Mathematical Research Letters **10**, 847–865 (2003)

SINGULAR TORSION POINTS ON ELLIPTIC CURVES

John Boxall and David Grant

Introduction

Let k be a perfect field and $\overline{k}$ an algebraic closure of k. We write Γ_k for the Galois group of $\overline{k}$ over k. Let G be a commutative algebraic group over k. We write the group law of G additively and denote the origin of G by O. For each integer n we denote by $[n]$ the multiplication-by-n map on G, by $G[n]$ the subgroup of points of $G(\overline{k})$ of order dividing n, and by $G[n]^*$ the subset of $G(\overline{k})$ of points of order n. We write $G_{\rm tors}$ for the group of all torsion points of $G(\overline{k})$. If Ω is a set of prime numbers, we let G_Ω denote the subgroup of $G_{\rm tors}$ consisting of points whose order is divisible only by primes in Ω.

We now recall the definition of a *singular torsion point* on an elliptic curve E over k, as given in [5]. Suppose the characteristic of k is not 2, and that $n \geq 1$ is an integer. We say that $P \in E[n]$ is a *singular n-torsion point* if for any local parameter t at O satisfying $[-1]^*t = -t$, any function $f_P \in \overline{k}(E)$ (defined up to constant multiples) with divisor $n(P - O)$ has a Laurent expansion at O of the form

$$f_P = \frac{a}{t^n} + O\Big(\frac{1}{t^{n-2}}\Big), \qquad a \neq 0,$$

(i.e., the coefficient of $\frac{1}{t^{n-1}}$ vanishes). We say that $P \in E_{\rm tors}$ is a *singular torsion point* if P is a singular n-torsion point when n is the order of P. We denote the set of all singular torsion points by $E_{\rm sing}$.

When k has characteristic zero, $E_{\rm sing}$ is a finite set. Indeed, by an easy specialization argument, it suffices to consider the case when k is a number field. As explained in [5], if J_m is the generalized Jacobian of E with modulus $m = 2O$, and $s : E \to J_m$ is the map that takes $P \in E(\overline{k})$ to the point in $J_m(\overline{k})$ representing the class of $P - O + (t)$, then $E_{\rm sing} = s^{-1}(s(E) \cap J_{m,{\rm tors}})$, so the finiteness of $E_{\rm sing}$ follows using a result of Hindry [14] which shows that $s(E) \cap J_{m,{\rm tors}}$ is finite. Singular torsion points are an elliptic curve analogue of torsion packets on jacobians (see for example [10]).

The purpose of the present paper is to show that for elliptic curves over number fields, the set of singular torsion points can be effectively determined, by showing that their orders can be effectively bounded in a strong way (see Corollaries D and E below). We also provide proofs of results announced at the

Received June 11, 2003.
Key words and phrases. Elliptic curves, torsion points.
2000 *Mathematics Subject Classification.* 11G05, 11G07, 14L10.

end of [5] (see Corollary B and Proposition C below). Before stating our results, we need some further definitions.

Definition 0.1. *Let Σ be a subset of $G(\overline{k})$. We say that Σ is geometrically-rigid if whenever $P, Q, R, S \in \Sigma$, then*

$$P + Q = R + S$$

implies that $P = R, S$, or $-Q$. If in addition Σ is Γ_k-invariant, we call Σ a Galois-invariant, geometrically-rigid, or GIGR (pronounced "Geiger") set of points.

We will see in section 2 that if the characteristic of k is not 2, then $E_{\text{sing}} - E[2]$ is a GIGR set.

Recall that Ribet defines $P \in G(\overline{k})$ to be *almost rational* [22] (see also [3]) if, whenever σ and $\tau \in \Gamma_k$ are such that $\sigma(P)+\tau(P) = 2P$, then $\sigma(P) = \tau(P) = P$. Note that all points of order at least 3 in a GIGR set (and hence singular torsion points of order at least 3) are almost rational. Ribet has proved that on an abelian variety defined over a number field, there are only finitely many almost rational torsion points. This gives a second proof that E_{sing} is finite when k has characteristic 0.

In what follows, we first study E_{sing} when E is defined over a finite extension of $\mathbb{Q}_p$, and then deduce that when E is defined over a number field, the orders of points in E_{sing} can be bounded depending only on the degree of the field. We normalize the p-adic valuation so that $\text{ord}_p(p) = 1$.

It is easy to see that points of order 2 are singular torsion (see Proposition 1.2 (*ii*)). We prove the following results.

Theorem A. *Let p be a prime number and let E be an elliptic curve over a finite extension K of $\mathbb{Q}_p$. Let e_K denote the ramification degree of K over $\mathbb{Q}_p$. Let $N \geq 3$ be an integer and suppose that E_{sing} contains a point of order N.*

(i) *Suppose E has potential multiplicative reduction, and let a be the largest integer such that K contains a primitive p^a-th root of unity. Then if p is odd, $\text{ord}_p(N) \leq a$, and if $p = 2$, $\text{ord}_2(N) \leq a + 1$. In particular, if $p \geq 3$ and $e_K < p - 1$, then $\text{ord}_p(N) = 0$, and if $p = 2$ and $e_K = 1$, then $\text{ord}_2(N) \leq 2$.*

(ii) *Suppose E has good reduction. If $p \geq 3$ and $e_K < p-1$, then $\text{ord}_p(N) \leq 1$. If $p = 2$ and $e_K = 1$, then $\text{ord}_2(N) \leq 3$.*

(iii) *If r is a positive integer, define $M(r)$ to be the largest real zero of the function*

$$f_r(x) = x^2 - r(r^2 - r + 6)x - 4(r - 1)(r - 2)x^{1/2} + 3(r^3 + r^2 + 1).$$

If E has good reduction, if $p \geq 3$ and if $p > M(e_K)$, then p does not divide N. Noting that $M(1) = 3$, we see in particular that if E has good reduction, $p \geq 5$, and $e_K = 1$, then p does not divide N.

A calculation shows that $M(2) = 13$, and that if $r = 3, 4, 5, 6$ then the smallest integer greater than $M(r)$ is respectively 35, 72, 131, 218. Furthermore, if $r \geq 7$, then $r^3 - r^2 < M(r) < r^3$. This implies in particular that

$$M(r+1) > M(r) \geq 2r + 1 > r + 1, \tag{1}$$

for all $r \geq 1$.

We note the following corollary to Theorem A stated in [5].

Corollary B. *Let E be a semistable elliptic curve defined over a number field K. Let Ω contain the set of primes 2, 3, and those p such that every prime of K over p is either ramified or a prime of bad reduction. Then $E_{\mathrm{sing}} \subseteq E_\Omega$.*

To get an effective determination of E_{sing}, we apply the following for elliptic curves over number fields.

For a prime ℓ, set $\delta = \delta(\ell) = 1$ when ℓ is odd, and $\delta(2) = 2$.

Proposition C. *Let k be a perfect field, G be a commutative algebraic group over k, Σ be the set of almost rational torsion points of $G(\overline{k})$, and let Ω be a finite set of primes. Define $L = \prod_{\ell \in \Omega} \ell^{\delta(\ell)}$. Let $k_1 = k(G[L])$, and suppose that there exist an integer M, divisible only by primes in Ω, such that $G(k_1) \cap G_\Omega \subseteq G[M]$. Then $\Sigma \cap G_\Omega \subseteq G[M]$.*

Note that such an M exists if G is a semi-abelian variety and k is a finite field, or a finite extension of $\mathbb{Q}$ or $\mathbb{Q}_p$. In this case, the result shows that the intersection of the set of almost rational torsion points — and hence the intersection with any GIGR set of torsion points — with G_Ω can, in principle, be effectively determined.

Here is another consequence of Theorem A and Proposition C.

Corollary D. *Let $d \geq 1$ be an integer. Then there exists an explicit integer N_d, such that for any elliptic curve E defined over a number field of degree at most d, we have $E_{\mathrm{sing}} \subseteq E[N_d]$.*

To see this, we recall that any elliptic curve E over a finite extension F of $\mathbb{Q}$ acquires semistable reduction over $F(E[12])$, which is an extension of F of degree at most $\#\big(GL_2(\mathbb{Z}/12\mathbb{Z})\big) = 2^9 \cdot 3^2$. Thus, replacing F by $F(E[12])$ if necessary, we can assume without loss of generality that E is a semistable elliptic curve defined over a number field F of degree at most d. We claim that the set Ω of primes which divide the order of singular torsion points is now bounded in terms of d. Indeed, if $p > M(d)$, then by (1), $p > d + 1$ and p is odd. Hence, if e is the absolute ramification degree of any prime of F, then by (1), $p > M(e) > e + 1$, and so $p \notin \Omega$. Now if Ω contains only primes lying below primes of F of potential multiplicative reduction, and N is the order of a singular torsion point, then Theorem A (i) bounds $\mathrm{ord}_p(N)$ for all $p \in \Omega$ in terms of d. So suppose now that Ω contains a prime below a prime $\mathfrak{p}$ of F of good reduction. Since the primes in Ω are bounded in terms of d, we deduce from Proposition C that the degree of $F' = F(E[L])$ is bounded only in terms

of d. Then $E_\Omega(F')$ can be bounded in terms of d by applying the Corollary on page 30 of [12] to a prime of F' above $\mathfrak{p}$.

Corollary E. *If E is a semistable elliptic curve over $\mathbb{Q}$, then $E_{\mathrm{sing}} \subseteq E[24]$.*

Indeed, Theorem A (*i*) and (*iii*) show in this case that if $p > 3$, then p does not divide the order N of a singular torsion point. Then (*i*) and (*ii*) give that $\mathrm{ord}_3(N) \leq 1$ and $\mathrm{ord}_2(N) \leq 3$. It is worth comparing this with a result of Calegari [9], who proved that if E is a semistable elliptic curve over $\mathbb{Q}$, then every almost rational torsion point is either rational or of order dividing $2^4 \cdot 3^3$ (see Theorem 1.2 of [9] for a more precise statement).

To summarize the proof of Theorem A, let E be an elliptic curve over K and let $P \in E_{\mathrm{sing}}$ be of order $N \geq 3$. Our purpose is to bound $\mathrm{ord}_p(N)$. To do this, we study separately the cases of potential multiplicative, good ordinary and supersingular reduction. In the case of multiplicative reduction, we reformulate the definition of singular torsion in terms of zeros of p-adic theta functions, and prove that these theta functions cannot have zeros at torsion points satisfying appropriate hypotheses. When the reduction is ordinary, there are two cases according as to whether the order of the reduction of P is strictly less than that of P or not. When the order doesn't decrease, we use the non-existence of singular torsion points of order a multiple of p over a field of characteristic $p \geq 3$. When the order does decrease, we use formal group arguments. Throughout the proof, extensive use is made of the action of Γ_K and various inertia subgroups on the torsion points of E, in the spirit of Lang [16] or Serre [23]. (For applications of similar ideas to torsion packets on quotients of Fermat curves and modular curves, see [1], [2], [3], [11], [26] and the survey [27].)

The paper consists of four sections. In the first, we review some simple properties of singular torsion points. In the second, we check that $E_{\mathrm{sing}} - E[2]$ is a GIGR set and study almost rational torsion points. In particular, we prove Proposition C and some related results, using ideas from [4] that simplify in the situation at hand. Proposition C generalizes Proposition 12 of [5], whose proof we promised to give in the present paper. Section 3 contains a proof Theorem A (*i*). In the final section, we prove the remaining assertions of Theorem A.

Acknowledgements. We would like to thank Matt Baker and Frank Calegari for drawing our attention to the notion of an almost rational point. This paper was completed while the first author was enjoying the hospitality of the University of Colorado at Boulder.

1. Preliminaries

We use the same notation as in the Introduction. However, for technical reasons, we want to extend the definition of singular torsion to ordinary elliptic curves in characteristic two. From a geometric point of view this definition is not very satisfying, and many of the basic properties of singular torsion points detailed below do not hold in characteristic two, but the ad hoc definition below will suffice for our purposes.

So, let E be an elliptic over a field k (of arbitrary characteristic). Let

$$y^2 + (a_1x + a_3)y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in k, \tag{2}$$

be a Weierstrass model of E. Then $[-1]^*x = x$, and $[-1]^*y = -y - a_1x - a_3$. If t is a local parameter at the origin, then $[-1]^*t$ is also a local parameter at the origin, and there exists $\alpha_t \in k$ such that $[-1]^*t = -t + \alpha_t t^2 + O(t^3)$ in the local ring at O. If s is a second local parameter at O, then there exist b, $c \in k$ with $b \neq 0$ and $s = bt + ct^2 + O(t^3)$. Therefore

$$\alpha_s = \frac{\alpha_t}{b} + \frac{2c}{b^2}. \tag{3}$$

From now on, if $P \in E[n] - \{O\}$, we denote by f_P a function with divisor $n(P - O)$. When k is of characteristic $\neq 2$, one finds that $P \in E[n]$ is a singular n-torsion point if and only if, for any local parameter t at O, we have, up to a multiplicative constant, an expansion

$$f_P = \frac{1}{t^n} + \frac{n}{2}\frac{\alpha_t}{t^{n-1}} + O\Big(\frac{1}{t^{n-2}}\Big). \tag{4}$$

When the characteristic of k is 2, we can use (4) to define a singular n-torsion point provided n is even. However, taking $t = \frac{x}{y}$ with x and y as in (2), we find that $\alpha_t = a_1$, which vanishes if and only if E is supersingular. Then, using (3), we see that E is supersingular if and only if $\alpha_s = 0$ for all local parameters s at O, and that E is ordinary if and only if $\alpha_s \neq 0$ for all s. It is for this reason that we restrict attention to ordinary elliptic curves in characteristic 2.

Definition 1.1. *Let k be a field, let E be an elliptic curve over k, and let $n \geq 1$ be an integer. If k is of characteristic two, we suppose E ordinary and n even. If $P \in E[n] - \{O\}$, we say that P is a* singular n-torsion point *if f_P satisfies* (4) *for all local parameters t at O. We say that P is a* singular torsion point *if it is a singular n-torsion point when n is the order of P.*

As just indicated, when k is of characteristic $\neq 2$, this definition is equivalent to the previous one. Note that in any characteristic, (3) implies that to show that $P \in E[n]$ is singular n-torsion, it suffices to check (4) for any local parameter t at O.

As before, we denote by E_{sing} the set of all singular torsion points of E.

If t is a local parameter at O, we say that f_P is *normalized* (with respect to t) if $f_P = \frac{1}{t^n} + O\big(\frac{1}{t^{n-1}}\big)$. Once a Weierstrass model (2) of E has been chosen, we usually take $t = \frac{x}{y}$ as local parameter, and normalized will mean normalized with respect to this choice of t.

Proposition 1.2. *Let E be an elliptic curve over k, and let $n > 1$, $m \geq 1$, be integers.*

(i) *If $P \in E[n]$, and $P \neq O$ is singular n-torsion, then P is singular mn-torsion.*

(ii) *We have $E[2]^* \subseteq E_{\text{sing}}$.*

Proof. (*i*) Suppose d is the precise order of P. Then the function $f_P^{\frac{mn}{d}}$ has divisor $mn(P-O)$. By hypothesis $f_P^{n/d} = \frac{1}{t^n} + \frac{n}{2}\frac{\alpha_t}{t^{n-1}} + O\big(\frac{1}{t^{n-2}}\big)$, and developing $f_P^{\frac{mn}{d}}$ by the binomial theorem gives the result.

(*ii*) Let E be defined as in (2), and take $t = x/y$. Then $x = \frac{1}{t^2} + \frac{a_1}{t} + O(1)$, and $f_P = x - x(P)$. The result thus follows from Definition 1.1. □

Similarly, one sees easily that if $P \in E[n]$, and $P \neq O$ is singular mn-torsion, that when m is prime to the characteristic of k, then P is singular n-torsion. Also, if $\operatorname{char} k = p > 0$, and if $P \in E[n]$ and $P \neq O$, then P is always singular np-torsion.

Proposition 1.3. *Let k be a field of characteristic $p \geq 2$, and let E be an elliptic curve over k.*

(i) *If $p \geq 3$, then for all integers $n \geq 1$, $E[pn]^* \cap E_{\text{sing}} = \emptyset$.*
(ii) *If $p = 2$, then for all integers $n \geq 1$, $E[4n]^* \cap E_{\text{sing}} = \emptyset$.*

Proof. If E is supersingular, then $E[np]^*$ is empty for all $n \geq 1$ and there is nothing to prove. So suppose that E is ordinary and let $P \in E[np]^*$, and if $p = 2$ we suppose n is even. Let t be a parameter at the origin. We want to show for f_P normalized, if $f_P = \frac{1}{t^{np}} + \frac{A}{t^{np-1}} + O\big(\frac{1}{t^{np-2}}\big)$, then $A \neq 0$. To do this, we recall the basic fact that $\omega = df_P/f_P$ is a non-trivial holomorphic differential on E. Further, a calculation shows that $\omega = (A + O(t))dt$, and on an elliptic curve a non-trivial differential has no zeros, so $A \neq 0$. □

Now let p be a prime and suppose that $\overline{\mathbb{Q}}_p$ is a fixed algebraic closure of $\mathbb{Q}_p$. Let $\mathcal{O}$ be the valuation ring of $\overline{\mathbb{Q}}_p$ and k its residue field. When E has good reduction, we choose a Weierstrass model (2) of E with coefficients in $\mathcal{O}$ and such that the cubic over k obtained by reducing the coefficients is a Weierstrass model of the reduced elliptic curve $\tilde{E}$. In general, we denote by $\tilde{X}$ the reduction to k or to $\tilde{E}$ of some object X associated to $\mathcal{O}$ or to E, such as a polynomial over $\mathcal{O}$ or a point of $E(\overline{\mathbb{Q}}_p)$.

Lemma 1.4. *Let E be an elliptic curve over $\overline{\mathbb{Q}}_p$ with good reduction, and let $P \in E_{\text{tors}}$ be such that $\tilde{P} \neq \tilde{O}$. Let $n > 1$ be the order of P and $d \neq n$ the divisor of n such that $\tilde{P}$ is of order $\frac{n}{d}$.*

(i) *If f_P is normalized, we have $f_P \in \mathcal{O}[x, y]$ and $\tilde{f}_P = f_{\tilde{P}}^d$, where $f_{\tilde{P}}$ is the normalized function with divisor $\frac{n}{d}(\tilde{P} - \tilde{O})$.*
(ii) *If $d = 1$ and if $P \in E_{\text{sing}}$, then $\tilde{P} \in \tilde{E}_{\text{sing}}$.*

Proof. (*i*) Note that E and P are defined over some finite extension L of $\mathbb{Q}_p$, with ring of integers $\mathcal{O}_L$ and uniformizer π. Since O is the only pole of f_P, we certainly have $f_P \in L[x, y]$. By the hypotheses on P and $\tilde{P}$, we have $\big(x(P), y(P)\big) \in \mathcal{O}_L^2$. Hence, changing models we can suppose $\big(x(P), y(P)\big) = (0, 0)$, so that $a_6 = 0$. We first suppose that $\tilde{P}$ is not a two-torsion point. Hence $\tilde{a}_3 \in (\mathcal{O}_L/\pi)^*$, and so a_3 is a unit of $\mathcal{O}_L$. Then x is a local parameter at P, and we can develop y as a formal power series $y = a_3^{-1}x(a_4 + \cdots)$ that actually lies in $x\mathcal{O}_L[[x]]$.

Write $f_P = U(x) + yV(x)$ with U, V polynomials in $L[x]$. Then f_P has a bounded denominator as an element of $L[[x]]$, and the same is true of f_{-P}. Since $f_P f_{-P} = x^n$, Gauss's Lemma gives that $f_P, f_{-P} \in \mathcal{O}_L[[x]]$. Since $f_{-P} = U(x) + (-y - a_1x - a_3)V(x)$, subtracting f_{-P} from f_P gives $(2y + a_1x + a_3)V(x) \in \mathcal{O}_L[[x]]$, hence since $a_3 + a_1x + 2y$ is invertible, that $V(x) \in \mathcal{O}_L[[x]] \cap L[x] = \mathcal{O}_L[x]$. Our formula for f_P implies that $U(x) \in \mathcal{O}_L[[x]] \cap L[x] = \mathcal{O}_L[x]$, as well.

To deduce the second assertion, one notes that $\tilde{f}_P$ is clearly normalized, and its polar divisor is $n\tilde{O}$. But since the degree of the divisor of zeros can only increase with specialization, it is of the form $n\tilde{P} + D$, with D positive and with support not containing $\tilde{O}$. But then $D = 0$ since the divisor of a function is of degree 0. So comparing divisors on $\tilde{E}$ gives $\tilde{f}_P = c f_{\tilde{P}}^d$ for some $c \in k^*$. Then $c = 1$ since $\tilde{f}_P$ and $f_{\tilde{P}}$ are normalized. The case where $\tilde{P}$ is a two-torsion point is similar, but in that case we use that $\tilde{a}_4 \neq 0$ and that y is a local parameter at P.

(*ii*) Since $f_P \in \mathcal{O}[x, y]$ by (*i*) and $x \in \mathcal{O}((t))$, $y \in \mathcal{O}((t))$, we have $f_P \in \mathcal{O}((t))$ and $f_{\tilde{P}} \in k((t))$ is obtained by reducing the coefficients of f_P. The assertion is now clear. □

Remark. More generally, keeping to the notations of Lemma 1.4, we find that if $f \in \overline{\mathbb{Q}}_p(E)$ is a function whose divisor is of the form $\sum_i n_i P_i - nO$, the P_i being distinct non-zero torsion points of E none of which reduce to $\tilde{O}$, and if $f = \frac{1}{t^n} + O\big(\frac{1}{t^{n-1}}\big)$ at O, then $f \in \mathcal{O}[x, y]$ and the divisor of $\tilde{f}$ is $\sum_i n_i \tilde{P}_i - n\tilde{O}$. This follows at once from Lemma 1.4, since some power of f is a product of powers of the normalized f_{P_i}'s, and $\mathcal{O}[x, y]$ is a normal ring.

For a point P on E, we let $\bar{P} = -P$.

Proposition 1.5. *Let p be a prime, let E be an elliptic curve over $\overline{\mathbb{Q}}_p$ with ordinary reduction, and let $m \geq 1$ be an integer.*

(i) *Let $p \geq 3$ and let $P \in E[pm]^*$ be such that $\tilde{P} \in \tilde{E}[pm]^*$. Then $P \notin E_{\text{sing}}$.*
(ii) *Let $p = 2$ and let $P \in E[4m]^*$ be such that $\tilde{P} \in \tilde{E}[4m]^*$. Then $P \notin E_{\text{sing}}$.*
(iii) *Let $p = 2$ and let $P \in E[8m]^*$ be such that $\tilde{P} \in \tilde{E}[4m]^*$. Then $P \notin E_{\text{sing}}$.*

Proof. (*i*) and (*ii*). These follow directly from Lemma 1.4 (*ii*) and Proposition 1.3.

(*iii*) We can assume that $\tilde{E}$ is ordinary and fix a model (2) where now a_1 is a unit of $\mathcal{O}$, and take $t = \frac{x}{y}$. Write $S = [2m]P$, so that S is of order 4 and $\tilde{S}$ of order 2. Let g be a function with divisor $2mP + \bar{S} - (2m + 1)O$, which we can suppose normalized by the condition $g = \frac{1}{t^{2m+1}} + \frac{A}{t^{2m}} + O\big(\frac{1}{t^{2m-1}}\big)$. Then $g^4 = f_P f_{-S}$, so that $g \in \mathcal{O}[x, y]$ by Lemma 1.4 (*i*), and so $A \in \mathcal{O}$. Write $f_{-S} = x^2 + ay + bx + c$, so that again $a, b, c \in \mathcal{O}$. Since $x = \frac{1}{t^2} + \frac{a_1}{t} + O(1)$ and $x = ty$, we have $f_{-S} = \frac{1}{t^4} + \frac{2a_1 + a}{t^3} + O\big(\frac{1}{t^2}\big)$.

Now suppose that P is singular, so that $f_P = \frac{1}{t^{8m}} + \frac{4ma_1}{t^{8m-1}} + O\big(\frac{1}{t^{8m-2}}\big)$. Then, comparing coefficients of $\frac{1}{t^{8m+3}}$ in $g^4 = f_P f_{-S}$ gives

$$4A = 2(2m+1)a_1 + a. \tag{5}$$

Now $f_S = x^2 - a(y + a_1x + a_3) + bx + c$ and $f_S f_{-S} = (x - x(S))^4$, so that the coefficient of x^3 in $f_S f_{-S}$ is $-4x(S) = 2b - a(a_1 + a)$. Since $x(S) \in \mathcal{O}$, we deduce that

$$2b - a(a_1 + a) \in 4\mathcal{O}. \tag{6}$$

Also, by Lemma 1.4 (i), $\tilde{f}_{-S} = (f_{-\tilde{S}})^2 = \big(x - x(-\tilde{S})\big)^2 = x^2 - x(-\tilde{S})^2$, so that a and b lie in the maximal ideal $\mathcal{M}$ of $\mathcal{O}$. But since E has ordinary reduction, a_1, and therefore also $a_1 + a$, is a unit of $\mathcal{O}$. We deduce from (6) that $a \in 2\mathcal{M}$. But then (5) implies that $a_1 \in \mathcal{M}$, which is a contradiction. □

2. Singular torsion and almost rational torsion points

We continue to use the notation already introduced.

Lemma 2.1. *If E is an elliptic curve over a field k of characteristic not 2, then $E_{\mathrm{sing}} - E[2]$ is geometrically-rigid.*

Proof. Since k is of characteristic not 2, we use a Weierstrass model (2) with $a_1 = a_3 = 0$. Let $P, Q, R, S \in E_{\mathrm{sing}}$ satisfy $P + S = Q + R$. Then there is a function $g \in \overline{k}(E)$ with divisor $P + \bar{Q} + \bar{R} + S - 4O$. Furthermore, we can suppose that g is of the form $x^2 + ay + bx + c$ with $a, b, c \in \overline{k}$. Note that if the characteristic of k is $p > 0$, then by Proposition 1.5 (i), the orders of P, Q, R, and S are prime to p. So in any case, we can choose $n \in \mathbb{N}^*$ not divisible by the characteristic of k and annihilating P, Q, R and S. Let F_P be the power of f_P with divisor $n(P - O)$ and define $F_{\bar{Q}}$, $F_{\bar{R}}$ and F_S analogously. Then $g^n = F_P F_{\bar{Q}} F_{\bar{R}} F_S$, and the four points are all singular n-torsion points by Proposition 1.2 (i), so we find that $g^n = \frac{1}{t^{4n}} + O\big(\frac{1}{t^{4n-2}}\big)$ and hence $g = \frac{1}{t^4} + O\big(\frac{1}{t^2}\big)$. Since $x = \frac{1}{t^2} + O(1)$, this implies that $a = 0$ and therefore $[-1]^* g = g$. Thus the zero-divisor of g is stable under $[-1]^*$, and since $P, Q, R, S \notin E[2]$, the Lemma follows. □

Since E_{sing} is clearly Γ_k-invariant, it follows that $E_{\mathrm{sing}} - E[2]$ is a GIGR set.

Although we shall only use the remaining results of this section in the case where G is an elliptic curve E and $\Sigma = E_{\mathrm{sing}} - E[2]$, we state them in greater generality in view of the applications of these results to other sets of almost rational torsion points (see [6] and [13]).

The following is elementary. Let p be a prime. Recall we set $\delta = \delta(p) = 1$ when p is odd, and $\delta(2) = 2$.

Lemma 2.2. *For any prime p, all $b > 1$, and $2 \le r \le b$, we have*

$$\mathrm{ord}_p\Big(\binom{b}{r} p^{(r-1)\delta}\Big) > \mathrm{ord}_p(b).$$

Proposition 2.3. *Let G be a commutative algebraic group over a field k, let p be a prime number, and let Δ be a subgroup of Γ_k that acts trivially on $G[p^\delta]$.*

(i) *If $P \in G[p^n]^*$ and $\tau \in \Delta$ doesn't fix P, then the order of $(\tau-1)P$ divides $p^{n-\delta}$.*
(ii) *If $P \in G[p^\infty]$ and $\tau \in \Delta$ doesn't fix P, then setting $Q = (\tau-1)P$, for all $b \geq 1$, the order of $\tau^b(P) - P$ is the same as the order of $[b]Q$.*
(iii) *If $P \in G[p^\infty]$ and $\tau \in \Delta$ doesn't fix P, there exists a $\sigma \in \Delta$, a power of τ, such that $O \neq \sigma(P) - P \in G[p^\delta]$.*

Proof. (*i*) By hypothesis, there exists a $\tau \in \Delta$ such that $\tau(P) \neq P$. Let $m \leq n-1-\delta$ be the largest integer such that τ acts non-trivially on $[p^m]P$. Then since $\tau([p^{m+1}]P) = [p^{m+1}]P$, we have $O \neq \tau([p^m]P) - [p^m]P \in E[p]$ and $\tau(P) - P = (\tau-1)P$ is of order p^{m+1}.

(*ii*) The case $b = 1$ is trivial. For every $b \geq 2$, we have

$$\tau^b(P) - P = [b]Q + \sum_{r=2}^{b} [\binom{b}{r}](\tau-1)^{r-1}(Q). \tag{7}$$

By Lemma 2.2 and (*i*), the order of $[\binom{b}{r}](\tau-1)^r(Q)$ is a proper divisor of the order of $[b]Q$, for all $2 \leq r \leq b$, so by (7) the order of $\tau^b(P) - P$ is the same as the order of $[b]Q$.

(*iii*) Let P be of order p^n. By hypothesis, there exists a $\tau \in \Delta$ such that $\tau(P) \neq P$. Let $Q = (\tau-1)P$. We can take b so that $[b]Q \in G[p^\delta]$, $[b]Q \neq O$, and then applying (*ii*) we can take $\sigma = \tau^b$. □

Proposition 2.4. *Let G be a commutative algebraic group over a field k, and suppose $\tau \in \Gamma_k$ acts trivially on $G[p^\delta]$. Suppose we can write $P \in G_{\mathrm{tors}}$ as $P = Q + R$ with $R \in G[p^\infty]$, $\tau(Q) = Q$ and $\tau(R) \neq R$. Then P cannot be almost rational.*

Proof. By Proposition 2.3 (*iii*), there exists $\sigma \in \Gamma_k$, a power of τ, such that $O \neq \sigma(R) - R = \sigma(P) - P \in G[p^\delta]$. Put $W = \sigma(P) - P$. Then $\sigma(W) = W$, and therefore $\sigma(P) = P + W$ and $\sigma^2(P) = P + 2W$. Hence

$$P + \sigma^2(P) = 2\sigma(P).$$

If P is almost rational, then so is $\sigma(P)$, hence $P = \sigma(P)$, a contradiction. □

Proof of Proposition C. Suppose that $P \in \Sigma \cap G_\Omega$, but $P \notin G[M]$. Let π be any element of Γ_{k_1} such that $Q = \pi(P) - P \neq O$. Breaking Q into its prime-power components and applying Proposition 2.3 (*ii*) to each, we see that for any $b \geq 1$, the order of $\pi^b(P) - P$ is the same as that of $[b]Q$. We can choose b divisible only by primes in Ω and such that $O \neq [b]Q \in G[L]$. If now $\tau = \pi^b$, then τ fixes $\tau(P) - P$, so that $\tau^2(P) + P = 2\tau(P)$. Thus if P were almost rational, $\tau(P) = P$, a contradiction. □

3. The case of multiplicative reduction

In this section we prove Theorem A (i), and we keep the notation used therein. In particular, K is a finite extension of $\mathbb{Q}_p$, and E is an elliptic curve over K with potential multiplicative reduction. Since E_{sing} is independent of the choice of model for E, replacing E by a quadratic twist if necessary, we can assume that E has split multiplicative reduction over K. We therefore have at our disposal Tate's theory of p-adic uniformization of E (see for example [25], pp 422–448). We first recall some aspects of that theory. Let $q \in K$ be the parameter associated to E. Let C_p be the completion of an algebraic closure of $\mathbb{Q}_p$, and let $u \in C_p^*$ be a variable. As in [25], we have the theta function

$$\Theta(u,q) = (1-u)\prod_{n\geq 1}(1-q^n u)(1-q^n u^{-1})/(1-q^n)^2,$$

which is analytic in u, and has a simple zero at every point $u \in q^{\mathbb{Z}}$. Furthermore, it satisfies the functional equation

$$\Theta(uq,q) = -(1/u)\Theta(u,q).$$

We now define $\theta(u,q) = \sum_{n\in\mathbb{Z}} q^{(n+1)n/2}u^{n+1}(-1)^n$, which is also easy to check is analytic in u and has the same functional equation

$$\theta(uq,q) = -(1/u)\theta(u,q),$$

as Θ. Therefore Θ and θ differ only by a multiplicative constant, so θ also has a simple zero at every point $u \in q^{\mathbb{Z}}$. Let $P \in C_p^*/q^{\mathbb{Z}} \cong E(C_p^*)$ be of order N. We can represent P as $Q^r\zeta^s$, where Q is a chosen N^{th}-root of q, ζ is a primitive N^{th}-root of unity, and $0 \leq r,s < N$ and $\gcd(r,s,N) = 1$. It follows from the functional equation for θ that we can take

$$f_P(u) = (1/u^r)(\theta(uQ^{-r}\zeta^{-s},q)/\theta(u,q))^N.$$

To see if P is a singular torsion point, we need to expand f_P in terms of any odd parameter at the origin t. Since "odd" in this setting translates to a function being sent to its negative under the transformation $u \to u^{-1}$, we can expand any such t as a power series in $v = u - u^{-1}$, convergent in a neighborhood of $v = 0$, with only odd powers appearing. Hence to see if P is singular, we can multiply f_P by v^N and expand in terms of v and see if the linear term vanishes. From the functional equation, it is clear that $\theta(u,q)/(1-u)$ is even, so we need only check the vanishing of the linear term in v of

$$\theta(uQ^{-r}\zeta^{-s},q)^N v^N/(u^r(1-u)^N),$$

but for this it suffices to check the vanishing of the linear term in $1-u$. A straightforward calculation shows that this term vanishes if and only if $\psi(r,s,N)$, defined by

$$\psi(r,s,N) = \sum_{n\in\mathbb{Z}} q^{n(n-1)/2}Q^{-rn}\zeta^{-sn}(-1)^n(-r/N - 1/2 + n), \tag{8}$$

vanishes. That is, $P \in E_{\text{sing}}$ if and only if $\psi(r,s,N)=0$. Our goal is to prove if $N \geq 3$, and a is the largest integer such that K contains a primitive p^a-th root of unity, then $\text{ord}_p(N) \leq a$ if $p \geq 3$, and if $p=2$, $\text{ord}_2(N) \leq a+1$.

Let $\alpha = \frac{1}{2} + \frac{r}{N}$. It is convenient to rewrite the condition $\psi(r,s,N)=0$ in (8) as

$$\sum_{n\in\mathbb{Z}} (n-\alpha)(-1)^n \zeta^{-sn} Q^{n(n-1)N/2-rn} = 0. \tag{9}$$

Elementary manipulations show that the vanishing of $\psi(r,s,N)$ depends only on the values of $r, s \mod N$, and that $\psi(r,s,N)$ vanishes if and only if $\psi(-r,-s,N)$ does. Hence without loss of generality we can assume that $0 \leq \alpha \leq \frac{1}{2}$.

Lemma 3.1. *If $P = Q^r\zeta^s$ represents a singular torsion point, then $\alpha \in \mathbb{Z}_p$, or $\alpha = 0$ or $\frac{1}{2}$. In other words, if p is odd and $p|N$, then r/N is a p-adic integer, so p does not divide s. If $p=2$ and $2|N$, then $2r/N$ is a 2-adic integer, so if $4|N$, s is odd.*

Proof. If $\alpha \notin \mathbb{Z}_p$, then $\text{ord}_p(n-\alpha) = \text{ord}_p(\alpha)$ is independent of n, and if $\alpha \neq 0, \frac{1}{2}$, then $n(n-1)N/2 - rn = m(m-1)N/2 - rm$ for $n, m \in \mathbb{Z}$ if and only if $n = m$. This implies that the different terms in the series (8) have different valuations and so the sum cannot vanish, and hence P is not a singular torsion point. □

So to complete the proof of Theorem A (i), we need to consider three cases:

(a) Suppose $\alpha = 0$. Then $r = -\frac{1}{2}N$ and N is even. We regroup the summands for n and $-n$ in (9) to get

$$\psi(-\frac{N}{2}, s, N) = \sum_{n\geq 1} n(-1)^n(\zeta^{-sn} - \zeta^{sn})Q^{\frac{n^2N}{2}}.$$

Suppose $\zeta^s \neq 1$. Since $n \mapsto \frac{n^2N}{2}$ is a strictly increasing function of $n \geq 1$, and $\zeta^{-s} - \zeta^s$ divides $\zeta^{-ns} - \zeta^{ns}$ for all $n \geq 1$, we find that the summand for $n=1$ in $\psi(-\frac{N}{2}, s, N)$ has strictly smaller p-adic valuation than all the others, and so $\psi(-\frac{N}{2}, s, N)$ cannot vanish. Hence if $\psi(-\frac{N}{2}, s, N) = 0$, we have $\zeta^s = 1$, so $s = 0$. Lemma 3.1 now gives in this case that for p odd, $\text{ord}_p(N) = 0$, and when $p = 2$, $\text{ord}_2(N) \leq 1$.

(b) Suppose $\alpha = \frac{1}{2}$. We note that $r = 0$, and that the quadratic form $x \mapsto \frac{x(x-1)}{2}N$ is symmetric about $x = \frac{1}{2}$. Thus, combining the summands with $n = 1$ and $n = 0$, $n = 2$ and $n = -1$, and in general $n = m$ and $n = -m+1$ in (9), we get by an argument similar to (a) that $\zeta^s = -1$, so again for p odd, $\text{ord}_p(N) = 0$, and when $p = 2$, $\text{ord}_2(N) \leq 1$.

(c) Suppose that $0 < \alpha < \frac{1}{2}$ is in $\mathbb{Z}_p$. Then since the quadratic form $x \mapsto \frac{x(x-1)}{2}N - rx$ is symmetric about $x = \alpha$, its values at 0, 1, −1, 2, −2, 3, −3, etc., form a strictly increasing sequence. Note the summand for n in the left hand side of (9) has p-adic order equal to $\text{ord}_p(n-\alpha) + (\frac{n(n-1)}{2}N - rn)\text{ord}_p(Q)$. Now at least one of $-\alpha$ and $1-\alpha$ is a p-adic unit. Hence, if the left hand side of (9) vanishes, the p-adic valuation of the summands for $n = 0$ and $n = 1$ must be

the same, since otherwise one of them will have p-adic valuation strictly smaller than all the other summands. When this happens, we must have $\mathrm{ord}_p(-\alpha) > 0$ and therefore $\mathrm{ord}_p(1-\alpha) = 0$.

To conclude, we use a Galois-theoretic argument. Write $\frac{r}{N} = \frac{r_0}{N_0}$ with r_0 and N_0 coprime integers. By Lemma 3.1, N_0 is not a multiple of p when p is odd, and when $p = 2$, if N is even, $N_0 = 2N'$ with N' odd. Write also $\frac{s}{N} = \frac{s_1}{N_1 p^b}$, with N_1 not divisible by p and s_1 prime to $N_1 p^b$. Fix Q_0 with $Q_0 = Q^{N/N_0}$ and write $\zeta^{-s} = \zeta_1\zeta_0$, where ζ_1 is a primitive N_1-th root of 1 and ζ_0 a primitive p^b-th root of unity. Then the vanishing condition (9) is equivalent to

$$\sum_{n\in\mathbb{Z}} (n-\alpha)(-1)^n \zeta_1^n \zeta_0^n Q_0^{\frac{n(n-1)}{2}N_0 - nr_0} = 0. \tag{10}$$

Fix a primitive N_0-th root of unity η. For any $g \in \Gamma_K$, define a function ϵ with values in $\mathbb{Z}/N_0\mathbb{Z}$ by $g(Q_0) = Q_0\eta^{\epsilon(g)}$. Now take $g \in \Gamma_K$, and apply $1 - g$ to (10). Since the action of Γ_K is continuous and $\alpha \in \mathbb{Z}_p$, we get

$$\sum_{n\in\mathbf{Z}} (n-\alpha)(-1)^n \big(\zeta_1^n\zeta_0^n - g(\zeta_1)^n \eta^{-\epsilon(g)nr_0} g(\zeta_0)^n\big) Q_0^{\frac{n(n-1)}{2}N_0 - nr_0} = 0.$$

The summand with $n = 0$ vanishes. Recall that $\mathrm{ord}_p(n-\alpha) \geq 0$ for all n and that $\mathrm{ord}_p(1-\alpha) = 0$. Suppose that $g(\zeta_1)\eta^{-\epsilon(g)r_0} g(\zeta_0) \neq \zeta_1\zeta_0$. Since the sequence $n \mapsto \frac{n(n-1)}{2}N_0 - nr_0$ is strictly increasing when n takes the values 1, -1, 2, -2, $\ldots$, and $\zeta_1\zeta_0 - g(\zeta_1)\eta^{-\epsilon(g)r_0} g(\zeta_0)$ divides $\zeta_1^n\zeta_0^n - g(\zeta_1)^n\eta^{-\epsilon(g)nr_0} g(\zeta_0)^n$ for all $n \in \mathbb{Z}$, we deduce that the summand for $n = 1$ has valuation strictly smaller than all the others, and so the sum of the series cannot vanish, a contradiction.

It follows that $g(\zeta_1)\eta^{-\epsilon(g)r_0} g(\zeta_0) = \zeta_1\zeta_0$ for all $g \in \Gamma_K$. Take p odd. Then since ζ_1 and η are roots of unity of order prime to p, and ζ_0 is a primitive p^b-th root of unity, we deduce that $g(\zeta_1)\eta^{-\epsilon(g)r_0} = \zeta_1$ and $g(\zeta_0) = \zeta_0$ for all $g \in \Gamma_K$. In particular, the second equality implies that $\zeta_0 \in K$ and, since we defined a as the largest integer such that a primitive p^a-root of unity was in K, we conclude that $\mathrm{ord}_p(N) = b \leq a$ as claimed. Now if $p = 2$, $-\eta$ is a primitive N'-th root of unity, so we get that $g(\zeta_1^2)(-\eta)^{-2\epsilon(g)r_0} g(\zeta_0^2) = \zeta_1^2\zeta_0^2$ for all $g \in \Gamma_K$. We conclude as before that $\zeta_0^2 \in K$, and so $\mathrm{ord}_2(N) \leq \max(1, b) \leq a + 1$ as desired. □

4. The Case of Good Reduction

In this section we complete the proof of Theorem A in the Introduction. Since we have already established (i) we can suppose that E has good reduction.

Recall we have an elliptic curve E over a finite extension K of $\mathbb{Q}_p$. Identifying $\overline{K} = \overline{\mathbb{Q}}_p$, we have that $\mathcal{O}$ is the ring of integers of $\overline{K}$, and k its residue field. If F is an extension of K contained in $\overline{K}$, we denote by $\mathcal{O}_F$ the ring of integers of F and by $\mathcal{M}_F$, k_F, respectively, the maximal ideal and residue field of $\mathcal{O}_F$. We denote by e_F the ramification degree of F over $\mathbb{Q}_p$ (when defined). We let I_F denote the inertia subgroup of Γ_F.

We fix once and for all a Weierstrass model (2) with coefficients $a_i \in \mathcal{O}_K$. We take $t = \frac{x}{y}$ as a parameter for the formal group $\hat{E}$ over $\mathcal{O}_K$ at the origin, so if $[p]_{\hat{E}}t = \sum_{r\geq 1} b_r t^r$ as an endomorphism of the formal group, then $b_r \in \mathcal{O}_K$ for all r. We write $\tilde{E}$ for the special fiber of our Weierstrass model. We define $h = h(E)$ (the height of the formal group) to be 1 if $\tilde{E}$ is ordinary and 2 if it is supersingular. Then it is well-known that $\hat{E}[p^r] \simeq (\mathbb{Z}/p^r\mathbb{Z})^h$ and $\tilde{E}[p^r] \simeq \mathbb{Z}/p^{r(2-h)}\mathbb{Z}$ as abstract groups for all $r \geq 1$. Indeed we have an exact sequence

$$O \to \hat{E}[p^r] \to E[p^r] \to \tilde{E}[p^r] \to O \tag{11}$$

for all integers $r \geq 1$.

Lemma 4.1. (i) *We have $b_r \in p\mathcal{O}_K$ for all r not divisible by p.*
(ii) *if E has ordinary reduction, then $b_p \in \mathcal{O}_K^*$.*
(iii) *if E has supersingular reduction, then $b_r \in \mathcal{M}_K$ for all $r \leq p^2 - 1$ but $b_{p^2} \in \mathcal{O}_K^*$.*

Proof. (*i*) is IV 4.4 in [24]. For (*ii*) and (*iii*), see [24] IV 7.5. □

We know that the Tate module $T_p(E)$ is a $\mathbb{Z}_p$-module of rank 2. Thus we have a continuous representation $\rho : \Gamma_K \to \mathrm{Aut}_{\mathbb{Z}_p}(T_p(E))$. If $n \geq 1$ is an integer, we denote by K_n the extension $K(E[p^n])$ of K and by $\rho_n : \Gamma_K \to \mathrm{Aut}_{\mathbb{Z}/p^n\mathbb{Z}}(E[p^n])$ the corresponding representation on $E[p^n]$. Let L_n be the maximal unramified extension of K_n, so that I_{K_n} can be identified with Γ_{L_n}. Similarly, let L be the maximal unramified extension of K.

We now complete the proofs of Theorem A (*ii*), and (*iii*). It is convenient to treat separately the cases of ordinary and supersingular reduction.

4.1. The ordinary reduction case. Let $V = \hat{E}[p^\infty]$. Since E has ordinary reduction, $T(V) = \varprojlim V \cap E[p^n]$ is a rank one $\mathbb{Z}_p$-submodule of $T_p(E)$. Hence $E[p^\infty]$ contains a subgroup U such that $E[p^\infty] = V \oplus U$, and such that $T(U) = \varprojlim U \cap E[p^n]$ is a second rank one $\mathbb{Z}_p$-submodule of $T_p(E)$ such that $T_p(E) = T(U) \oplus T(V)$. By (11) the reduction map $E(\overline{\mathbb{Q}}_p) \to \tilde{E}(k)$ induces an isomorphism $U \simeq \tilde{E}[p^\infty]$. If we fix a choice of U and generators u of $T(U)$ and v of $T(V)$, then $\rho_n(\Gamma_K)$ can be identified with a subgroup of the group of upper triangular matrices in $GL_2(\mathbb{Z}/p^n\mathbb{Z})$ and $\rho_n(I_K)$ with a subgroup of the group T_n of matrices of the form $\begin{pmatrix} 1 & \theta \\ 0 & b \end{pmatrix}$, where $\theta \in \mathbb{Z}/p^n\mathbb{Z}$ and $b \in (\mathbb{Z}/p^n\mathbb{Z})^*$. The proof of the following is straightforward.

Lemma 4.2. (i) *Let $M = \begin{pmatrix} 1 & \theta \\ 0 & b \end{pmatrix} \in T_1$, where $\theta \in \mathbb{F}_p$ and $b \in \mathbb{F}_p^*$. If $b \neq 1$, then the order of M in T_1 is equal to the order of b in $\mathbb{F}_p^*$.*
(ii) *Let $p = 2$. Then T_2 is a dihedral group of order 8.*

Lemma 4.3. *Let $r \geq 1$ and let $P \in \hat{E}[p^r]^*$. Then* $\mathrm{ord}_p(t(P)) = \frac{1}{p^{r-1}(p-1)}$.

Proof. Since $[p]_{\hat{E}}(t) = pt + O(t^2)$, Lemma 4.1 shows that the Newton polygon (see [15], page 89) of $[p]_{\hat{E}}(t)$ has a single non-horizontal segment of length $p-1$ and slope $-\frac{1}{p-1}$. Since $[p]_{\hat{E}}(t(P)) = 0$ if and only if $P \in \hat{E}[p]$, this proves the result when $r = 1$. The case $r > 1$ is proved by induction by considering the Newton polygon of $[p]_{\hat{E}}(t) - t(Q)$ for $Q \in \hat{E}[p^{r-1}]^*$. □

We also have a continuous representation $\hat{\rho} : \Gamma_K \to \mathrm{Aut}_{\mathbb{Z}_p}(T(V)) \simeq \mathbb{Z}_p^*$ under which $\hat{\rho}(\Gamma_K)$ can be identified with a closed subgroup of $\mathbb{Z}_p^*$.

Lemma 4.4. (i) *Suppose $p \geq 3$ and $e_K < p-1$. Then no point v_n of V of order p^n with $n \geq 2$ is rational over L_1.*

(ii) *Suppose $p = 2$ and $e_K = 1$. Then no point of V of order 2^n with $n \geq 4$ is rational over L_2.*

Proof. (*i*) Suppose for a contradiction that V contains a point v_n of order p^n rational over L_1, with $n \geq 2$. Then since $e_K < p-1$, p does not divide e_K, and Lemma 4.3 implies that $\hat{\rho}(I_K)$ is a subgroup of $\mathbb{Z}_p^*$ of index less than $p-1$ and therefore contains $1 + p\mathbb{Z}_p$ but is not equal to it. It follows that there exists an $r > 1$ such that $\mathrm{Gal}(L(V[p^n])/L)$ contains an element of order rp^{n-1} for all $n \geq 1$. If $v_n \in L_1$, then $L(V[p^n]) \subseteq L_1$, so there is a surjective homomorphism from some subgroup of T_1 to a cyclic group of order rp^{n-1}. But according to Lemma 4.2 (*i*) this is not possible if $n \geq 2$.

(*ii*) This is similar to (*i*), using Lemma 4.2 (*ii*) instead of (*i*). The crux is that there are no surjective homomorphisms from a subgroup of a dihedral group of order 8 to $(\mathbb{Z}/2^n\mathbb{Z})^\times$ for $n \geq 4$. □

Proof of Theorem A (ii) in the ordinary case. Let $P \in E[N]^*$, and suppose $P \in E_{\mathrm{sing}}$ and that $N \geq 3$. We write $P = Q + R$ with Q of order prime to p and $R = u_m + v_n$, with $u_m \in U$ of order p^m and $v_n \in V$ of order p^n. Thus $\mathrm{ord}_p(N) = \max(m, n)$.

(*a*) Suppose $m \geq n$. If $m \geq \delta$, then $\tilde{P} \in \tilde{E}[N]^*$ and so $P \notin E_{\mathrm{sing}}$ by Proposition 1.5 (*i*) and (*ii*). If $m < \delta$ the result holds by hypothesis.

(*b*) Suppose $p = 2$, $n \geq 3$ and $m = n-1$. Then $\tilde{P} \in \tilde{E}[\frac{N}{2}]^*$ and so $P \notin E_{\mathrm{sing}}$ by Proposition 1.5 (*iii*).

Thus, to complete the proof of Theorem A (*ii*) in the ordinary case, we can suppose $m < n$ when p is odd and $m < n-1$ when $p = 2$. Suppose p is odd. By applying Proposition 2.4 to all elements of I_{K_1}, we have $R \in L_1$. If $m = 0$, since by hypothesis, $e_K < p-1$, Lemma 4.4 (*i*) gives $n \leq 1$. If $m \geq 1$, $[p^{m-1}]u_m \in L_1$ and hence $[p^{m-1}]v_n \in L_1$, so by Lemma 4.4 (*i*), $n - m + 1 \leq 1$, a contradiction. Hence $\mathrm{ord}_p(N) \leq 1$. The case $p = 2$ and $n \geq 4$ is similar. By Proposition 2.4 we have $R \in L_2$. If $m \leq 2$, $v_n \in L_2$, and by hypothesis, $e_K = 1$, so by Lemma 4.4 (*ii*) we have $n \leq 3$. If $m \geq 2$, $[p^{m-2}]u_m \in L_2$ and hence $[p^{m-2}]v_n \in L_2$, and $n - m + 2 \leq 3$, a contradiction. Hence $\mathrm{ord}_2(N) \leq 3$. □

Proof of Theorem A (iii) in the ordinary case. We now have $p \geq 3$. Let $P \in E_{\mathrm{sing}}$ be of order $N \geq 3$. If p verifies the hypotheses of Theorem A (*iii*), then

$e_K < p-1$ by (1), and from what has just been proved we deduce that $\mathrm{ord}_p(N) \leq 1$. Hence it suffices to eliminate the possibility that $\mathrm{ord}_p(N) = 1$.

The extension $K(\hat{E}[p])/K$ is abelian and the action of I_K on $\hat{E}[p]$ is given by a character $I_K \to \mathbb{F}_p^*$ whose image we denote by G. Let $M = K(\hat{E}[p])$, so $\#(G) = e_M/e_K$. Let s be the index of G in $\mathbb{F}_p^*$.

We first remark that s divides e_K. Indeed, by Lemma 4.3, $(p-1)|e_M$, and $e_K|e_M$, so that $\mathrm{lcm}(p-1, e_K)$ divides e_M. Hence $s = (p-1)/\#(G) = (p-1)e_K/e_M$ divides $(p-1)e_K/\mathrm{lcm}(p-1, e_K) = \gcd(p-1, e_K)$, and $s|e_K$.

Let b be a generator of G. Since $e_K < p-1$, $G \neq \{1\}$, and so $b \neq 1$. Let (u_1', v_1') be a $\mathbb{Z}/p\mathbb{Z}$-basis of $E[p]$ with $u_1' \in U$ and $v_1' \in V$. Then I_K contains an element τ such that with respect to this basis $\rho_1(\tau) = \begin{pmatrix} 1 & \theta \\ 0 & b \end{pmatrix}$, where $\theta \in \mathbb{F}_p$. Since $b \neq 1$, one sees that $\begin{pmatrix} 1 & \theta \\ 0 & b \end{pmatrix}$ fixes $u_1' - \frac{\theta}{b-1}v_1'$, and so replacing u_1' by this point we can suppose that $\tau(u_1') = u_1'$ and $\tau(v_1') = bv_1'$. From this, we deduce the following.

Lemma 4.5. *Let $w \in G$. Then after possibly changing U, there exists a $\sigma \in I_K$ such that $\sigma(u_1) = u_1$ for all $u_1 \in U \cap E[p]$ and $\sigma(v_1) = wv_1$ for all $v_1 \in V \cap E[p]$.*

Lemma 4.6. *Let $P \in E_{\mathrm{sing}}$ be of order $N \geq 3$, and let $p \geq 3$ be a prime such that $e_K < p-1$. Let $M(r)$ be as defined in the statement of Theorem A (iii).*

(i) *Suppose there exists $(x, y, z) \in (\mathbb{F}_p^*)^3$ such that $1 + x^s = y^s + z^s$, $1 + x^s \neq 0$, $y^s \neq 1$ and $z^s \neq 1$. Then $\mathrm{ord}_p(N) = 0$.*

(ii) *Let q be a power of a prime and let $r > 0$ divide $q-1$. If $q > M(r)$, then there exists $(x, y, z) \in (\mathbb{F}_q^*)^3$ such that $1 + x^r = y^r + z^r$, $1 + x^r \neq 0$, $y^r \neq 1$ and $z^r \neq 1$.*

Proof. (*i*) Since $\mathbb{F}_p^*$ is cyclic, G is just the subgroup of s-th powers in $\mathbb{F}_p^*$. We write $P = Q + u_1 + v_1$ with Q of order prime to p, $u_1 \in U$, $v_1 \in V$. Since we already know that $\mathrm{ord}_p(N) \leq 1$, we can suppose $u_1 \in E[p]$ and $v_1 \in E[p]$. Then by Lemma 4.5, there exist α, β, $\gamma \in I_K$ such that $\alpha(u_1) = \beta(u_1) = \gamma(u_1) = u_1$, $\alpha(v_1) = x^s v_1$, $\beta(v_1) = y^s v_1$ and $\gamma(v_1) = z^s v_1$. By the Néron-Ogg-Shafarevich criterion (see for example [24] p184), $\alpha(Q) = \beta(Q) = \gamma(Q) = Q$, and therefore $P + \alpha(P) = \beta(P) + \gamma(P)$. Therefore, since E_{sing} is Γ_K-invariant, Lemma 2.1 implies that either $P + \alpha(P) = O$, or $P = \beta(P)$, or $P = \gamma(P)$. But then if $v_1 \neq O$, either $1 + x^s = 0$, or $y^s = 1$, or $z^s = 1$, a contradiction. So $v_1 = O$, and Proposition 1.5 (*i*) shows $u_1 = O$ as well.

(*ii*) Let V_r denote the set of $\mathbb{F}_q$-points on the surface $1 + x^r = y^r + z^r$ in affine three-space. Then we find, using Theorem 6.37 of [17], that $\#(V_r) \geq q^2 - (r^3 - 4r^2 + 6r - 3)q - (r^2 - 3r + 2)\sqrt{q}$. The result will be proved if we can show that V_r contains a point that does not lie in the subset $S = Z \cup V_x \cup V_y \cup V_z$, where Z, V_x, V_y and V_z are the $\mathbb{F}_q$-points of the algebraic sets defined respectively by $xyz = 0$, by $1 + x^r = 0$ and $y^r + z^r = 0$, by $y^r = 1$ and $x^r = z^r$, and by $z^r = 1$ and $x^r = y^r$. The maximal size of S is attained when -1 is an r-th power and

elementary methods show that this value is at most

$$B(r) := 3(q + (r^2 - 3r + 2)\sqrt{q} + r - 1) - 3r + 3r^2(q-1) - 3r^3.$$

We conclude that there exists $(x, y, z) \in (\mathbb{F}_q^*)^3$ as required whenever $q^2 - (r^3 - 4r^2 + 6r - 3)q - (r^2 - 3r + 2)\sqrt{q} - B(r) = q^2 - (r^3 - r^2 + 6r)q - 4(r^2 - 3r + 2)\sqrt{q} + 3r^3 + 3r^2 + 3 > 0$. Referring to the definition of f_r in the statement of Theorem A, we deduce that $f_r(q) > 0$ when $q > M(r)$. □

Since s is a divisor of e_K, we deduce from (1) that if $p > M(e_K)$ then $e_K < p - 1$ and so $\mathrm{ord}_p(N) = 0$, which completes the proof of Theorem A (*iii*) in the case of ordinary reduction. □

4.2. The supersingular reduction case. In this case we have $\hat{E}[p^\infty] = E[p^\infty]$. Recall $[p]_{\hat{E}}(t) = \sum_{i \geq 1} b_i t^i$.

Lemma 4.7. *Let $r \geq 1$ and let $P \in E[p^r]^*$. Suppose that $e_K \leq p + 1$. Let $\mu = \mathrm{ord}_p(b_p) > 0$.*

(i) *If $\mu \geq p/(p+1)$, then $\mathrm{ord}_p(t(P)) = \frac{1}{p^{2(r-1)}(p^2-1)}$.*

(ii) *If $\mu < p/(p+1)$, then $\mathrm{ord}_p(t(P)) = \frac{\mu}{p^{2r-1}(p-1)}$, or $\mathrm{ord}_p(t(P)) = \frac{1-\mu}{p^{2(r-1)}(p-1)}$.*

Proof. First note that since $E[p] \cong (\mathbb{Z}/p\mathbb{Z})^2$, $E[p]^*$ has $p + 1$ orbits C_i under the action of multiplication of $(\mathbb{Z}/p\mathbb{Z})^*$, and since each multiplication is an automorphism of $\hat{E}[p]$, that $c_i = \mathrm{ord}_p\big(t(P)\big)$ is the same for all P in a fixed orbit C_i. We have two cases: (A), in which c_i is the same for all i, or (B), in which $c_i < c_j$ for some i, j. In (B), since in a formal group $t(P + Q) = t(P) + t(Q)$ modulo quadratic terms, we have $c_k = c_i$ for all $k \neq j$. It follows that in (A), the Newton polygon of $[p]_{\hat{E}}(t)$ has one segment with non-horizontal slope and length $p^2 - 1$, so must be of slope $-\frac{1}{p^2-1}$ and so we must have $\mu \geq p/(p + 1)$. In (B), the Newton polygon must have two non-horizontal segments of distinct non-zero slopes, the segment of lesser slope having length $p - 1$, and the other having length $p^2 - p$. It follows that $\mu < p/(p+1)$, and that the segment of length $p-1$ has slope $(1 - \mu)/(1 - p)$, and the segment of length $p^2 - p$ has slope $\mu/(p - p^2)$. Since $[p]_{\hat{E}}(t(P)) = 0$ if and only if $P \in E[p]$, this proves (i) and (ii) when $r = 1$. Now suppose $r \geq 1$ and that the assertions have been proved with r replaced by $r - 1$. Let $Q \in E[p^{r-1}]^*$ and consider the power series $[p]_{\hat{E}}(t) - t(Q)$. In (A), we get immediately that its Newton polygon has one non-horizontal segment of length p^2 with slope $-\frac{1}{p^{2(r-1)}(p^2-1)}$, and in (B), a calculation shows that since $e_K \leq p + 1$, the Newton polygon has one non-horizontal segment of length p^2 with slope either $-\frac{\mu}{p^{2r-1}(p-1)}$, or $-\frac{1-\mu}{p^{2(r-1)}(p-1)}$. In either case, the set of zeros of $[p]_{\hat{E}}(t) - t(Q)$ is just $\{P \in \hat{E}[p^r]^* \mid [p]P = Q\}$. This proves the assertion at level r. □

We call (A) of the last proof the *one-slope case* and (B) the *two-slope case*, in reference to the shape of the Newton polygon of $[p]_{\hat{E}}$. In the two-slope case, we refer to the line C_j as the *fixed line*, since it is fixed by Γ_K.

Lemma 4.8. (i) *Suppose p is odd and $e_K \leq p-1$. Then no point $P \in E[p^n]^*$ with $n \geq 2$ is rational over L_1.*

(ii) *Suppose $p = 2$ and $e_K = 1$. Then no point $P \in E[2^n]^*$ with $n \geq 4$ is rational over L_2.*

Proof. (*i*) By assumption $\mathrm{ord}_p(e_K) = 0$, and $\mathrm{ord}_p(\#(GL_2(\mathbb{Z}/p\mathbb{Z}))) = 1$, so we get $\mathrm{ord}_p(e_{L_1}) \leq 1$. By Lemma 4.7, this prevents $P \in E[p^n]^*$ with $n \geq 2$ being rational over L_1.

(*ii*) This is similar to (*i*), noting that $\mathrm{ord}_2(\#(GL_2(\mathbb{Z}/4\mathbb{Z}))) = 5$. □

Proof of Theorem A (ii) in the supersingular case. Again, let $P \in E[N]^*$ with $N \geq 3$, and write $P = Q + R_n$, with Q of order prime to p and $R_n \in E[p^n]^*$. Let n_0 be the largest integer such that $E(L_\delta)$ contains a point of order p^{n_0}. If $n > n_0$, then there exists a $\tau \in I_{L_\delta}$ such that $\tau(R_n) \neq R_n$. Since $\tau(Q) = Q$ by the Néron-Ogg-Shafarevich criterion, we deduce from Proposition 2.4 that $P \notin E_{\mathrm{sing}}$. By Lemma 4.8, $n_0 \leq 1$ when p is odd, and $n_0 \leq 3$ when $p = 2$. □

Note that the proof of Theorem A (*ii*) in the supersingular case shows equally well that if P is an almost rational torsion point of order N, and $e_K \leq p-1$, then $\mathrm{ord}_p(N) \leq 1$ if p is odd, and $\mathrm{ord}_2(N) \leq 3$ if $p = 2$.

Proof of Theorem A (iii) in the supersingular case. Again we take $p \geq 3$. Let $P \in E_{\mathrm{sing}}$ be of order $N \geq 3$. By Theorem A (*ii*), we know since $M(e_K) \geq e_K + 1$ that $\mathrm{ord}_p(N) \leq 1$ when p satisfies the conditions of Theorem A (*iii*). Hence it suffices to eliminate the possibility $\mathrm{ord}_p(N) = 1$.

Suppose first that we are in the one-slope case. Let I_w denote the wild inertia subgroup of I_K. Recall that I_w is the maximal normal pro-p-subgroup of I_K. Let $I_t = I_K/I_w$ be the tame inertia group.

Lemma 4.9. *Suppose we are in the one-slope case. Then I_w acts trivially on $E[p]$, and $E[p]$ has the structure of an $\mathbb{F}_{p^2}$-vector space of dimension one such that the action of I_t on $E[p]$ is given by a character $I_t \to \mathbb{F}_{p^2}^*$.*

Proof. This is well-known when $e_K = 1$, and the proof in general mimics that of Proposition 9 of [23]. This is possible since, by Lemma 4.7 (*i*), $\mathrm{ord}_p(t(P)) = \frac{1}{p^2-1}$ is independent of $P \in E[p]^*$. □

By Lemma 4.9 we view $E[p]$ as an $\mathbb{F}_{p^2}$-vector space of dimension one. Then the action of I_K on $E[p]$ is given by a character $I_K \to \mathbb{F}_{p^2}^*$, whose image we denote by G. Let s be the index of G in $\mathbb{F}_{p^2}^*$. As in the ordinary case, since K_1/K is totally ramified, we see that s divides e_K. Since $e_K < p-1 < p^2-1$, we deduce that $G \neq \{1\}$.

Lemma 4.10. *Suppose we are in the one-slope case. Let $P \in E_{\mathrm{sing}}$ be of order $N \geq 3$, and let $p \geq 3$ be a prime such that $e_K < p-1$. Let $M(r)$ be as defined in the statement of Theorem A (iii).*

(i) *Suppose there exists* $(x, y, z) \in (\mathbb{F}_{p^2}^*)^3$ *such that* $1+x^s = y^s+z^s$, $1+x^s \neq 0$, $y^s \neq 1$ *and* $z^s \neq 1$. *Then* $\mathrm{ord}_p(N) = 0$.
(ii) *If* $p^2 > M(s)$, *then there do exist* $(x, y, z) \in (\mathbb{F}_{p^2}^*)^3$ *satisfying the conditions in* (*i*).

Proof. (*i*) Since $\mathbb{F}_{p^2}^*$ is a cyclic group, G is just the subgroup of s-th powers in $\mathbb{F}_{p^2}^*$. We write $P = Q+R$ with Q of order prime to p and R of order a power of p. By Theorem A (*ii*), $R \in E[p]$. By the definition of G, there exist α, β, $\gamma \in I_K$ such that $\alpha(R) = x^sR$, $\beta(R) = y^sR$ and $\gamma(R) = z^sR$. By the Néron-Ogg-Shafarevich criterion, $\alpha(Q) = \beta(Q) = \gamma(Q) = Q$ and therefore $P + \alpha(P) = \beta(P) + \gamma(P)$. Again we conclude that $P + \alpha(P) = O$, or $P = \beta(P)$, or $P = \gamma(P)$, so in any case $R = O$.

(*ii*) Let $q = p^2$ in Lemma 4.6 (*ii*). □

Since $p^2 > p$, we deduce that if $p > M(e_K)$ then $p^2 > M(e_K)$ and also $e_K < p - 1$ by (1). Since s is a divisor of e_K, it follows from Lemma 4.10 that if $p > M(e_K)$, then $\mathrm{ord}_p(N) = 0$. This completes the proof of Theorem A (*iii*) in the one-slope case.

Suppose we are now in the two-slope case.

Lemma 4.11. (i) *Suppose* $e_K \leq p + 1$ *in the two-slope case. Then there is a basis* u, v *for* $E[p]$ *such that* v *is in the fixed line, and an element* $\sigma \in \mathrm{Gal}(K_1/K)$ *of order* p *such that* $\sigma(v) = v$ *and* $\sigma(u) = u + v$.
(ii) *Suppose that* $P \in E_{\mathrm{sing}}$ *is of the form* $Q+[\alpha]u+[\beta]v$ *with* Q *of order prime to* p *and* $\alpha, \beta \in \mathbb{Z}/p\mathbb{Z}$. *Then* $\alpha = 0$.

Proof. (*i*) Since there is a fixed line, $\mathrm{Gal}(K_1/K)$ is contained in a Borel subgroup of $GL_2(\mathbb{F}_p)$ fixing the fixed line, and let I be the inertia subgroup. Recall $\mu = a/e_K$ for some positive integer a, and $\mu < p/(p+1)$. Then since $e_K \leq p+1$, we have $a < p$. Hence by the proof of Lemma 4.7, if $R \in E[p]^*$ is not in the fixed line, $\mathrm{ord}_p(t(R)) = a/(e_Kp(p-1))$, so p divides the order of I. Hence I contains a transvection σ, and there is a basis u, v for $E[p]$, v in the fixed line, such that $\sigma(v) = v$ and $\sigma(u) = u + v$.

(*ii*) Note that $\sigma(Q) = Q$ and $\sigma([\beta]v) = [\beta]v$. Hence $P+\sigma^2(P) = \sigma(P)+\sigma(P)$, so $P = \sigma(P)$ or $2\sigma(P) = O$. The latter is excluded since $N \geq 3$, and the former implies $\alpha = 0$. □

By Lemma 4.11 (*ii*), we can write $P = Q + [\beta]v$ with Q of order prime to p and $\beta \in \mathbb{Z}/p\mathbb{Z}$. We suppose from now on that $e_K < p - 1$. As at the beginning of the proof of Theorem A (*iii*) in the ordinary case, I_K acts on the fixed line via a character $I_K \to \mathbb{F}_p^*$, whose image we denote by G. Again, the index of G divides e_K. Arguing as in the proof of Lemma 4.6 and taking $q = p$ we deduce that $\mathrm{ord}_p(N) = 0$ if $p > M(e_K)$. □

References

[1] M. Baker, B. Poonen. *Torsion packets on curves*. Compositio Math. **127** (2001), 109–116.

[2] M. Baker, *Torsion points on modular curves*, Invent. Math. **140** (2000), 487–509.

[3] M. H. Baker, K. A. Ribet. *Galois theory and torsion points on curves*. Journal de Théorie des Nombres de Bordeaux, **15** (2003), 11–32.

[4] J. Boxall. *Sous-variétés algébriques de variétés semi-abéliennes sur un corps fini*, London Mathematical Society Lecture Notes **215**, (1995), 69–80.

[5] J. Boxall, D. Grant. *Theta functions and singular torsion on elliptic curves*, in *Number Theory for the Millenium*, Bruce Berndt, et. al. editors. A K Peters, Natick, (2002), 111–126.

[6] ———, *Some remarks on almost rational torsion points*. (In preparation.)

[7] A. Buium. *On a question of Mazur*. Duke Math. J. **75** (1994), 639–644.

[8] ———, *Geometry of p-jets*. Duke Math. J. **82** (1996), 349–367.

[9] F. Calegari. *Almost rational torsion points on semistable elliptic curves*. Internat. Math. Res. Notices, (2001), 487–503.

[10] R. F. Coleman. *Ramified torsion points on curves*. Duke Math. J. **54** (1987), 615–640.

[11] R. F. Coleman, A. Tamagawa, P. Tzermias. *The cuspidal torsion packet on the Fermat curve*. J. Reine Angew. Math. **496** (1998), 73–81.

[12] M. Flexor, J. Oesterlé. *Sur les points de torsion des courbes elliptiques*. In *Séminaire sur les pinceaux de courbes elliptiques*, edited by L. Szpiro. Astérisque **183** (1990), 25–36.

[13] D. Grant, D. Shaulis. *The cuspidal torsion packet on hyperelliptic Fermat quotients*. To appear in Journal de Théorie des Nombres de Bordeaux.

[14] M. Hindry. *Autour d'une conjecture de Serge Lang*, Invent. Math. **94** (1988), 575–603.

[15] N. Koblitz. *p-adic numbers, p-adic analysis and zeta functions*. Graduate Texts in Mathematics **58**, (1977).

[16] S. Lang. *Division points on curves*. Ann. Mat. Pura. Appl. **70** (1965), 229-234.

[17] R. Lidl, H. Niederreiter. *Finite Fields*. Encyclopedia of Mathematics and its Applications **20**, 2nd edition, Cambridge University Press, (1997).

[18] B. Mazur. *Arithmetic on curves*. Bull. Amer. Math. Soc. (N.S.) **14** (1986), 207–259.

[19] L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, Invent. Math. **124** (1996) 437–449.

[20] P. Parent, *Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres*. J. reine angew. Math. **506** (1999), 85–116.

[21] M. Raynaud. *Courbes sur une variété abélienne et points de torsion*, Invent. Math. **71** (1983), 207–233.

[22] K. Ribet, M. Kim. *Torsion points on modular curves and Galois theory*. Notes of a series of talks by K. Ribet in the Distinguished Lecture Series, Southwestern Center for Arithmetic Algebraic Geometry, May 1999. arXiv:math.NT/0305281

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

[24] J. H. Silverman. *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics **106**, Springer-Verlag, (1986).

[25] ———, *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics **151**, Springer-Verlag, (1994).

[26] A. Tamagawa. *Ramification of torsion points on curves with ordinary semistable Jacobian varieties*. Duke Math. J. **106** (2001), 281–319.

[27] P. Tzermias. *The Manin-Mumford conjecture: a brief survey*. Bull. London Math. Soc. **32** (2000), 641–652.

Département de mathématiques et de mécanique, CNRS – UMR 6139, Université de Caen, Esplanade de la Paix, 14032 Caen cedex, France
E-mail address: boxall@math.unicaen.fr

Department of Mathematics, University of Colorado at Boulder, Boulder, Colorado 80309-0395 USA
E-mail address: grant@boulder.colorado.edu