Journal de Théorie des Nombres
de Bordeaux **15** (2003), 11–32

Galois theory and torsion points on curves

par Matthew H. BAKER et Kenneth A. RIBET

Résumé. Dans cet article, nous exposons diverses techniques de théorie de Galois qui s'appliquent à l'étude des points de torsion des courbes. En particulier, nous donnons de nouvelles démonstrations de résultats de A. Tamagawa et des auteurs concernant les points de torsion des courbes à "bonne" ou "semi-stable" réduction "ordinaire" en un nombre premier donné. Nous donnons également de nouvelles démonstrations de : (1) la conjecture de Manin-Mumford : il n'y a qu'un nombre fini de points de torsion sur une courbe de genre au moins 2 plongée dans sa jacobienne par l'application d'Albanese ; et (2) : la conjecture de Coleman-Kaskel-Ribet : pour un nombre premier $p \geq 23$, les seuls points de torsion appartenant à la courbe $X_0(p)$ plongée dans sa jacobienne par un plongement cuspidal sont les pointes (et les points de branchement hyperelliptique lorsque $X_0(p)$ est hyperelliptique et $p \neq 37$). Afin de rendre l'exposition aussi utile que possible, nous donnons des références pour tous les résultats sur les courbes modulaires qui interviennent dans notre discussion.

Abstract. In this paper, we survey some Galois-theoretic techniques for studying torsion points on curves. In particular, we give new proofs of some results of A. Tamagawa and the present authors for studying torsion points on curves with "ordinary good" or "ordinary semistable" reduction at a given prime. We also give new proofs of: (1) The Manin-Mumford conjecture: There are only finitely many torsion points lying on a curve of genus at least 2 embedded in its Jacobian by an Albanese map; and (2) The Coleman-Kaskel-Ribet conjecture: If p is a prime number which is at least 23, then the only torsion points lying on the curve $X_0(p)$, embedded in its Jacobian by a cuspidal embedding, are the cusps (together with the hyperelliptic branch points when $X_0(p)$ is hyperelliptic and p is not 37). In an effort to make the exposition as

Manuscrit reçu le 21 février 2002.
The authors' research was partially supported by an NSF Postdoctoral Fellowship and by NSF grant DMS-9970593. The authors thank Bjorn Poonen and Ron Fertig for providing useful comments on earlier drafts of this manuscript.

useful as possible, we provide references for all of the facts about modular curves which are needed for our discussion.

1. Introduction

This paper surveys Galois-theoretic techniques for studying torsion points on curves that have been developed in recent years by A. Tamagawa and the present authors.

We begin with a brief history of the problem of determining the set of points of a curve that map to torsion points of the Jacobian of the curve.

Let K be a number field, and suppose that X/K is an algebraic curve[1] of genus $g \geq 2$. Assume, furthermore, that X is embedded in its Jacobian variety J via a K-rational Albanese map i; thus there is a K-rational divisor D of degree one on X such that $i = i_D : X \hookrightarrow J$ is defined on $\overline{K}$-valued points by the rule $i(P) = [(P) - D]$, where $[\,\cdot\,]$ denotes the linear equivalence class of a divisor on X. When D is a K-rational point P_0, we often refer to P_0 as the *base point* of the embedding i_{P_0}.

Let $T := J(\overline{K})^{\mathrm{tors}}$ denote the torsion subgroup of $J(\overline{K})$.

Theorem 1.1. *The set $X(\overline{K}) \cap T$ is finite.*

Theorem 1.1 was stated as the *Manin–Mumford conjecture* by S. Lang in 1965. In his article [14], Lang reduced this conjecture to a second conjectural statement, which concerns the action of Galois groups on torsion points of abelian varieties over finitely generated fields. This latter statement is still unproven, despite recent partial progress by Serre, Wintenberger (see [30]) and other authors. The first proof of the Manin–Mumford conjecture was provided by M. Raynaud [23], who combined Galois-theoretic results on torsion points of J with a subtle analysis of the reductions mod p^2 of X and J for a suitable prime p. A second proof was given by R. Coleman[2] in [6] using p-adic integration to analyze the set of primes that may ramify in the field generated by a torsion point on X.

Raynaud also proved the following generalized version of the Manin–Mumford conjecture (see [24]):

Theorem 1.2. *Let K be a field of characteristic zero, and let A/K be an abelian variety. Let V be a subvariety of A which is not the translate by a torsion point of a positive-dimensional abelian subvariety B of A. Let $T := A(\overline{K})^{\mathrm{tors}}$. Then the set $T \cap V$ is not Zariski-dense in V.*

[1] By an algebraic curve, we mean a complete, nonsingular, and absolutely irreducible variety of dimension one over a field.

[2] The results of Tamagawa that we present in section 4 of this paper are closely related to Coleman's work in [6], although the methods are different.

One can use Theorem 1.2 to establish uniform bounds for the cardinality of $X(\overline{K}) \cap T$ as one varies the Albanese embedding; see [3] for details.

It is also possible to generalize Theorem 1.2 in several different directions, replacing T by the division group of any finitely generated subgroup of $A(\overline{K})$, or by any sequence of points in $A(\overline{K})$ whose canonical height tends to zero. See [21] for precise statements and further results.

In this paper, however, we focus on the original problem: What can we say about the intersection $X(\overline{K}) \cap T$ when X is a curve? We are particularly interested in explicit determination of this intersection for particular classes of curves. We mention the following three results:

1. (*Curves of genus 2*) B. Poonen's paper [22] gives an algorithm (which has been implemented on a computer) for determining the intersection $X(\overline{\mathbf{Q}}) \cap T$ when $X/\mathbf{Q}$ is a genus 2 curve embedded in its Jacobian using a Weierstrass point. Poonen's method relies crucially on ideas of Buium [4] and Coleman [6].

2. (*Fermat curves*) Suppose X is the plane curve given by the equation $x^m + y^m = z^m$ for $m \geq 4$. The *cusps* of X are the points $(x, y, z) \in X(\overline{\mathbf{Q}})$ such that $xyz = 0$. Rohrlich [27] proved that the difference of two cusps is always torsion as an element of J. Fix a cusp c and embed X in J using c as a base point. Coleman, Tamagawa, and Tzermias [8] prove:

Theorem 1.3. *The torsion points on X in the embedding $i_c : X \hookrightarrow J$ are precisely the cusps.*

The proof of this theorem involves, among other things, Coleman's p-adic integration methods, complex multiplication theory, and results on class numbers of cyclotomic fields.

3. (*Modular curves*) In [2] and [29], the authors independently prove a conjecture of Coleman, Kaskel, and Ribet [7] concerning torsion points on the modular curve $X_0(p)$ in the cuspidal embedding.

Recall that a curve X/K of genus $g \geq 2$ over a field K is *hyperelliptic* if there exists a degree 2 map $f : X \to \mathbf{P}^1$ defined over $\overline{K}$. Such a map, if it exists, is necessarily unique (up to an automorphism of $\mathbf{P}^1$), and the ramification points of f are called the *hyperelliptic branch points*.

The Coleman–Kaskel–Ribet conjecture is the following statement.

Theorem 1.4. *Let $p \geq 23$ be a prime number, and let X be the modular curve $X_0(p)$. Let H be the set of hyperelliptic branch points on X when X is hyperelliptic and $p \neq 37$, and otherwise let $H = \emptyset$. Then the set of torsion points on X in the embedding $i_\infty : X \hookrightarrow J$ is precisely $\{0, \infty\} \cup H$.*

Note that the condition $p \geq 23$ in Theorem 1.4 is equivalent to the genus of $X_0(p)$ being at least 2.

We do not discuss results (1) or (2) further in this paper, but we will say much more about the modular curves $X_0(p)$, and we give a complete proof of Theorem 1.4 in section 5.

Remark 1.5. It is easy to obtain results similar to Theorem 1.4 for $X_0(mp)$ or $X_1(mp)$ with $p \geq 23$ prime and m arbitrary by utilizing the natural map $X_0(mp) \to X_0(p)$. See [2, Proposition 4.1] for details.

Remark 1.6. Though the proof of Theorem 1.4 we give in this paper is simpler than the previously published ones, it still relies upon a number of deep results, e.g. Grothendieck's semistable reduction theorem, Mazur's detailed study of the arithmetic of $X_0(p)$ and $J_0(p)$, and the second author's level-lowering theorem.

Here is a brief outline of the contents of this paper. In section 2 we discuss what it means for an element of a module to be "almost fixed" by a group action, and we prove some elementary lemmas about such elements. We then show how these ideas can be combined with a result of Serre to give a simple proof of the Manin–Mumford conjecture. In section 3, we study torsion points on Abelian varieties which are almost fixed by the action of an inertia group. This is done, following Tamagawa, in the abstract setting of "ordinary semistable" and "ordinary good" modules. In section 4, the abstract algebraic manipulations of section 3 are placed in a geometric context, with Theorems 4.1 and 4.3 as the reward. In section 5, we discuss the proof of Theorem 1.4. We attempt to give references for all of the facts we use about modular curves and their Jacobians. The material in section 5 relies on section 2 up through and including Lemma 2.7, and on section 3 up through Theorem 3.6, so the reader who is only interested in reading the proof of Theorem 1.4 can skip section 4 and the other parts of sections 2 and 3. In order to preserve the flow of the paper, a few results quoted in the body of the paper are relegated to appendices.

Acknowledgements. We include fairly detailed proofs of all results presented in this paper in order to keep the exposition reasonably self-contained. However, a number of the proofs in this paper can also be found in [2], [29], and [13]. All results in sections 3 and 4, except for Proposition 3.7, are due to Tamagawa, and appear in his paper [29]. However, most of the proofs in section 3 are new. The proof of Theorem 5.1 which we give combines elements from both [2] and [29].

2. Almost Rational Points and the Manin–Mumford Conjecture

In this section K is a field and X/K is an algebraic curve of genus at least 2.

The results of this section and the next are motivated by the following simple observation, which plays a key role in the proof of the Coleman–Kaskel–Ribet conjecture.

Lemma 2.1. *Suppose X is embedded in its Jacobian J via a K-rational Albanese map i_D. Let $P \in X(\overline{K})$; if X is hyperelliptic, assume that P is not a hyperelliptic branch point. Suppose that there exist $g, h \in \mathrm{Gal}(\overline{K}/K)$ such that $gP + hP = 2P$ in J. Then $gP = hP = P$.*

Proof. To be pedantic, we write $Q = i_D(P)$, so that P is a point on X and $Q = [(P) - (D)]$ is its image in the Jacobian of X. We are given that $gQ + hQ = 2Q$ in J, so that the degree-zero divisors $(gP) - (gD) + (hP) - (hD)$ and $2(P) - 2(D)$ are linearly equivalent. Since D is K-rational, it follows that the divisors $(gP)+(hP)$ and $2(P)$ on X are linearly equivalent, so that there exists a rational function f on X whose divisor is $(gP)+(hP)-2(P)$. Since P is not a hyperelliptic branch point, f must be constant, so that $gP = hP = P$, as desired.[3] $\square$

Lemma 2.1 suggests the following definition.

Definition 1. Let G be a group, and let M be a $\mathbf{Z}[G]$-module. An element P of M is *almost fixed* (by G) if $(g + h - 2)P = 0$ with $g, h \in G$ implies that $(g - 1)P = (h - 1)P = 0$.

The module M is almost fixed if $(g + h - 2)M = 0$ with $g, h \in G$ implies that $(g - 1)M = (h - 1)M = 0$.

Remark 2.2. If $G = G_K$ is the absolute Galois group of a field K, we will often use the term *almost rational* instead of almost fixed.

We will be particularly interested in the set of almost rational *torsion points* of M.

Example 2.3. *The set of almost rational torsion points of $\mathbf{G}_m(\overline{\mathbf{Q}})$ is μ_6, the group of sixth roots of unity.*

The proof is left as an exercise for the reader (or see [2, Lemma 3.14]).

We now prove some elementary lemmas concerning almost fixed elements and almost fixed modules.

Lemma 2.4. *Let P be an almost fixed element of the $\mathbf{Z}[G]$-module M.*

1. *If $\sigma \in G$, then σP is almost fixed.*
2. *If $g \in G$ and $(g - 1)^2 P = 0$, then $(g - 1)P = 0$.*

[3] Notice how we are using that J is both the Albanese and Picard variety for X. The interplay between the two properties of J lies behind many of the geometric results discussed in this paper.

Proof. For the first part, notice that if $(g+h-2)\sigma P = 0$, then

$$(\sigma^{-1}g\sigma + \sigma^{-1}h\sigma - 2)P = 0,$$

which implies that $(\sigma^{-1}g\sigma - 1)P = (\sigma^{-1}h\sigma - 1)P = 0$. Therefore both g and h fix σP, as desired.

For the second statement, we are given that $(g^2 - 2g + 1)P = 0$. Multiplying on the left by g^{-1}, we find that $(g + g^{-1} - 2)P = 0$, and therefore $(g-1)P = 0$ by the definition of "almost fixed." □

Lemma 2.5. *Let M be a $\mathbf{Z}[G]$-module. If M is generated by almost fixed elements, then M is almost fixed.*

Proof. Let $P_1, \ldots, P_k$ be almost fixed elements that generate M as a $\mathbf{Z}[G]$-module, and let g, h be elements of G such that $(g+h-2)M = 0$. Then $(g+h-2)(\sigma P_i) = 0$ for all $\sigma \in G$ and all $i = 1, \ldots, k$. By Lemma 2.4, each σP_i is almost fixed, and therefore both g and h fix all of the σP_i. As the σP_i generate M as a $\mathbf{Z}$-module, it follows that both g and h fix every element of M. Therefore M is almost fixed. □

Remark 2.6. It is not true that if M is almost fixed then every element of M is almost fixed. For example, let M be the 2-dimensional $(\mathbf{Z}/5\mathbf{Z})$-vector space $(\mathbf{Z}/5\mathbf{Z})^2$, and let $G = (\mathbf{Z}/4\mathbf{Z})$ act on M by sending a generator to $A := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. A short computation shows that M is almost fixed, but the vector $v := \begin{bmatrix} 2 \\ 1 \end{bmatrix}$ is not, since $Av + A^2v = 2v$ but $Av \neq v$.

Let us return to the geometric situation of Lemma 2.1, so that K is a field, $G_K = \mathrm{Gal}(K^{\mathrm{sep}}/K)$ is the absolute Galois group of K, and X/K is a curve of genus $g \geq 2$, embedded in its Jacobian J via a K-rational Albanese map.

If $P \in X(\overline{K})$, then following A. Tamagawa, we say that the pair (X, P) is *exceptional* if X is hyperelliptic and P is a hyperelliptic branch point on X.

The following is a reformulation of Lemma 2.1 using our new terminology.

Lemma 2.7. *Let P be a $\overline{K}$-valued point of X. Then either (X, P) is exceptional, or P is almost rational.*

We illustrate the usefulness of the notion of almost rationality by presenting a short proof of the Manin–Mumford conjecture.

The proof exploits the following deep result[4] due to Serre.

[4]This result was presented in Serre's Collège de France lectures (1985–1986), but the proof has not yet been published. The main theorems of [12] and [19] both depend on this result.

Theorem 2.8. *Let K be a finitely generated field of characteristic zero. Let A/K be an abelian variety of dimension g, and let $\rho : G_K \to \mathbf{GL}_{2g}(\hat{\mathbf{Z}})$ denote the Galois representation arising from the adelic Tate module of A. Let $\hat{\mathbf{Z}}^* \subset \mathbf{GL}_{2g}(\hat{\mathbf{Z}})$ denote the subgroup of homotheties. Then the group $\hat{\mathbf{Z}}^*/\left(\rho(G_K) \cap \hat{\mathbf{Z}}^*\right)$ has finite exponent.*

We will also need the following lemma (compare with Example 2.3):

Lemma 2.9. *Let e be a positive integer. Then there is a positive constant $C(e)$ such that for all integers $m > C(e)$, there exist $x, y \in (\mathbf{Z}/m\mathbf{Z})^*$ such that $x^e, y^e \neq 1$ but $x^e + y^e = 2$.*

Proof. By the Chinese remainder theorem, it suffices to consider the case where $m = p^k$ is a prime power.

If $k = 1$, we want to look at $\mathbf{F}_p$-rational points on the projective curve C defined by $x^e + y^e = 2$. By the Weil bounds, $\#C(\mathbf{F}_p) = p + 1 + O(\sqrt{p})$. Since the number of points $(x, y) \in C(\mathbf{F}_p)$ with one of x^e, y^e being 0 or 1 is at most $(e+1)^2$, the result follows in this case.

Finally, suppose $k \geq 2$. If $p > e$, Hensel's lemma guarantees the existence of $x, y \in \mathbf{Z}/p^k\mathbf{Z}$ such that $x^e = 1 + p^{k-1}$, $y^e = 1 - p^{k-1}$. Since $x^e y^e = 1$, we have $x, y \in (\mathbf{Z}/m\mathbf{Z})^*$. ☐

We can now prove the following finiteness result:

Theorem 2.10. *Let K be a finitely generated field of characteristic zero, and let A/K be an abelian variety. Then the set of almost rational torsion points on A is finite*[5]*.*

Proof. By Theorem 2.8, there exists a positive integer e such that the group $\hat{\mathbf{Z}}^*/\left(\rho(G_K) \cap \hat{\mathbf{Z}}^*\right)$ has exponent e. Let P be a torsion point on A of order $m > C(e)$. By Lemma 2.9, there exist $x, y \in (\mathbf{Z}/m\mathbf{Z})^*$ such that $x^e, y^e \neq 1$ but $x^e + y^e = 2$. Since $(\hat{\mathbf{Z}}^*)^e \subseteq \rho(G_K) \cap \hat{\mathbf{Z}}^*$, we can choose $g, h \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ such that g, h act on $A[m]$ as x^e and y^e, respectively. Then $(g + h - 2)P = 0$ but neither g nor h fixes P, so P is not almost rational. It follows that the set of almost rational torsion points on A is finite. ☐

The Manin–Mumford conjecture follows easily from 2.10:

Corollary 2.11. *Let K be as above, and let X be a curve of genus at least 2, embedded in its Jacobian J by an Albanese map. Then the set of torsion points on X is finite.*

---

[5] See also [5], in which the author classifies almost rational torsion points on semistable elliptic curves over $\mathbf{Q}$.

Proof. The set of hyperelliptic branch points on X is finite, as is the set of almost rational torsion points on J. The result therefore follows from Lemma 2.7. □

3. Ordinary semistable and almost unramified modules

In this section, R will denote the ring of integers in a finite *unramified* extension K of $\mathbf{Q}_p$, where p is an *odd* prime.[6]

We will denote by I the inertia subgroup of $G := \mathrm{Gal}(\overline{K}/K)$, and by I^{tame} the inertia subgroup of $\mathrm{Gal}(K^{\mathrm{tame}}/K)$, where K^{tame} is the maximal tamely ramified extension of K. Recall that the group $I^{\mathrm{wild}} := \mathrm{Gal}(\overline{K}/K^{\mathrm{tame}})$ is a pro-p group, and that I^{tame} is canonically isomorphic to the group $\varprojlim \mathbf{F}_{p^n}^*$, where the transition maps are given by taking norms.

For each $n \geq 1$, we denote by $I(n)$ the (normal) subgroup of I fixing all of the p^nth roots of unity in $\overline{K}$, and we let $I(\infty)$ be the intersection of $I(n)$ for all natural numbers n, so that $I(\infty)$ is the subgroup of I fixing all p-power roots of unity.

The motivation for the results in this section comes from the following observation:

Lemma 3.1. *Let X/K be a curve of genus at least 2, embedded in its Jacobian J via a K-rational Albanese map. Suppose that J is semistable, that $P \in X(\overline{K})$ is a torsion point of order prime to p, and that (X, P) is not exceptional. Then I fixes P, i.e., P is unramified.*

Proof. Grothendieck showed in [11, Proposition 3.5] that if A/K is a semistable abelian variety and $P \in A(\overline{K})$ has order prime to p, then $(\sigma - 1)^2 P = 0$ for all $\sigma \in I$. Therefore in our situation we have

$$\sigma P + \sigma^{-1} P - 2P = \sigma^{-1}(\sigma - 1)^2 P = 0$$

for all $\sigma \in I$. The result now follows from Lemma 2.7. □

We now make some definitions.

Definition 2. Let M be a $\mathbf{Z}[I]$-module. An element $P \in M$ (resp. M itself) is *almost unramified* if P (resp. M) is almost fixed with respect to the action of I.

In other words, M is almost unramified if and only if whenever $(g + h - 2)M = 0$ with $g, h \in I$, we have $(g - 1)M = (h - 1)M = 0$.

[6] For the case $p = 2$, see Tamagawa's paper [29].

Definition 3. A finite $\mathbf{Z}[I]$-module M is *ordinary semistable* if there exists an exact sequence of $\mathbf{Z}[I]$-modules

$$0 \to M' \to M \to M'' \to 0 \tag{1}$$

such that:

(i) I acts on M' via[7] the cyclotomic character χ
(ii) I acts trivially on M''.

For each finite $\mathbf{Z}[I]$-module M, there is a unique decomposition $M = M_p \oplus M_{\text{non-}p}$, where M_p has p-power order and $M_{\text{non-}p}$ has order prime to p. Using this notation, we have the following definition.

Definition 4. A finite $\mathbf{Z}[I]$-module M is *ordinary good* if it is ordinary semistable and, in addition, I acts trivially on $M_{\text{non-}p}$.

The definitions of ordinary good and ordinary semistable modules are motivated by the following:

Definition 5. An abelian variety A/K has *ordinary semistable reduction* if the connected component of the closed fiber of the Néron model of A over R is an extension of an ordinary abelian variety by a torus.

Theorem 3.2. *Let A be an abelian variety over K and let n be a positive integer.*

1. *If A has good ordinary reduction over R, then $A[n]$ is an ordinary good $\mathbf{Z}[I]$-module.*
2. *If A has ordinary semistable reduction over R, then $A[n]$ is an ordinary semistable $\mathbf{Z}[I]$-module.*

Proof. This is a consequence of Grothendieck's study in SGA7 of Galois actions on torsion points of semistable abelian varieties. See [29] for details and precise references. □

As a prototype of results to come, we have the following lemma (compare with Lemma 3.1):

Lemma 3.3. *Suppose M is an ordinary semistable and almost unramified $\mathbf{Z}[I]$-module of order prime to p. Then I acts trivially on M.*

Proof. Let M' and M'' be as in the definition of "ordinary semistable". Since the order of M' is prime to p and M' is cyclotomic, I acts trivially on M'. Since I acts trivially on M'' as well, it follows that $(g-1)^2M = 0$

[7] If N is a torsion abelian group, then N is naturally a $\hat{\mathbf{Z}}$-module. Also, the inertia group I comes equipped with a cyclotomic character $\chi : I \to \hat{\mathbf{Z}}^*$. It therefore makes sense to say that a torsion I-module N is cyclotomic: this means that $\sigma n = \chi(\sigma)n$ for all $\sigma \in I$ and $n \in N$. Note that if N is cyclotomic and has order prime to p, then I acts trivially on N, and that in general if N is cyclotomic, then I will act on N through its abelian quotient $I/I(\infty)$.

for all $g \in I$. But since M is also almost unramified, Lemma 2.4 tells us that $(g-1)M = 0$, so that I acts trivially on M, as desired. □

With an eye toward applying the results of this section to the study of ramified torsion points on curves, we now undertake an investigation of modules that are both almost unramified and ordinary semistable. All $\mathbf{Z}[I]$-modules which appear are assumed to be finite unless otherwise specified.

Lemma 3.4. *If M is an ordinary semistable and almost unramified $\mathbf{Z}[I]$-module, then $I(\infty)$ acts trivially on M. Therefore, the action of I on M factors through its abelian quotient $I/I(\infty) \cong \mathbf{Z}_p^*$.*

Proof. Since $I(\infty)$ acts trivially on both M' and M'' in the filtration (1) coming from the definition of "ordinary semistable," it follows that $(g-1)^2 M = 0$ for all $g \in I(\infty)$. That M is almost unramified then implies, by Lemma 2.4, that $I(\infty)$ acts trivially on M. □

Proposition 3.5. *Let M be an ordinary semistable and almost unramified $\mathbf{Z}[I]$-module. Let p^m be the order of M_p, and let g, h be elements of I such that $\chi(g) + \chi(h) \equiv 2 \bmod p^m$. Then $(g+h-2)M_p = 0$.*

Proof. Let $0 \to M' \to M \to M'' \to 0$ be the filtration of M given by (1), let $M'_p = M' \cap M_p$, and let M''_p be the image of M_p in M'' under the given surjection.

Then we have an exact sequence

$$0 \to M'_p \to M_p \to M''_p \to 0 \tag{2}$$

of modules of p-power order which again satisfies properties (i) and (ii) in the definition of "ordinary semistable."

Since I acts on M'_p via the cyclotomic character, and since we are assuming that $p > 2$, the subgroup $(M'_p)^I$ of inertia invariants in M'_p must be zero.

The identity $\chi(g)+\chi(h) = 2 \bmod p^m$ implies that $\alpha := g+h-2$ kills both M'_p and M''_p. Therefore α acts on M_p via a homomorphism $\phi : M''_p \to M'_p$. Since the action of I on M is abelian by Lemma 3.4, ϕ is a homomorphism of I-modules, and therefore (since I acts trivially on M'') the image of ϕ is contained in $(M'_p)^I = 0$. It follows that α kills M_p, as desired. □

Theorem 3.6. *Let M be an ordinary semistable and almost unramified $\mathbf{Z}[I]$-module.*

1. *The group $I(1)$ acts trivially on M.*
2. *If $p \geq 5$ and M is ordinary good, then I acts trivially on M.*

Proof. Let $g \in I(1)$. Since $\chi(g)$ is 1 mod p and $\chi : I \to \mathbf{Z}_p^*$ is surjective, we can find h in $I(1)$ such that $\chi(g) + \chi(h) = 2$ in $\mathbf{Z}_p$. By Proposition 3.5, $(g + h - 2)M_p = 0$, where M_p again denotes the p-primary part of M. Also, by Lemma 3.4 we know that $I(\infty)$ acts trivially on M, from which it follows by Lemma A.1 and the definition of "ordinary semistable" that the action of the pro-p group $I(1)/I(\infty)$ on $M_{\text{non-}p}$ is trivial. Therefore $(g+h-2)M = 0$. As M is almost unramified, it follows that $(g-1)M = 0$. This proves part 1 of the theorem.

To prove part 2, assume that $p \geq 5$ and that M is ordinary good. Then $g \in I$ acts trivially on M whenever we can solve the equation $\chi(g)+\chi(h) = 2$ in $\mathbf{Z}_p$, i.e., whenever $\chi(g)$ is not 2 mod p. Thus the set of $g \in I$ acting trivially on M forms a subgroup of I whose image H in $I/I(1)$ contains at least $p-2$ elements. Since $I/I(1)$ has order $p-1$ and $p \geq 5$, it follows that $H = I/I(1)$. Therefore I acts trivially on M. □

We take a moment to remind the reader of our running assumption that p is odd.

Proposition 3.7. *Let M be an ordinary semistable and almost unramified $\mathbf{Z}[I]$-module. Then M_p' is killed by p and $M_p = M_p' \oplus (M_p)^I$.*

Proof. By Theorem 3.6, $I(1)$ acts trivially on M. Since I acts via the p-adic cyclotomic character χ on M_p', it follows that $pM_p' = 0$.

To prove the second statement, consider the exact sequence

$$0 \to M_p' \to M_p \to M_p'' \to 0$$

given by (2). As we have already seen, $(M_p')^I = 0$. As I acts on M_p' through its abelian quotient $I/I(1)$, we can apply Sah's lemma (Lemma A.2) to an element g of I such that $\chi(g)$ is 2 mod p, and we see that $H^1(I, M_p') = 0$. Therefore the natural map $(M_p)^I \to (M_p'')^I = M_p''$ is an isomorphism, which is equivalent to the desired statement that $M_p = M_p' \oplus (M_p)^I$. □

Corollary 3.8. *In addition to the hypotheses of the proposition, suppose we are given an element $g \in I$ and an integer $r \in \mathbf{Z}$ such that $\chi(g) \equiv -r$ (mod p). Then $(g + r)(g + g^{-1} - 2)M = 0$.*

Proof. By Proposition 3.7, we have

$$M = M_p' \oplus (M_p)^I \oplus M_{\text{non-}p}$$

and $pM_p' = 0$, so it follows from the definition of "ordinary semistable" that

$$(g + r)(g - 1)^2 M = 0.$$

Therefore

$$g^{-1}(g + r)(g^2 - 2g + 1)M = 0,$$

which gives the desired result. □

Corollary 3.9. *Suppose M is an ordinary semistable and almost unramified cyclic $\mathbf{Z}[I]$-module, and that P is a generator. If I acts nontrivially on M, then the group of elements of I that fix P is precisely $I(1)$.*

Proof. We know by Theorem 3.6 that $I(1)$ acts trivially on M. Since I acts nontrivially on M but trivially on $M_{\text{non-}p}$ (by Lemma 3.3), p must divide the order of M. We then see from Proposition 3.7 that p exactly divides the order of M'_p, and that I acts on M'_p via the mod p cyclotomic character. In particular, we can use Proposition 3.7 to write P as $x+y$, where $x \in M'_p$ and $y \in M^I$. We must have $x \neq 0$, or else I would fix σP for all $\sigma \in I$ and therefore act trivially on M. It follows that $(g-1)P = (\chi(g)-1)x \neq 0$ for all $g \in I$ such that $\chi(g) \not\equiv 1 \pmod p$, i.e., for all $g \in I - I(1)$. □

4. Ramified torsion points on curves

As in the previous section, K denotes a finite unramified extension of $\mathbf{Q}_p$, with $p \neq 2$.

Throughout this section, X will denote a curve over K, embedded in its Jacobian J via a K-rational Albanese map.

In this section, we apply the results of section 3 to the study of torsion points on X. The idea, due to Tamagawa, is to use elements of the inertia group I which act nontrivially on a torsion point $P \in X(\overline{K})$ to produce rational functions on X of small degree.

We first recall some basic facts about algebraic curves which can be found, for example, in [10, III.5].

If $P \in X(\overline{K})$, we denote by $\mathrm{WM}(P)$ the *Weierstrass monoid* at P consisting of all nonnegative integers m such that there exists a rational function on X of degree exactly m having no poles outside P. It is clear from the definition that $0 \in \mathrm{WM}(P)$, and that if $a, b \in \mathrm{WM}(P)$ then $a+b \in \mathrm{WM}(P)$, so that $\mathrm{WM}(P)$ is indeed a monoid.

Let $\mathbf{N}$ denote the monoid $\{0, 1, 2, \ldots\}$ of nonnegative integers, together with the operation of addition. The complement of $\mathrm{WM}(P)$ in $\mathbf{N}$, which we denote by $\mathrm{WG}(P)$, is called the set of *Weierstrass gaps* at P. It follows from the Riemann–Roch theorem that $\mathrm{WG}(P)$ has exactly g elements. A point P on X is called a *Weierstrass point* if there exists $m \in \mathrm{WM}(P)$ such that $1 \leq m \leq g$, or equivalently, if $\mathrm{WG}(P) \neq \{1, 2, \ldots, g\}$. It is well known that a curve of genus $g \geq 2$ has at most $g^3 - g$ Weierstrass points.

We now investigate the implications of the results of the previous section for ramified torsion points on curves.

Part 2a of the following theorem was originally proved by Coleman using p-adic integration techniques. The rest of the theorem is due to Tamagawa.

Theorem 4.1. *Let X be a curve over K whose Jacobian J has ordinary semistable reduction, and suppose X is embedded in J using a K-rational point.*

Let P be a torsion point on X. Then:

1. *The group $I(1)$ fixes P.*

2a. *If $p \geq 5$ and J has good ordinary reduction, then P is unramified.*

2b. *If $p = 3$ and J has good ordinary reduction, then either P is unramified or $3 \in \mathrm{WM}(P)$.*

Proof. When (X, P) is exceptional, the result follows from Proposition B.1. So we may assume that (X, P) is not exceptional.

By Theorem 3.2, the $\mathbf{Z}[I]$-submodule M of J generated by P is ordinary semistable, and is ordinary good when J has good ordinary reduction. Since (X, P) is not exceptional, it follows from Lemmas 2.7 and 2.5 that M is almost unramified. Parts 1 and 2a therefore follow from Theorem 3.6.

For part 2b, note that if $\sigma \in I$ does not fix P, then $\sigma P - P$ has order p in J by Proposition 3.7. Therefore the divisor $p(\sigma P) - p(P)$ is principal. $\square$

Proposition 4.2. *Suppose J has ordinary semistable reduction, and let P be a torsion point of J lying on X which is ramified at p. Assume also that (X, P) is not exceptional. Let r be a positive integer such that $r \not\equiv 0, 1$, or $-1 \pmod p$. Then the integer $2r - 1$ lies in $\mathrm{WM}(P)$; i.e., there exists a rational function of degree $2r - 1$ on X with no poles outside P.*

Proof. Let M be the $\mathbf{Z}[I]$-module generated by P. Then as in the proof of Theorem 4.1, M is ordinary semistable and almost unramified. By hypothesis, I acts nontrivially on M. Also, by Corollary 3.9, $\sigma P \neq P$ for all $\sigma \in I$ such that $\chi(\sigma) \not\equiv 1 \pmod p$. Since χ is surjective, given any positive integer r such that $r \not\equiv 0 \pmod p$, we can find $\sigma \in I$ such that $\chi(\sigma) \equiv -r \pmod p$. If in addition $r \not\equiv 1$ or $-1 \pmod p$, then $\sigma^2 P \neq P$. By Corollary 3.8, we also know that $(\sigma + \sigma^{-1} - 2)(\sigma + r)P = 0$ in J. Multiplying this expression out, we find that there exists a rational function f on X whose divisor is

$$(\sigma^2 P) + (r - 2)(\sigma P) + r(\sigma^{-1} P) - (2r - 1)(P).$$

The proposition now follows from the fact that the degree of f is $2r - 1$, since P does not equal $\sigma^{-1} P$, σP, or $\sigma^2 P$. $\square$

The following is one of the main theorems of Tamagawa [29].

Theorem 4.3. *Assume that J has ordinary semistable reduction, that (X, P) is not exceptional, and that P is a ramified torsion point on X. Then:*

1. *If $p \geq 5$, then $g \leq 4$.*
2. *If $p \geq 7$, then $g \leq 3$.*
3. *If $p \geq 29$, then $g \leq 2$.*

Proof. Suppose, for example, that $p \geq 5$. Taking $r = 2, 3$ in Proposition 4.2, we see that $3, 5 \in \mathrm{WM}(P)$. By Lemma A.3, it follows that $\mathrm{WG}(P) \subseteq \{1, 2, 4, 7\}$, and therefore $g \leq 4$. Similarly, if $p \geq 7$, then taking $r = 4$ we find that 7 is also in $\mathrm{WM}(P)$, and therefore $\mathrm{WG}(P) \subseteq \{1, 2, 4\}$, so that $g \leq 3$. Finally, suppose $p \geq 29$ and $g = 3$. We know from Corollary 3.9 that the stabilizer of P in I is precisely $I(1)$. Therefore the set $\{\sigma P \mid \sigma \in I\}$ has $p - 1 \geq 28$ elements. Since $3 \in \mathrm{WG}(P)$, P must be a Weierstrass point, and therefore all of the points σP with $\sigma \in I$ must be Weierstrass points. Since there are at most $g^3 - g = 24$ Weierstrass points on X, this is a contradiction. □

We conclude this section with an intriguing open problem. The following conjecture was made by R. Coleman [6]:

Conjecture 4.4. *Let $p \geq 5$ be a prime number, and suppose that $K/\mathbf{Q}_p$ is an unramified finite extension. Let X/K be a curve of genus $g \geq 2$, embedded in its Jacobian via a K-rational Albanese map. Suppose furthermore that X has good reduction over K. Then every torsion point $P \in X(\overline{K})$ is unramified.*

In [6], Coleman proved this conjecture in the following cases:
(i) X has ordinary reduction
(ii) X has superspecial reduction
(iii) $p > 2g$.

The hypotheses of the conjecture are necessary—see [1, Appendix] for an example.

On the other hand, Theorem 4.3 shows that with a few more restrictions on the prime p, the conclusion of the conjecture remains true if X merely has ordinary semistable reduction over K. It would be interesting to try to use the Galois-theoretic methods surveyed in this paper to prove additional cases of Coleman's conjecture.

5. Torsion points on modular curves

In this section, we use the results of section 3 to give a short proof of the Coleman–Kaskel–Ribet conjecture.

We first recall some facts about the modular curves $X_0(p)$, for which a basic reference is Mazur [16].

Fix a prime number $p \geq 5$. The modular curve $X_0(p)$ is a compactified coarse moduli space for degree-p isogenies between elliptic curves.

As a Riemann surface, $X_0(p)$ can be thought of as the quotient of the complex upper half plane $\mathcal{H}$ by the action of the group $\Gamma_0(p)$, suitably compactified by adding the two cusps 0 and ∞. As an algebraic curve, $X_0(p)$ is defined over $\mathbf{Q}$ and the cusps 0 and ∞ are $\mathbf{Q}$-rational points.

From now on we assume that $p \geq 23$, which is equivalent to assuming that the genus g of $X_0(p)$ is at least 2.

To simplify notation, we let $X := X_0(p)$ and $J := J_0(p)$.

There is an involution w_p of X, called the Atkin–Lehner involution, which interchanges 0 and ∞. We note that w_p always has fixed points ([20, §2]).

The quotient of X by w_p will be denoted by $X_0^+(p)$, or simply X^+. Its genus will be denoted by g^+.

For $p \geq 23$, we have $g^+ = 0$ if and only if $p \in \{23, 29, 31, 41, 47, 53, 71\}$.

It is known (see [20]) that X is hyperelliptic if and only if either $g^+ = 0$ or $p = 37$.

For each $Q \in X(\overline{\mathbf{Q}})$, we can define an embedding i_Q of X into J by sending $P \in X(\overline{\mathbf{Q}})$ to the linear equivalence class of the degree-zero divisor $[(P) - (Q)]$.

We call i_∞ the *standard embedding* of X into J, and we let T_∞ be the set of torsion points on X in the standard embedding.

We now recall the Coleman–Kaskel–Ribet conjecture (see Theorem 1.4).

Theorem 5.1. *For all prime numbers $p \geq 23$,*

$$T_\infty = \begin{cases} \{0, \infty\} & \text{if} \quad g^+ > 0 \\ \{0, \infty\} \cup \{\text{hyperelliptic branch points}\} & \text{if} \quad g^+ = 0. \end{cases}$$

Before we can prove the conjecture, we need to review some more facts about X and J. We begin with some definitions and elementary facts, all of which can be found in [16].

The *cuspidal subgroup* C of J is the cyclic subgroup of J generated by the class of the degree-zero divisor $(0) - (\infty)$ on X.

The *Shimura subgroup* Σ of J is the kernel of the map $J_0(p) \to J_1(p)$ induced via Picard functoriality from the natural map $X_1(p) \to X_0(p)$.

Both C and Σ have order $n := (p-1)/(\gcd(p-1, 12))$.

The endomorphism ring of $J_{\overline{\mathbf{Q}}}$ contains (and in fact equals) the *Hecke algebra* $\mathbf{T}$ generated by w_p and by the Hecke operators T_l, with l prime and different from p.

The *Eisenstein ideal* is the ideal $\mathfrak{I}$ of $\mathbf{T}$ generated by w_p+1 and the differences $T_l-(l+1)$ for $l\neq p$. A maximal ideal $\mathfrak{m}$ of $\mathbf{T}$ is *Eisenstein* if it contains $\mathfrak{I}$.

The subgroup

$$J[\mathfrak{I}] := \{\, P\in J(\overline{\mathbf{Q}}) \mid tP=0 \text{ for all } t\in\mathfrak{I}\,\}$$

contains both C and Σ. We list below some additional properties of this subgroup which we will need—see [9] for a complete picture of $J[\mathfrak{I}]$ as a Galois module.

In addition to the above definitions and relatively simple facts, the proof of Theorem 5.1 will also require the following ten more difficult facts about X and J. For the reader's benefit, we provide references and/or sketch the proofs for each of these facts.

1: *J has good reduction outside p, and has purely toric (hence ordinary semistable) reduction at p.*
This is due to Igusa and Deligne–Rapoport. See [16, Theorem A.1] for a discussion and references.

2: *$J(\mathbf{Q})^{\mathrm{tors}}=C$.*
This is [16, Theorem 1].

3: *If $P\in X(\mathbf{Q})\cap J(\mathbf{Q})^{\mathrm{tors}}$, then $P\in\{0,\infty\}$.*
When $p\neq 37,43,67,163$, this is a consequence of the fact that, by [16, Theorem 7.1], $X(\mathbf{Q})=\{0,\infty\}$. For the four exceptional cases, see [7, Proof of Proposition 1.2].

4: *The natural map $\mathbf{Z}\to\mathbf{T}/\mathfrak{I}$ induces an isomorphism $\mathbf{Z}/n\mathbf{Z}\approx\mathbf{T}/\mathfrak{I}$.*
This is [16, II, Proposition 9.7].

5: *$J[\mathfrak{I}]$ is a free $\mathbf{T}/\mathfrak{I}$-module of rank 2.*
This follows from the analysis in [16, Ch. II, §16–18], as noted in [25, §3].

6: *The set of torsion points of $J(\overline{\mathbf{Q}})$ that are unramified at all primes above p is precisely $J[\mathfrak{I}]$.*
This is [25, Proposition 3.3].

7: *Let M be a finite torsion $\mathbf{T}[\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})]$-submodule of $J(\overline{\mathbf{Q}})$, and let V be a Jordan–Hölder factor of M. Let $\mathfrak{m}$ be the maximal ideal in $\mathbf{T}$ that annihilates V and consider V as a representation of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ over the field $\mathbf{T}/\mathfrak{m}$. If $\mathfrak{m}$ is Eisenstein, then V is one-dimensional and isomorphic to either $\mathbf{Z}/l\mathbf{Z}$ or μ_l, where l is the characteristic of $\mathbf{T}/\mathfrak{m}$. If $\mathfrak{m}$ is not Eisenstein, then V is isomorphic to the standard two-dimensional irreducible representation $\rho_{\mathfrak{m}}:\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})\to\mathbf{GL}_2(k)$ attached to $\mathfrak{m}$.*
See [16, Chapter II] for a proof, and [25, Theorem 2.1] for a discussion of the proof.

8: *Suppose $l\mid n$, and let I be an inertia subgroup at l of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. If M is a $\mathbf{Z}[I]$-module such that $M\subseteq J[\mathfrak{I}]$, then M is ordinary good.*

This follows from Fact 7, together with results of Oort and Tate on finite flat group schemes of prime order. See [29, Proposition 2.3, $(v) \Rightarrow (i)$] for details.

9: *If* $\mathfrak{m} \mid p$, *then* $\rho_{\mathfrak{m}}$ *is not* finite *at* p *in the sense of* [28, §2.8].
This is a consequence of Mazur's level-lowering theorem (see [26, Theorem 1.1]), since if $\rho_{\mathfrak{m}}$ were finite at p, it would have to be modular of level 1, which is impossible.

10: *If* $\mathfrak{m} \mid p$, *then* $\rho_{\mathfrak{m}}(I)$ *is non-abelian for every inertia group* I *of* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ *at* p.
We sketch an argument similar to the one given in [29, §4, (1-2)]: Let M be the $\mathbf{T}/\mathfrak{m}[I]$-module giving rise to $\rho_{\mathfrak{m}}$. Then M is ordinary semistable as a $\mathbf{Z}[I]$-module, so that M has a filtration $0 \to M' \to M \to M'' \to 0$ in which I acts trivially on M'' and on M' via χ. As in the proof of Proposition 3.7, if the action of I on M is abelian, then Sah's lemma (Lemma A.2) shows that $M = M' \oplus M''$, and therefore M is finite at p. This contradicts Fact 9.

Proof of Theorem 5.1:

Let P be a point of X such that $i_\infty(P)$ is torsion.

When (X, P) is exceptional, the result follows from [7, Proposition 1.1][8]. So we will assume from now on that (X, P) is not exceptional.

By Fact 3, it is enough to prove that P is defined over $\mathbf{Q}$.

Claim 1: P is unramified at p.

Proof.

Let I be an inertia subgroup at p of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. Since J has ordinary semistable reduction at p by Fact 1, and since (X, P) is not exceptional, it follows from Theorem 3.6 that $I(1)$ fixes P. Applying the same argument to every conjugate of P, we see that I acts on the $\mathbf{T}[\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})]$-module M generated by P through its abelian quotient $I/I(1)$.

If p divides the order of M, then I acts through an abelian quotient on some Jordan–Hölder factor V of M associated to a maximal ideal $\mathfrak{m}$ of residue characteristic p. But Fact 10 tells us that the action of I on V is necessarily non-abelian, a contradiction.

---

[8]We briefly recall the argument. For $p \neq 37$, the fact that the hyperelliptic branch points are torsion points in the embedding i_∞ follows directly from the fact that in those cases, w_p coincides with the hyperelliptic involution. For if P is fixed by w_p, then since the hyperelliptic involution acts as -1 on J, we have

$$2[(P) - (\infty)] = [(P) - (\infty)] + [w_p(P) - w_p(0)] = [(0) - (\infty)],$$

which is torsion. The case $p = 37$ is more complicated, and follows from explicit calculations found in [18, §5].

Therefore M has order prime to p. By Lemma 3.3, it follows that I acts trivially on M. Since this is true for all inertia groups I at p, it follows that P is unramified at p. $\square$

Claim 2: $i_\infty(P) \in J[\mathfrak{I}]$.

Proof. This follows from Fact 6 and Claim 1. $\square$

Claim 3: If P is not a cusp then $g^+ = 0$.

Proof. Let $Q := i_\infty(P)$. Since w_p interchanges the two cusps on X, there is a unique cusp on X^+, which we also call ∞. So the fiber of the degree two map $\pi : X \to X^+$ over ∞ is just $\{0, \infty\}$. Let J^+ be the Picard (Jacobian) variety of X^+. The fact that J^+ is also the Albanese variety of X^+ implies there is a commutative diagram

$$\begin{array}{ccc} X & \xrightarrow{i_\infty} & J \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\pi_*} \\ X^+ & \xrightarrow{i_\infty} & J^+ \end{array}$$

If $\pi^* : J^+ \to J$ denotes the map induced by Picard functoriality, then the composite map $\pi^* \circ \pi_* : J \to J$ is the map $1 + w_p$. Also, π^* is injective; this is a consequence (see [3, Lemma 6]) of the fact that w_p has fixed points. Since $\mathfrak{I}$ contains $1 + w_p$, it follows that if $Q \in J[\mathfrak{I}]$, then Q is sent to zero under the projection π_*.

Therefore, when $g^+ > 0$ (so that the map $i_\infty : X^+ \to J^+$ is an embedding), we have $P = 0$ or $P = \infty$ as desired. $\square$

Claim 4: P is unramified at 2 and 3.

Proof. By Claim 3, we may assume that $g^+ = 0$, i.e., that p belongs to the set of prime numbers $\{23, 29, 31, 41, 47, 53, 71\}$. An explicit calculation shows that $3 \nmid n$, and that $2 \mid n$ if and only if $p = 41$.

So by Claim 2 and Fact 7, we are reduced to the case $p = 41$, where we have $n = 10$. We need to show in this case that P is unramified at 2. Since $4 \nmid n$, it follows from Fact 5 that M_2 is killed by 2.

Let I be an inertia group of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ at 2, and suppose there exists $\sigma \in I$ such that $\sigma P \neq P$. Since J has good reduction at 2, I acts trivially on $M_{\text{non-2}}$, so $\sigma Q - Q \in M_2$, and therefore $2(\sigma Q - Q) = 0$. It follows that the divisor $2(\sigma P) - 2(P)$ is principal on X, so (X, P) is exceptional, a contradiction. $\square$

Claim 5: P is defined over $\mathbf{Q}$.

Proof. By Fact 7(i) and Claim 2, P is unramified at all primes $l \nmid n$. It suffices to show that P is unramified at all $l \geq 5$ such that $l \mid n$. Fix such a prime l and an inertia group I at l in $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. Let M be the $\mathbf{Z}[I]$-submodule of $J[\mathfrak{I}]$ generated by Q. By Fact 8, M is an ordinary good $\mathbf{Z}[I]$-module. Also, since (X, P) is not exceptional, it follows from Lemma 2.7 that M is almost unramified. Theorem 3.6 then implies that I acts trivially on M, as desired. □

This concludes the proof of Theorem 5.1.

For generalizations to torsion points on X in noncuspidal Albanese embeddings into J, and to certain other modular curves, plus an application to Mordell–Weil ranks, see [2, §4].

Appendix A. Some elementary algebraic results

For the sake of completeness, we give the statements and proofs of some elementary algebraic results used in this paper.

Lemma A.1. *Let G be a group, and let M be a finite $\mathbf{Z}[G]$-module of order prime to p. Suppose that the action of G on M factors through a finite p-group G', and that $(g-1)^2 = 0$ for all $g \in G$. Then G acts trivially on M.*

Proof. Let $q = p^k$ be the order of G', and let $g \in G$. Then

$$0 = (g^q - 1)M = ([1 + (g-1)]^q - 1)M = q(g-1)M$$

by the binomial theorem. Since M has order prime to p, it follows that $(g-1)M = 0$. □

The following elementary result from group cohomology is known as Sah's lemma. Our proof is adapted from [15, Lemma 8.8.1].

Lemma A.2 (Sah's lemma)**.** *Let G be a group, let M be a G-module, and let g be in the center of G. Then $H^1(G, M)$ is killed by the endomorphism $x \mapsto gx - x$ of M. In particular, if this endomorphism is an automorphism, then $H^1(G, M) = 0$.*

Proof. Let $f : G \to M$ be a 1-cocycle. Then for all $h \in G$,

$$f(h) = f(ghg^{-1}) = f(g) + gf(hg^{-1}) = f(g) + g[f(h) + hf(g^{-1})].$$

Therefore

$$(g-1)f(h) = gf(h) - f(h) = -f(g) - ghf(g^{-1}) = -f(g) - hgf(g^{-1}).$$

But the cocycle condition implies that $f(1) = 0$, so

$$0 = f(1) = f(gg^{-1}) = f(g) + gf(g^{-1})$$

and therefore $(g-1)f(h) = (h-1)f(g)$, so that $(g-1)f$ is a coboundary. $\square$

Recall that a *monoid* is a a set S together with an associative composition law on S and an identity element $e \in S$.

We denote by $\mathbf{N}$ the monoid consisting of all nonnegative integers.

If $a_1, \dots, a_k \in \mathbf{N}$, we denote by $\langle a_1, \dots, a_k \rangle$ the monoid

$$\{n_1 a_1 + \cdots + n_k a_k \mid n_i \in \mathbf{N}\}.$$

It is the smallest submonoid of $\mathbf{N}$ containing $a_1, \dots, a_k$.

The following result is sometimes called the "postage stamp lemma":

Lemma A.3. *If a, b are relatively prime positive integers and m is any integer such that $m \geq (a-1)(b-1)$, then $m \in \langle a, b \rangle$.*

Proof. Since no two of the b integers $m - ar$ $(0 \leq r \leq b-1)$ are congruent modulo b, one of them must be divisible by b, say $m - ar_0 = bs_0$. As

$$bs_0 = m - ar_0 \geq (a-1)(b-1) - a(b-1) = -b + 1,$$

we must have $s_0 \geq 0$, so that $m \in \langle a, b \rangle$ as claimed. $\square$

Appendix B. The exceptional case

In this appendix, K denotes a finite unramified extension of $\mathbf{Q}_p$ with $p \neq 2$, and X/K is a curve of genus at least 2, embedded in its Jacobian J via a K-rational Albanese map.

The following result, which is essentially [29, Proposition 3.1], was used in the proof of Theorem 4.1.

Proposition B.1. *Suppose J has ordinary semistable reduction. Let $P \in X(\overline{K})$ be a torsion point, and suppose (X, P) is exceptional. Then:*

1a. *$\sigma^2 P = P$ for all $\sigma \in I$.*

1b. *The group $I(1)$ fixes P.*

2. *If J has good ordinary reduction, then P is unramified.*

Proof. Let M be the $\mathbf{Z}[I]$-submodule of J generated by P. Since P is a Weierstrass point on X, so is σP, and therefore the divisors $2(P)$ and $2(\sigma P)$ on X are linearly equivalent for all $\sigma \in I$. It follows that $2(\sigma - 1)P = 0$ in M. Applying the same argument to every conjugate of P, we see that I acts trivially on $2M$. In particular, since p is odd, $(\sigma - 1)M_p = 0$ for all $\sigma \in I$.

Also note that by Lemma A.1, I^{wild} acts trivially on $M_{\text{non-}p}$, and therefore I acts on M through its quotient I^{tame}.

If J has ordinary good reduction, then $(\sigma - 1)M_{\text{non-}p} = 0$ for all $\sigma \in I$ and therefore I acts trivially on M as desired.

In general, since M is ordinary semistable, we have $(\sigma-1)^2 M_{\text{non-}p} = 0$ for all $\sigma \in I$. Since $(\sigma-1)M_p = 0$ as well, we see that in fact $(\sigma-1)^2 M = 0$ for all $\sigma \in I$. Adding this to the relation $2(\sigma-1)M = 0$, we find that $(\sigma^2-1)M = 0$ for all $\sigma \in I$. This proves (1a). Statement (1b) now follows from the fact that $I(1)$ is contained in the subgroup of I topologically generated by $\{\sigma^2 \mid \sigma \in I\}$. Explicitly: I acts on M through a finite quotient I' of I^{tame} isomorphic to $\mathbf{F}_{p^n}^*$ for some $n \geq 1$. The image of σ in I' has norm 1 in $\mathbf{F}_p$ if and only if $\sigma \in I(1)$. The result now follows from the fact that an element of $\mathbf{F}_{p^n}^*$ is a square if and only if its norm to $\mathbf{F}_p^*$ is a square. $\square$

References

[1] M. Baker, *Torsion points on modular curves.* Ph.D. thesis, University of California, Berkeley, 1999.

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

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

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

[5] F. Calegari, *Almost rational torsion points on elliptic curves.* International Math. Res. Notices **10** (2001), 487–503.

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

[7] R. F. Coleman, B. Kaskel, K. Ribet, *Torsion points on* $X_0(N)$. In Proceedings of a Symposia in Pure Mathematics, **66** (Part 1) Amer. Math. Soc., Providence, RI (1999), 27–49.

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

[9] J. Csirik, *On the kernel of the Eisenstein ideal.* J. Number Theory **92** (2002), 348–375.

[10] H. M. Farkas, I. Kra, *Riemann Surfaces* (second edition). Graduate Texts in Mathematics, vol. 71, Springer-Verlag, Berlin and New York, 1992.

[11] A. Grothendieck, *SGA7 I, Exposé IX*, Lecture Notes in Mathematics, vol. 288, Springer-Verlag, Berlin and New York, 1972, 313–523.

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

[13] M. Kim, K. Ribet, *Torsion points on modular curves and Galois theory*, preprint.

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

[15] S. Lang, *Fundamentals of Diophantine Geometry.* Springer-Verlag, Berlin and New York, 1983.

[16] B. Mazur, *Modular curves and the Eisenstein ideal.* Publ. Math. IHES **47** (1977), 33–186.

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

[18] B. Mazur, P. Swinnerton-Dyer, *Arithmetic of Weil curves.* Invent. Math. **25** (1974), 1–61.

[19] M. McQuillan, *Division points on semi-abelian varieties.* Invent. Math. **120** (1995), 143–159.

[20] A. P. Ogg, *Hyperelliptic modular curves.* Bull. Soc. Math. France **102** (1974), 449–462.

[21] B. Poonen, *Mordell–Lang plus Bogomolov.* Invent. Math. **137** (1999), 413–425.

[22] B. Poonen, *Computing torsion points on curves*, Experimental Math. **10** (2001), no. 3, 449–465.

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

[24] M. Raynaud, *Sous-variétés d'une variété abélienne et points de torsion*, in Arithmetic and Geometry, Vol. I, Progr. Math. 35, Birkhäuser, Boston, 1983, 327–352.

[25] K. RIBET, *Torsion points on $J_0(N)$ and Galois representations*, in "Arithmetic theory of elliptic curves" (Cetraro, 1997), 145–166, Lecture Notes in Math. **1716**, Springer-Verlag, Berlin and New York, 1999.

[26] K. RIBET, *On modular representations of* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ *arising from modular forms.* Invent. Math. **100** (1990), 431–476.

[27] D. E. ROHRLICH, *Points at infinity on the Fermat curves.* Invent. Math. **39** (1977), 95–127.

[28] J.-P. SERRE, *Sur les représentations modulaires de degré* 2 *de* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. Duke Math. J. **54** (1987), 179–230.

[29] A. TAMAGAWA, *Ramified torsion points on curves with ordinary semistable Jacobian varieties.* Duke Math. J. **106** (2001), 281–319.

[30] J.-P. WINTENBERGER, *Démonstration d'une conjecture de Lang dans des cas particuliers*, preprint.

Matthew H. BAKER
Department of Mathematics
University of Georgia
Athens, GA 30602-7403
USA
E-mail : `mbaker@math.uga.edu`

Kenneth A. RIBET
Department of Mathematics
University of California
Berkeley, CA 94720-3840
USA
E-mail : `ribet@math.berkeley.edu`