all, of the auxiliary results needed in our proofs, which are elementary.

Let p be a prime. We remark that the proofs of Theorems 2 and 3 make use of the real-analytic structure and the theory of Tate curves, respectively, to bound the power of p which can occur in $|E'(K)_{\mathrm{tors}}|$. We suspect that this is just a convenience which simplifies the arguments, and we are thus led to ask the following:

Question 1. Let E/K be an elliptic curve such that $\mathrm{End}_K(E) \cong \mathbf{Z}$. Then is E isogenous over K to an elliptic curve E'/K such that $E'(K)_{\mathrm{tors}}$ is cyclic of order dividing $w(K)$?

It is necessary that some condition be placed on $\mathrm{End}_K(E)$, as the case $K = \mathbf{F}_{p^n}$ makes clear. In §4, we examine the situation when E has complex multiplication over K. In particular, we provide an example which shows that Theorem 1 is in general false if we allow CM over K. However, under a suitable condition (that K admit a complex embedding ϕ such that $\phi(K)$ is stable under complex conjugation), versions of Theorem 1 and Question 1 can be stated which incorporate the statements above and the evidence in the CM case.

As to the question of whether the bound $w(K)$ is optimal, we have even less to say. In §2, we show that if K contains $\boldsymbol{\mu}_p$ and if $E(K)$ contains nontrivial p-torsion, then so does any elliptic curve isogenous to E over K. One can ask if more is in fact true:

Question 2. Suppose that $p^n|w(K)$. If E/K contains a K-rational point of exact order p^d with $d \leq n$, then does every elliptic curve E'/K isogenous to E over K contain a K-rational point of exact order p^d?

Speculating even further, one can ask

Question 3. Does there exist an elliptic curve E/K with $\mathrm{End}_K(E) \cong \mathbf{Z}$ such that $\inf|E'(K)_{\mathrm{tors}}| = w(K)$, where the infimum is taken over those E'/K which are isogenous to E over K?

As in Question 1, the CM case must be excluded, although in §4 we formulate a version of this question for CM elliptic curves in the special case that K admits a complex embedding under which it is conjugation-stable.

We now fix notation. If L is a field, $w(L)$ is the number of roots of unity in L (assuming of course that this is finite). Let E be an elliptic curve defined over a field K. In what follows, we shall denote by $[n]$ the multiplication-by-n map in $\mathrm{End}(E)$, the endomorphism ring of E. By $\mathrm{End}_K(E)$ we mean the subring of $\mathrm{End}(E)$ consisting of those endomorphisms defined over K. The identity element of E will be denoted by O. If A is any abelian group, we denote by $A[n]$ the elements of A annihilated by n; more generally, if $\phi\colon A \to A'$ is a homomorphism of abelian groups, we sometimes denote the kernel of ϕ by $A[\phi]$. The subgroup generated by an element g of a group G will be denoted by $\langle g\rangle$. The cardinality of a set S will be written as $|S|$. Finally, K will always denote a field which is finitely generated over its prime field.

2. Preliminary observations

Let $\phi\colon E \to E'$ be an isogeny of elliptic curves defined over K. Let $\overline{K}$ be an algebraic closure of K, and denote the Galois group of $\overline{K}$ over K by $G_{\overline{K}/K'}$. From the exact sequence of $G_{\overline{K}/K}$-modules

$$0 \to E[\phi] \to E(\overline{K})_{\mathrm{tors}} \to E'(\overline{K})_{\mathrm{tors}} \to 0$$

we obtain the cohomology exact sequence

$$\begin{aligned} 0 \longrightarrow E(K)[\phi] \longrightarrow E(K)_{\mathrm{tors}} \longrightarrow E'(K)_{\mathrm{tors}} & \\ \xrightarrow{\partial_\phi} H^1(G_{\overline{K}/K}, E[\phi]) \longrightarrow H^1(G_{\overline{K}/K}, E(\overline{K})_{\mathrm{tors}})[\phi] \longrightarrow 0. & \end{aligned}$$

From this sequence, we obtain the basic relation between the orders of the torsion subgroups of E and E':

$$|E'(K)_{\mathrm{tors}}| = \frac{|\operatorname{im}\partial_\phi|}{|E(K)[\phi]|} \cdot |E(K)_{\mathrm{tors}}|. \tag{1}$$

Equation (1) suggests that in order to "reduce" torsion, one should use isogenies with pointwise K-rational kernels. This is in fact the case. Let $\mathscr{E}$ be an isogeny class over K. Let us say that an elliptic curve $E_0/K \in \mathscr{E}$ is *minimal* if for every $E/K \in \mathscr{E}$, $|E(K)_{\mathrm{tors}}| \geq |E_0(K)_{\mathrm{tors}}|$.

Proposition 1. *Let $\phi\colon E \to E^*$ be an isogeny of elliptic curves defined over K, with E^* minimal. Then ϕ may be factored as $E \xrightarrow{\phi_0} E' \xrightarrow{\lambda} E^*$ with E' minimal and ϕ_0 a composite of isogenies each of which have pointwise K-rational kernels.*

Proof. If $\deg\phi = 1$ or E is minimal, there is nothing to show. Otherwise, one concludes from (1) that $E(K)[\phi] \neq \{O\}$. Letting $E_1 = E/E(K)[\phi]$, we may factor ϕ as $E \xrightarrow{\tilde{\phi}} E_1 \xrightarrow{\phi_1} E^*$ with $\ker\tilde{\phi} = E(K)[\phi]$ and $\deg\phi_1 < \deg\phi$. By induction, ϕ_1 has the desired form, and so therefore does ϕ. □

In case K is a number field, a more refined analysis of the map ∂_ϕ probably involves the subgroups $Ш_{\mathrm{tors}}(E/K) \subset Ш(E/K)$ and $S^{(\phi)}_{\mathrm{tors}}(E/K) \subset S^{(\phi)}(E/K)$ defined by

$$Ш_{\mathrm{tors}}(E/K) = \ker\left(H^1(G_{\overline{K}/K}, E(\overline{K})_{\mathrm{tors}}) \to \prod_{v \in M_K} H^1(G_v, E(\overline{K_v})_{\mathrm{tors}})\right)$$

and

$$S^{(\phi)}_{\mathrm{tors}} = \ker\left(H^1(G_{\overline{K}/K}, E[\phi]) \to \prod_{v \in M_K} H^1(G_v, E(\overline{K_v})_{\mathrm{tors}})\right)$$

which fit together, as usual, in the following exact sequence:

$$0 \to \operatorname{im}\partial_\phi \to S^{(\phi)}_{\mathrm{tors}}(E/K) \to Ш_{\mathrm{tors}}(E/K)[\phi] \to 0.$$

We now consider the extent to which p-torsion can be reduced in the case that K contains pth roots of unity. We will see below that, in the absence of pth roots of unity, we can always eliminate p-torsion. On the other hand, we have the following:

Proposition 2. *Suppose that K contains the pth roots of unity, and let E/K be an elliptic curve containing nontrivial p-torsion. Then every elliptic curve E'/K isogenous to E over K contains nontrivial p-torsion.*

Proof. We need only consider isogenies of p-power degree. Let $P \in E(K)$ be a point of exact order p.

Suppose first that $\phi\colon E \to E'$ is defined over K and is of degree p. If $\phi(P) \neq O$, then $\phi(P)$ is our desired point of order p on E'. Otherwise, P generates $\ker\phi$. Via the Weil pairing $\ker\phi \times \ker\hat{\phi} \to \boldsymbol{\mu}_p$, we conclude that $\ker\hat{\phi}$ and $\boldsymbol{\mu}_p$ are isomorphic as $G_{\overline{K}/K}$-modules, and so $E'(K)$ contains a point of order p.

Suppose now that $\phi\colon E \to E'$ is defined over K and is of degree p^m. If $\phi(P) \neq O$, we are done. Otherwise, we obtain a commutative diagram:

$$\begin{tikzcd}
E \arrow[r, "\phi"] \arrow[d] & E' \\
E/\langle P\rangle \arrow[ur] &
\end{tikzcd}$$

The vertical isogeny is of degree p and defined over K, so $E/\langle P\rangle$ contains a K-rational point of order p. The diagonal isogeny is of degree p^{m-1} and defined over K, and so by induction $E'(K)$ contains a point of order p. □

We now assume that p is a prime which does not divide $w(K)$. Suppose that $E(K)$ contains a point P of order p. Let $E' = E/\langle P\rangle$, and $\phi\colon E \to E'$ be the canonical map with kernel $\langle P\rangle$.

Lemma 1. *Let p be a prime $\neq \operatorname{char} K$ and not dividing $w(K)$. Suppose that $\operatorname{End}_K(E) \cong \mathbf{Z}$. If $E'(K)$ contains a point P' of order p, and $\phi'\colon E' \to$*

$E'/\langle P'\rangle = E''$ denotes the canonical map, then $\phi'\circ\phi$ is cyclic, and the elliptic curves E, E', and E'' are mutually nonisomorphic over K.

Proof. It is clear that $E \ncong E'$ over K and that $E' \ncong E''$ over K. Suppose that $E \cong E''$ over K. Then $\phi'\circ\phi \in \mathrm{End}_K(E)$, from which we conclude that $\phi'\circ\phi = [p]$. It then follows that $\phi' = \hat{\phi}$, the isogeny dual to ϕ. In particular, $\ker\hat{\phi}$ is pointwise K-rational. But this contradicts the fact that the Weil pairing $e_\phi \colon \ker\phi\times\ker\hat{\phi} \to \boldsymbol{\mu}_p$ is Galois equivariant and nondegenerate. Hence $E \ncong E''$ over K, and $\phi\circ\phi'$ is cyclic, being of order p^2. □

Lemma 2. *Let p be a prime $\neq \mathrm{char}\,K$ and not dividing $w(K)$. Let*

$$E_0 \xrightarrow{\phi_0} E_1 \xrightarrow{\phi_1} \cdots \xrightarrow{\phi_{n-2}} E_{n-1} \xrightarrow{\phi_{n-1}} E_n$$

be a sequence of elliptic curves and isogenies defined over K satisfying:

1. *The elliptic curves $E_0, \ldots, E_{n-1}$ are mutually nonisomorphic over K.*
2. $\mathrm{End}_K(E_i) \cong \mathbf{Z}$ *for $i = 0, \ldots, n$.*
3. $\ker\phi_i$ *is cyclic of order p, generated by $P_i \in E_i(K)_{\mathrm{tors}}$ for $i = 0, \ldots, n-1$.*

Then:

(a) *For $i = 0, \ldots, n-1$, let $\lambda_i = \phi_{n-1}\circ\cdots\circ\phi_i$, and choose $T_i \in E_i(\overline{K})$ as follows: $T_{n-1} = P_{n-1}$, and for $0 \le i \le n-2$, $\phi_i(T_i) = T_{i+1}$. Then* $\ker\lambda_i$ *is cyclic of order p^{n-i}, generated by T_i.*

(b) *The elliptic curves $E_0, \ldots, E_n$ are mutually nonisomorphic over K.*

Proof. For $n = 1$, (a) and (b) are clear. Assume that statements (a) and (b) are true for all such chains of length less than n. We note that it suffices to show (a). For then, λ_0 is cyclic, and we have $E_i \ncong E_j$ except possibly for $i = 0$ and $j = n$; but if $E_0 \cong E_n$ over K, then $\lambda_0 \in \mathrm{End}_K(E_0)$ is cyclic, which is impossible.

Assume that T_{i+1} generates $\ker\lambda_{i+1}$, which by induction is cyclic of order p^{n-i-1}. It is clear that $\lambda_i(T_i) = O$, and $\deg\lambda_i = p^{n-i}$. It therefore suffices to show that $[p^{n-i-1}]T_i \neq O$. So assume on the contrary that $[p^{n-i-1}]T_i = O$. First of all, $Q_i = [p^{n-i-2}]T_i \neq O$. For if not, then $O = \phi_i(Q_i) = [p^{n-i-2}]T_{i+1}$, contrary to the fact that T_{i+1} has order exactly p^{n-i-1}.

Now observe that $\{Q_i, P_i\}$ is a basis for $E_i[p]$: if $[a]Q_i + [b]P_i = O$, then $[ap^{n-i-2}]T_{i+1} = O$, whence p divides a, and so p divides b.

By Lemma 1, $\phi_{i+1}\circ\phi_i$ is cyclic of degree p^2. But $(\phi_{i+1}\circ\phi_i)(P_i) = O$, and $(\phi_{i+1}\circ\phi_i)(Q_i) = \phi_{i+1}([p^{n-i-2}]T_{i+1}) = [p^{n-i-2}]T_{i+2} = O$. So $E_i[p] \subset \ker(\phi_{i+1}\circ\phi_i)$, contrary to the cyclicity of $\phi_{i+1}\circ\phi_i$. □

Remarks. 1. A similar argument, in a more general setting, may be found in [5, Theorem 6.7.15].

2. Suppose that p^n is the exact power of p which divides $w(K)$. Then a version of Lemma 1 which involves cyclic isogenies whose kernels are pointwise rational and cyclic of order p^{n+1} is true. However, a composite of such isogenies need not be cyclic.

Proposition 3. *Let E/K be an elliptic curve such that* $\mathrm{End}_K(E) \cong \mathbf{Z}$. *Let p be a prime $\neq \mathrm{char}\,K$ and not dividing $w(K)$. Then E is isogenous over K to an elliptic curve E'/K such that p does not divide $|E'(K)_{\mathrm{tors}}|$.*

Proof. If $E(K)$ has no p-torsion, there is nothing to do. Otherwise, let $P \in E(K)$ have order p, and let $\phi: E \to E'/\langle P\rangle$ be the natural projection. If E' has no p-torsion, we are done; otherwise continue this process, thus building a sequence of cyclic p-isogenies which satisfies the hypotheses of Lemma 2. Since the number of distinct such isogenies up to isomorphism over K is finite, this process must eventually come to an end, thus producing a curve E' isogenous to E with no K-rational p-torsion. □

3. Bounding torsion

We now may state our main result.

Theorem 1. *Suppose that K is of characteristic 0. Then there is an integer D, divisible only by those primes dividing $w(K)$, such that for any elliptic curve E/K with $\mathrm{End}_K(E) \cong \mathbf{Z}$ there is an elliptic curve E'/K isogenous to E over K such that $|E'(K)_{\mathrm{tors}}|$ divides D.*

Proof. For any prime p not dividing $w(K)$, Proposition 3 affords an isogeny of p-power degree from E to an elliptic curve without p-torsion. Since such an isogeny does not affect the structure of the torsion prime to p, we may apply Proposition 3 for each p not dividing $w(K)$ to conclude that E is isogenous over K to an elliptic curve E'/K such that the only primes dividing $|E'(K)_{\mathrm{tors}}|$ are those dividing $w(K)$. Noting that Manin's local boundedness result [7] is true for elliptic curves over K then allows us to uniformly bound the exponents to which those primes divide $|E'(K)_{\mathrm{tors}}|$. □

Remark. In [7], the local boundedness theorem is proved only for number fields; for lack of a reference we indicate why it is true in this more general setting. One first notes that Manin's argument will work for any field k satisfying:

1. $X_0(n)(k)$ is finite for all n sufficiently large;
2. If $\mathrm{End}_k(E) \cong \mathbf{Z}$, then for each prime p there is a constant D_p such that for every twist E'/k of E/k, the order of a maximal cyclic p-subgroup of $E'(k)$ is $\leq D_p$.

Now suppose that k is finitely generated over $\mathbf{Q}$. Then the Mordell conjecture/Faltings theorem is true for k. (At the time of Manin's paper, the Mordell conjecture had not been proved; Manin relied on other methods, due to Demjanjenko, to establish Remark 1.)

In [7], it is shown that the statement in 2 follows from the statement that $T_pE \otimes \mathbf{Q}_p$ is an irreducible $\mathrm{Gal}(\overline{k}/k)$-module for all p [10, Theorem IV 2.1]. The proof of this result goes through for any field for which Shafarevich's theorem on the finiteness of isogeny classes is true; in particular, for fields finitely generated over $\mathbf{Q}$.

We now consider some cases in which explicit bounds can be obtained.

3.1. Real fields.

Theorem 2. *Suppose that K has a real embedding, and let E/K be an elliptic curve. Then E is isogenous over K to an elliptic curve E'/K such that $|E'(K)_{\mathrm{tors}}|$ divides 2.*

Proof. Fix an embedding of K into $\mathbf{R}$, and view E as an elliptic curve over $\mathbf{R}$. There is then a lattice $\Lambda = \mathbf{Z} + \mathbf{Z}\lambda \subset \mathbf{C}$ with $y = \mathrm{Im}\,\lambda > 0, \mathrm{Re}\,\lambda = 0$

or $\frac{1}{2}$, and a complex analytic isomorphism $\theta : \mathbf{C}/\Lambda \to E(\mathbf{C})$ defined over $\mathbf{R}$; moreover, Λ is unique and θ is determined up to multiplication by $[-1]$. In addition, $\operatorname{Re}\lambda = 0$ if and only if $E(\mathbf{R})$ has two components, in which case $E(\mathbf{R})$ corresponds via θ to

$$\{x \bmod \Lambda : x \in \mathbf{R},\ 0 \le x < 1\} \cup \{x + \tfrac{1}{2}iy \bmod \Lambda : x \in \mathbf{R},\ 0 \le x < 1\}.$$

If $\operatorname{Re}\lambda = \frac{1}{2}$, so $E(\mathbf{R})$ has one component, then $E(\mathbf{R})$ corresponds via θ to $\{x \bmod \Lambda : x \in \mathbf{R},\ 0 \le x < 1\}$.

Let $\mathscr{E}$ denote the K-isogeny class of E, and choose $E' \in \mathscr{E}$ such that $E'(\mathbf{C}) \cong \mathbf{Z}/\mathbf{Z}+\mathbf{Z}\lambda$ as above, with $\operatorname{Im}\lambda$ maximal. Observe then that $E'(\mathbf{R})^\circ$, the connected component of the identity of E', contains no nontrivial K-torsion. Indeed, suppose on the contrary that $P \in E'(K) \cap E'(\mathbf{R})^\circ$ is of order $n > 1$. Letting $E'' = E'/\langle P\rangle$, we have the following commutative diagram:

$$\begin{tikzcd} E'(\mathbf{C}) \arrow[r] & E''(\mathbf{C}) \\ \mathbf{C}/\mathbf{Z}+\mathbf{Z}\lambda \arrow[r] \arrow[u] & \mathbf{C}/\mathbf{Z}+\mathbf{Z}n\lambda \arrow[u] \end{tikzcd}$$

where the top horizontal arrow is the canonical isogeny $E' \to E'' = E'/\langle P\rangle$, the vertical arrows are the complex analytic isomorphisms mentioned above, and the bottom horizontal arrow is the map $z \bmod \mathbf{Z}+\mathbf{Z}\lambda \mapsto nz \bmod \mathbf{Z}+\mathbf{Z}n\lambda$. But this is impossible, by the maximality of $\operatorname{Im}\lambda$.

Finally, since [2] $E(\mathbf{R}) = E(\mathbf{R})^\circ$, we conclude that $|E(K)_{\mathrm{tors}}| \le 2$. □

In conjunction with Proposition 2 and the tables in [1], this result shows that for real fields, the bound of $w(K) = 2$ is optimal.

3.2. **Elliptic curves with nonintegral j-invariants.** We begin with an analysis of isogenies between Tate curves.

Let F be a field complete with respect to a discrete valuation v. By a *Tate curve over F* we mean an elliptic curve E/F with split multiplicative reduction. It is necessarily the case that $v(j(E)) < 0$. In general, given any elliptic curve E/F with $v(j(E)) < 0$, there is an extension L/F of degree at most 2 and a Tate curve E' over L such that E and E' are isomorphic over L (and if E has split multiplicative reduction, we can take $L = F$). Moreover, there is a unique $q \in F$ with $v(q) > 0$ such that we have a $\operatorname{Gal}(\overline{F}/L)$-equivariant analytic isomorphism $\psi : \overline{F}^*/q^{\mathbf{Z}} \to E(\overline{F})$, and $v(j(E)) = -v(q)$. We will refer to such an isomorphism as a *Tate parametrization.*

If E is a Tate curve over F, then $E(F) \cong F^*/q^{\mathbf{Z}}$; otherwise, $E(F) \cong \{x \bmod q^{\mathbf{Z}} : x \in L^*,\ N_{L/F}(x) \in q^{\mathbf{Z}}\}$.

We recall the following well-known fact.

Lemma 3. *Let E/F be an elliptic curve with $v(j(E)) < 0$, n an integer, and $\psi : \overline{F}/q^{\mathbf{Z}} \to E(\overline{F})$ the Tate parametrization.*

1. *If $(n, \operatorname{char} F) = 1$, then $E[n]$ is generated by $\psi(\zeta_n)$ and $\psi(q^{1/n})$, where ζ_n is a primitive nth root of unity and $q^{1/n} \in \overline{F}$ is any nth root of q.*
2. *If $p = \operatorname{char} F$, then $E[p^n]$ is generated by $\psi(q^{1/p^n})$.*

Let p be a prime. We now examine points of p-power order on E.

Lemma 4. *Let F_0 be a subfield F, and suppose that E/F_0 has nonintegral j-invariant. Suppose also that $E(F_0)$ contains a point P of exact order p^e. Let ψ be the Tate parametrization of E.*

1. *If E is a Tate curve over F and P is not a multiple of $\psi(\zeta_{p^e})$, then q has a p^eth root q^{1/p^e} in F, and $\psi(q^{1/p^e}) \in E(F_0)$.*
2. *If E is not a Tate curve over F and $e \geq 2$ if $p = 2$, then $\psi(\zeta_{p^e}) \in E(F_0)$, and $\langle P \rangle = \langle \psi(\zeta_{p^e}) \rangle$. Moreover, $e = 1$ if $p \neq 2$, and $e = 2$ if $p = 2$.*
3. *If E is not a Tate curve over F, $p = 2$, $e = 1$, and $P \neq \psi(-1)$, then $P = \psi(q^{1/2})$.*

Proof. (1) We may write $P = \psi(x \bmod q^{\mathbf{Z}})$ with $x \in F^*$ satisfying $x^{p^e} = q^r$ for some integer r, which we may assume without loss of generality satisfies $0 \leq r < p^e$. Since P is not a multiple of $\psi(\zeta_{p^e})$, we can assume further that $r \neq 0$.

Now observe that p does not divide r. For if $p|r$, then $x^{p^{e-1}} = q^{r/p} \in q^{\mathbf{Z}}$, contrary to the assumption that P has exact order p^e. Choose $r' \in \mathbf{Z}$ such that $rr' = 1 + \delta p^e$ with $\delta \in \mathbf{Z}$. Then $x^{r'p^e} = q^{1+\delta p^e}$, whence $(x^{r'}q^{-\delta})^{p^e} = q$. So $q^{1/p^e} = x^{r'}q^{-\delta}$ is a p^eth root of q, and $[r']P = \psi(x^{r'} \bmod q^{\mathbf{Z}}) = \psi(q^{1/p^e}) \in E(F_0)$ has exact order p^e.

(2) As above, we may write $P = \psi(x \bmod q^{\mathbf{Z}})$ with $x \in L^*$ satisfying $x^{p^e} = q^r$ for some integer r and $N_{L/F}(x) \in q^{\mathbf{Z}}$.

Assume that $r \neq 0$. Arguing as in (1), we conclude that q has a p^eth root $q^{1/p^e} \in L$ which satisfies $N_{L/F}(q^{1/p^e}) \in q^{\mathbf{Z}}$. Let w be the discrete valuation on L; then $w(N_{L/F}(q^{1/p^e})) = w(q^t)$ for some integer t. But then $2/p^e = t \in \mathbf{Z}$, which is impossible. Therefore, $r = 0$ and $\langle P \rangle = \langle \psi(\zeta_{p^e}) \rangle$. Since $\psi(\zeta_{p^e}) \in E(F_0)$, we have $N_{L/F}(\zeta_{p^e}) \in q^{\mathbf{Z}}$, from which we conclude that $e = 1$, unless $p = 2$, in which case $e = 2$.

(3) This follows immediately from Lemma 3. □

Remark. Note that if $p = \operatorname{char} F$ and $E(F_0)$ has a nontrivial p-power torsion point, then the proof of 2 implies that E is necessarily a Tate curve.

Lemma 5. *Let E, P, e, $F_0 \subset F$, and ψ be as in Lemma 4.*

1. *If E is a Tate curve over F and P is not a multiple of $\psi(\zeta_{p^e})$, then $E' = E/\langle P \rangle$ is defined over F_0, is a Tate curve over F, and $v(j(E')) = p^{-e}v(j(E))$.*
2. *If E is not a Tate curve over F and $P = \psi(\zeta_{p^e})$ then $E' = E/\langle P \rangle$ is defined over F_0, is not a Tate curve over F, and $v(j(E')) = p^e v(j(E))$.*
3. *If E is not a Tate curve over F, $p = 2$, $e = 1$, and $P \neq \psi(-1)$, then $E' = E/\langle P \rangle$ is defined over F_0, and $v(j(E')) = \frac{1}{2}v(j(E))$.*

Proof. In all cases, the fact that E' is defined over F_0 is obvious.

(1) By part (1) of Lemma 4, we may assume that $P = \psi(q^{1/p^e})$ with $q^{1/p^e} \in F^*$. We then have the following commutative diagram:

$$\begin{tikzcd}
1 \arrow[r] & \langle q^{1/p^e} \rangle \arrow[r] \arrow[d] & \overline{F}^*/q^{\mathbf{Z}} \arrow[r] \arrow[d, "\psi"] & \overline{F}^*/(q^{1/p^e})^{\mathbf{Z}} \arrow[r] \arrow[d, "\psi'"] & 1 \\
0 \arrow[r] & \langle P \rangle \arrow[r] & E(\overline{F}) \arrow[r] & E'(\overline{F}) \arrow[r] & 0
\end{tikzcd}$$

where ψ' completes the diagram and is a continuous $\mathrm{Gal}(\overline{F}/F)$-equivariant isomorphism. It follows that ψ' is a Tate parametrization, that E' is a Tate curve, and that $v(j(E')) = -v(q^{1/p^e}) = p^{-e}v(j(E))$.

(2) Using part (2) of Lemma 4, we obtain the following commutative diagram:

$$\begin{tikzcd}
1 \arrow[r] & \langle\zeta_{p^e}\rangle \arrow[r] \arrow[d] & \overline{F}^*/q^{\mathbf{Z}} \arrow[r, "\phi"] \arrow[d, "\psi"] & \overline{F}^*/(q^{p^e})^{\mathbf{Z}} \arrow[r] \arrow[d, "\psi'"] & 1 \\
0 \arrow[r] & \langle P\rangle \arrow[r] & E(\overline{F}) \arrow[r] & E'(\overline{F}) \arrow[r] & 0
\end{tikzcd}$$

where ψ' completes the diagram and is a $\mathrm{Gal}(\overline{F}/L)$-equivariant isomorphism. The map ϕ is $x \mapsto x^{p^e}$.

It is clear that ψ' is a Tate parameterization of E', and that $v(j(E')) = -v(q^{p^e}) = p^e v(j(E))$. Finally, if E' were a Tate curve over F, then E would be also: Since $\hat{\phi}$ has kernel $\langle q\rangle$, part (1) would imply that E is a Tate curve over F.

(3) The proof proceeds as in case (1), except that the vertical arrows need not be $\mathrm{Gal}(\overline{F}/F)$-equivariant. □

Proposition 4. *Suppose that* $\mathrm{char}\, F \neq 2$. *Let* F_0 *be a subfield of* F *which is finitely generated over its prime field, and let* p *be a prime number. Suppose that* $\boldsymbol{\mu}_{p^{d-1}} \subset F$ *but* $\boldsymbol{\mu}_{p^d} \not\subset F$. *Let* E *be an elliptic curve defined over* F_0 *with nonintegral j-invariant. Then* E *is isogenous over* F_0 *to an elliptic curve* E'/F_0 *such that the p-primary component of* $E'(F_0)_{\mathrm{tors}}$ *is cyclic of order* p^f, *with* $0 \leq f \leq d-1$.

Proof. Assume that E is a Tate curve over F. We first show that we can find an elliptic curve $\widetilde{E}/F_0$ isogenous over F_0 to E such that $j(\widetilde{E})$ is nonintegral and that the p-primary component of $\widetilde{E}(F_0)_{\mathrm{tors}}$ is annihilated by p^{d-1}.

If $E(F_0)$ has no points of order p^d, we are done. Otherwise, let $P \in E(F_0)$ be a point of exact order p^d. Since F contains no primitive p^dth roots of unity, we may apply part (1) of Lemma 4 and assume that $P = \psi(q^{1/p^d} \bmod q^{\mathbf{Z}})$. Consider then the curve $E_1 = E/\langle P\rangle$. If $E_1(F_0)$ has no points of order p^d, we are done; otherwise continue this process, thereby constructing a sequence of isogenous elliptic curves $E = E_0, E_1, \ldots, E_n$ defined over F_0 and, thanks to part (1) of Lemma 5, having nonintegral j-invariants which satisfy $-v(j(E_0)) > -v(j(E_1)) > \cdots > -v(j(E_n)) > 0$. Therefore, this process must eventually end, providing us with our desired curve $\widetilde{E}$.

We may therefore assume that the p-primary component of $E(F_0)_{\mathrm{tors}}$ is annihilated by p^{d-1}. The point $Q = \psi(\zeta_{p^{d-1}} \bmod q^{\mathbf{Z}}) \in E(F)$ has exact order p^{d-1}. If all points on $E(F_0)$ of order dividing p^{d-1} are multiples of Q, then we are done. Otherwise, $E(F_0)$ contains a point P of exact order p which is not a multiple of Q. It then follows from Lemma 3 and Lemma 4 that $q^{1/p} \in F^*$, and so we may assume without loss of generality that $P = \psi(q^{1/p} \bmod q^{\mathbf{Z}}) \in E(F_0)$ has exact order p.

Let $E_1 = E/\langle P\rangle$. By Lemma 5, we see that $v(j(E_1)) = p^{-1}v(j(E)) < 0$, and $E'(\overline{F}) \cong \overline{F}^*/(q^{1/p})^{\mathbf{Z}}$. Let $Q_1 = \psi_1(\zeta_{p^{d-1}} \bmod (q^{1/p})^{\mathbf{Z}})$, where ψ_1 is the continuous parametrization of the Tate curve E_1. The point Q_1 is of exact order p^{d-1}

on $E_1(F)$. If all points on $E_1(F_0)$ of ordering dividing p^{d-1} are multiples of Q_1, then we are done; otherwise, continue this process, thereby constructing a sequence of isogenous elliptic curves $E = E_0, E_1, \dots, E_n$ defined over F_0 with nonintegral j-invariants which satisfy $-v(j(E_0)) > -v(j(E_1)) > \cdots > -v(j(E_n)) > 0$. Therefore, this process must eventually end, providing us with our desired curve E'/F_0. We note that this argument is valid without the finiteness assumption and the characteristic restriction on F.

Suppose that E is not a Tate curve over F, and $E(F_0)$ contains points of order p^d with $d \geq 2$ if $p = 2$. By the remark following Lemma 4, we may assume that $p \neq \operatorname{char} F$. Then we apply part (2) of Lemma 5 as above to construct a sequence of elliptic curves $E_1, \dots, E_n$ defined over F_0 with $v(j(E_1)) > v(j(E_2)) > \cdots > v(j(E_n))$. The hypothesis on F_0 ensures that this process must eventually end, that is, we arrive at a curve without an F_0-rational point of order p^d.

So assume that $E(F_0)$ contains no points of order p^d. If p is odd, part (2) of Lemma 4 implies that the p-primary component of $E(F_0)$ is cyclic, of order dividing $w(F_0)$. If $p = 2$ and so $d = 2$), then this need not be the case. If $E(F_0)$ [2] is not cyclic (so $\operatorname{char} F \neq 2$), then $P = \psi(-1) \in E(F_0)$. The elliptic curve $E_1 = E/\langle P\rangle$ is not a Tate curve over F; proceeding as before we construct a sequence of elliptic curves $E_1, E_2, \dots, E_n$ defined over F_0 such that $v(j(E_1)) > v(j(E_2)) > \cdots > v(j(E_n))$. The hypothesis on F_0 ensures that this process must eventually stop, thereby producing an elliptic curve whose 2-torsion is cyclic.

The remaining case is $p = 2$ and $d = 1$; but under our hypotheses this implies that $\operatorname{char} F = 2$, which we have excluded. □

Theorem 3. *Suppose that* $\operatorname{char} K \neq 2$. *Let* E/K *be an elliptic curve, and suppose that* v *is a discrete valuation of* K *such that* $v(j(E)) < 0$. *Then* E *is isogenous over* K *to an elliptic curve* E'/K *such that* $E'(K)_{\mathrm{tors}}$ *is cyclic, of order dividing* $\prod_{p|w(K)} p^{\operatorname{ord}_p w(K_v)}$, *where* K_v *is the completion of* K *at* v.

Proof. Let l denote the multiplicative characteristic of K, so $l = \operatorname{char} K$ if K is of positive characteristic, and $l = 1$ otherwise. By virtue of Proposition 3, we may assume that the only primes dividing $|E(K)_{\mathrm{tors}}|$ are those dividing $lw(K)$. Embed K into its completion K_v; applying Proposition 4 to each prime dividing $lw(K_v)$ yields the theorem. □

4. Elliptic curves with complex multiplication

Let K be a number field, $k \subset K$ a quadratic imaginary field, and $\mathscr{E}$ a K-isogeny class of elliptic curves admitting complex multiplication by k, so that in particular, $\operatorname{End}(E) = \operatorname{End}_K(E)$ is isomorphic to an order in k, which we identify with $\operatorname{End}(E)$. Put

$$\mathscr{O}_{\mathscr{E}} = \bigcap_{E \in \mathscr{E}} \operatorname{End}(E);$$

note that $\mathscr{O}_{\mathscr{E}}$ is an order in k.

Let χ be the Hecke character attached to $\mathscr{E}$, and let $\mathfrak{f}$ be its conductor. We view χ as a homomorphism $I_K(\mathfrak{f}) \to k^*$, with $I_K(\mathfrak{f})$ denoting the group of fractional ideals of K relatively prime to $\mathfrak{f}$. Let $\sigma(-, K^{\mathrm{ab}}/K)$ denote the Artin symbol, with K^{ab} denoting the maximal abelian extension of K. The main theorem of complex multiplication, together with the isogeny invariance of χ, implies that for all $E \in \mathscr{E}$ and all $T \in E(\overline{K})$ of annihilator $\mathfrak{n}_T \subset \mathrm{End}(E)$,

$$T^{\sigma(\mathfrak{P}, K^{\mathrm{ab}}/K)} = \chi(\mathfrak{P})T \tag{2}$$

for all prime ideals $\mathfrak{P}$ of K not dividing $\mathfrak{f}\mathfrak{n}_T\mathscr{O}_K$. In particular, $\chi(\mathfrak{P}) \in \mathscr{O}_{\mathscr{E}}$.

Now suppose that there is an $E \in \mathscr{E}$ such that $E(K)$ contains a point T of exact order p^n. Let $\mathfrak{n}_T$ denote the annihilator ideal of T in $\mathrm{End}(E)$. Formula (2) implies that for all prime ideals $\mathfrak{P} \subset \mathscr{O}_K$ which do not divide $\mathfrak{f}\mathfrak{n}_T\mathscr{O}_K$, the Hecke character satisfies the congruence $\chi(\mathfrak{P}) \equiv 1 \bmod \mathfrak{n}$, where $\mathfrak{n} = \mathfrak{n}_T \cap \mathscr{O}_{\mathscr{E}}$. Note that $p^n \in \mathfrak{n}$.

For each $E' \in \mathscr{E}$, let $\mathfrak{n}' = \mathfrak{n}\,\mathrm{End}(E')$. Formula (2) and the congruence condition satisfied by χ imply that $\sigma(\mathfrak{P}, \overline{K}/K)$ fixes $E'[\mathfrak{n}']$ pointwise for all prime ideals $\mathfrak{P}$ of $\mathscr{O}_K$ not dividing $\mathfrak{f}\mathfrak{n}'\mathscr{O}_K$. Čebotarev density then implies that $E'[\mathfrak{n}'] \subset E'(K)$. In particular, $E'(K)$ contains a point of exact order p^n.

Example. In this example, we show that in the CM case, every curve in a given isogeny class over K can have a point of order p^n, even though the field K does not contain the p^nth roots of unity. From the discussion above, it suffices to produce a single elliptic curve over K with CM and a point of order p^n.

Let $E/\mathbf{Q}$ have CM by the ring of integers in a quadratic imaginary field k. Let $p \neq 2, 3$ be a prime which splits in k and at which E has good reduction; to fix ideas, write $p\mathscr{O}_k = \mathfrak{p}\mathfrak{p}'$. Put $K = k(E[\mathfrak{p}^n])$, and now view E as an elliptic curve over K. Certainly $E(K)$ contains points of exact order p^n. It is well known that K/k is unramified away from $\mathfrak{p}\Delta_{E/K}$. It follows that K does not contain the p^nth roots of unity, since otherwise K/k would be ramified above $\mathfrak{p}'$, which does not divide $\mathfrak{p}\Delta_{E/K}$.

Let us say that an isogeny class $\mathscr{E}$ (with or without CM) is *m-exceptional* if every $E/K \in K \in \mathscr{E}$ has a K-rational point of order m but K does not contain the mth roots of unity. We have just seen that if p splits in k, then there can be p^n-exceptional isogeny classes, with n arbitrarily large. We note that this cannot happen if p does not split in k.

To see this, note first that from the discussion above, it suffices to bound p-power torsion for a single elliptic curve in the given isogeny class. We will always choose a curve $E/K \in \mathscr{E}$ with CM by the full ring of integers of k.

Consider first the case where p is inert. If $P \in E(K)$ has exact order p^n, then $E[p^n] \subset E(K)$, since P generates $E[p^n]$ as an $\mathscr{O}_k/p^n\mathscr{O}_k$-module. It follows that K contains the p^nth roots of unity.

If p ramifies in k and $E(K)$ contains a point P of exact order p^n, then K contains the p^{n-1}th roots of unity. For, letting $\mathfrak{p}^2 = p\mathscr{O}_k$, we see that $\mathfrak{p}^{2n-1}$ divides the annihilator of P. The theory of complex multiplication then implies that K contains the ray class field of k of conductor $\mathfrak{p}^{2n-1}$. Since $\mathfrak{p}^{2n-1} = \mathfrak{p}p^{n-1}\mathscr{O}_k$, we can conclude that K contains the ray class field of k of conductor p^{n-1}, and this field contains the p^{n-1}th roots of unity.

Under a mild assumption on K, we can obtain some control on the p^n-torsion in an isogeny class even when p splits in k.

Proposition 5. *Let E be an elliptic curve over K with complex multiplication over K. Suppose K admits a complex embedding ϕ such that $\phi(K) = \overline{\phi}(K)$. If*

p^n does not divide $w(K)$, then $E(K)_{\text{tors}}$ contains no points of order $p^{n+e(p)-1}$, where $e(p)$ denotes the ramification index of p in $\mathcal{O}_k$.

Proof. We may assume that E has CM by the full ring of integers of k. If p does not split in k, then we see from the discussion above that the result is true with no additional hypotheses on K. Therefore we may assume that $p\mathcal{O}_k = \mathfrak{p}\mathfrak{p}'$. Identify K with its image $\phi(K) \subset \mathbf{C}$, so we have $k \subset K \subset \mathbf{C}$. Suppose that $P \in E(K)$ has exact order p^n; without loss of generality we may assume that the annihilator of P is $\mathfrak{p}^n\mathfrak{p}'^\nu$ with $\nu \le n-1$. Let h_E be the Weber function on E, and denote by $k(\mathfrak{c})$ the ray class field of k of conductor $\mathfrak{c}$.

The theory of complex multiplication implies that

$$k(j(E), h_E(P)) = k(\mathfrak{p}^n\mathfrak{p}'^\nu) \subset K.$$

Using the conjugation-invariance of both k and K, we see that

$$k(j(\overline{E}), h_{\overline{E}}(\overline{P})) = k(\mathfrak{p}'^n\mathfrak{p}^\nu) \subset K,$$

since the annihilator of $\overline{P}$ is $\mathfrak{p}'^n\mathfrak{p}^\nu$ (the bar denotes complex conjugation). We therefore obtain that

$$k(p^n) \subset k(\mathfrak{p}^n\mathfrak{p}'^\nu)k(\mathfrak{p}'^n\mathfrak{p}^\nu) \subset K,$$

from which we conclude that $\boldsymbol{\mu}_{p^n} \subset K$. □

In light of this result, we can state a modified version of Question 1.

Question 4. Let K be a number field, E/K an elliptic curve, and $\mathcal{O}$ the maximal order in $\operatorname{End}_K(E)\otimes\mathbf{Q}$. Suppose further that K admits a complex embedding ϕ such that $\phi(K) = \overline{\phi}(K)$. Then is E isogenous over K to an elliptic curve E'/K such that $E'(K)_{\text{tors}}$ is cyclic of order dividing

$$\prod_{p \mid w(K)} p^{\operatorname{ord}_p w(K)+e(p)-1},$$

where $e(p)$ is the ramification index of p in $\mathcal{O}$?

We now turn to a version of Question 2 which incorporates the CM case. Being somewhat suspicious about the presence of the ramification indices for those primes which ramify in $\mathcal{O}$, we stay on the safe side and pose the following:

Question 5. Let K, $\mathcal{O}$, and $e(p)$ be as in the conjecture above. Does there exist an elliptic curve E/K such that $w(K) \mid \inf|E'(K)_{\text{tors}}| \mid \prod_{p\mid w(K)} p^{\operatorname{ord}_p w(K)+e(p)-1}$, where the infimum is taken over all E'/K which are isogenous to E over K?

References

1. B. Birch and W. Kuyk, Editors, *Modular functions of one variable.* IV, Lecture Notes in Math., vol. 476, Springer-Verlag, Berlin and New York, 1975.
2. S. Kamienny, *Torsion points on elliptic curves and q-coefficients of modular forms*, Invent. Math. **109** (1992), 221–229.
3. S. Kamienny and B. Mazur, *Rational torsion of prime order in elliptic curves over number fields*, preprint, 1992.
4. N. Katz, *Galois properties of torsion points on abelian varieties*, Invent. Math. **62** (1981), 481–502.
5. N. Katz and B. Mazur, *Arithmetic moduli of elliptic curves*, Ann. of Math. Stud., no. 108, Princeton Univ. Press, Princeton, NJ, 1985.

6. S. Lang, *Elliptic functions*, Addison-Wesley, Reading, MA, 1973.

7. Ju. Manin, *The p-torsion of elliptic curves is uniformly bounded*, Izv. Akad. Nauk SSSR **33** (1969), 433–438.

8. B. Mazur, *Rational isogenies of prime degree*, Invent. Math. **44** (1978), 129–162.

9. A. Néron, *Problèmes arithmétiques et géométriques attachés à la notion de rang d'une courbe algébrique dans un corps*, Bull. Soc. Math. France **80** (1952), 101–166.

10. J.-P. Serre, *Abelian l-adic representations and elliptic curves*, Benjamin, New York, 1968.

11. Yu. G. Zarhin, *Abelian varieties in characteristic p*, Math. Notes **19** (1976), 240–246.

Department of Mathematics, Louisiana State University, Baton Rouge, Louisiana 70803-4918

E-mail address: ross@math.lsu.edu