Computing Torsion Points on Curves

Bjorn Poonen

CONTENTS

This research was supported by NSF grant DMS-9801104, a Sloan Fellowship, and a Packard Fellowship. Part of it was done at the Isaac Newton Institute, where the author was supported by a Rosenbaum Fellowship.

1991 AMS Subject Classification: Primary, 11G30; Secondary, 14H25, 14K15, 14K20, 11G10

Keywords: torsion packet, torsion point, Manin–Mumford conjecture, Greenberg functor, Greenberg transform, p-adic integrals, hyperelliptic torsion packet, cuspidal torsion packet, Kummer surface

Let X be a curve of genus $g \geq 2$ over a field k of characteristic zero. Let $X \hookrightarrow A$ be an Albanese map associated to a point P_0 on X. The Manin–Mumford conjecture, first proved by Raynaud, asserts that the set T of points in $X(\bar{k})$ mapping to torsion points on A is finite. Using a p-adic approach, we develop an algorithm to compute T, and implement it in the case where $k = \mathbb{Q}$, $g = 2$, and P_0 is a Weierstrass point. Improved bounds on #T are also proved: for instance, in the context of the previous sentence, if in addition X has good reduction at a prime $p \geq 5$, then $\#T \leq 2p^3 + 2p^2 + 2p + 8$.

1. INTRODUCTION

Let X be a curve of genus $g \geq 2$ over a field k of characteristic zero. Suppose that X is embedded in its Jacobian A by the Albanese map ι associated to a basepoint $P_0 \in X(k)$. We write $X \cap A_{\text{tors}}$ for $X(\bar{k}) \cap A(\bar{k})_{\text{tors}}$, where $A(\bar{k})_{\text{tors}}$ is the set of points of finite order in the group $A(\bar{k})$ of geometric points of A. If we define an equivalence relation on $X(\bar{k})$ by writing $P \sim Q$ if and only if there exists $n \geq 1$ such that the divisor $n(P-Q)$ is principal, then $X \cap A_{\text{tors}}$ is the equivalence class of P_0; it is called a *torsion packet*.

The Manin–Mumford conjecture, first proved by Raynaud [1983], says that $X \cap A_{\text{tors}}$ is finite. Many different proofs were given later, by Coleman [1987], Hindry [1988], Hrushovski [$\geq$ 2001], Buium [1996], Ullmo [1998], and Ribet [1999]. All known proofs use Galois action in some way, the rough idea being that if a torsion point P lies on X, then X must pass through all Galois conjugates of P as well, which contradicts the geometry in some way if the orbit is "large." In the proofs of Raynaud, Coleman, Hrushovski, and Buium, p-adic methods also play a significant role. In Ullmo's proof, the Manin–Mumford conjecture is a corollary of the more general "Bogomolov conjecture" about points of small height on curves; here the Galois ingredient is the

"equidistribution of small points" proved by Szpiro, Ullmo, and Zhang [Szpiro et al. 1997]. The Manin–Mumford conjecture has been generalized in many directions; see [Poonen 1999] or the detailed survey [Tzermias 2000], for instance.

Our goal is to describe an algorithm for *computing* $X \cap A_{\mathrm{tors}}$, when X is presented by explicit equations over a number field k. We make the algorithm explicit enough in the case that $k = \mathbb{Q}$, $g = 2$, and P_0 is a Weierstrass point, that it can be programmed in GP-PARI. The algorithm is in the spirit of the proofs of Raynaud and Buium: after using Coleman's study [1987] of ramified torsion points on curves, we bound the residue classes modulo p^2 on the curve in which torsion points might lie. The technical ingredients include the Greenberg functor [Greenberg 1961; 1963] and Coleman's p-adic abelian integrals [Coleman 1985].

Many efforts have been made to compute $X \cap A_{\mathrm{tors}}$ for various curves: modular curves [Coleman et al. 1999; Baker 2000; Tamagawa 2001], Fermat curves [Coleman 1986; Coleman et al. 1998], abelian étale coverings of $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ [Coleman 1989] and other isolated low genus curves [Voloch 1997; Boxall and Grant 2000]. Our approach, which is partly inspired by a calculation of Voloch [1997] for a special situation, has the advantage of being less reliant on special properties of the curve, so that it is easier to automate. Our computer program succeeded in computing $X \cap A_{\mathrm{tors}}$ for all curves attempted except one: see Section 14. Perhaps even that one would have succumbed if we had had a little more memory at our disposal, or if we had used a package with a more memory-efficient approach to factoring high degree polynomials over small finite fields.

The sections up to Section 4 outline the theoretical basis for the algorithm. Sections 5 through 11 deal with making the method explicit and efficient. Section 12 gives some general bounds for torsion points on genus 2 curves in terms of only a prime of good reduction. The existence of such bounds in theory, for every genus, was already known to Raynaud [1983, p. 208, bottom], and explicit bounds were given by Buium [1996], but the bounds are enough improved here that they can actually be used to simplify the computation; this is explained in Section 13. Section 14 gives a list of curves whose torsion packets were computed by our program.

2. NOTATION

For any scheme X over $\mathbb{Z}_p$, let $X_s := X \times \mathbb{F}_p$ denote the special fiber.

For any commutative group variety G over $\mathbb{F}_p$, let $F = F_G$ denote the Frobenius endomorphism. Let $V = V_G$ denote Verschiebung, the unique endomorphism satisfying $FV = VF = p$ in $\operatorname{End} G$. For instance, if G is a g-dimensional abelian variety, then F and V are isogenies of degree p^g. If $\varphi \in \operatorname{End} G$, then $G[\varphi]$ denotes the group scheme kernel of φ, and $\#G[\varphi]$ denotes its order as a group scheme.

3. GREENBERG TRANSFORM

Let k be a perfect field of characteristic $p > 0$. The Greenberg functor Gr_n of level n takes a scheme X locally of finite type over the ring $W_n(k)$ of length n Witt vectors, and associates to it a scheme $\mathcal{X}$ locally of finite type over k, such that $X(W_n(L)) = \mathcal{X}(L)$ for any k-algebra L, functorially in X and L. We call $\mathcal{X}$ the *level n Greenberg transform* of X. See [Bosch et al. 1990, p. 276] for a brief exposition, or see Greenberg's original papers [1961; 1963] for more details. Also see [Buium 1996], where the Greenberg transform is related to "p-jet spaces." The construction is similar to that of "Weil restriction of scalars." If X is smooth of relative dimension d over $W_n(k)$, then $\mathcal{X}$ is smooth of relative dimension nd over k. Furthermore, Gr_n respects open and closed immersions. An example: if X is the curve $f(x, y) = 0$ in $\mathbb{A}^2_{W_2(k)}$, then $\mathcal{X} = \mathrm{Gr}_2(X)$ is the subscheme of $\mathbb{A}^4_k$ defined by the two Witt coordinate equations in x_0, x_1, y_0, y_1 obtained when x and y are replaced by length-2 Witt vectors $[x_0, x_1]$ and $[y_0, y_1]$, and $f([x_0, x_1], [y_0, y_1]) = 0$ is expanded using the rules for Witt vector arithmetic.

Now suppose that A is an abelian scheme of relative dimension g over $\mathbb{Z}_p$, and let A_s denote its special fiber. (We could work with more general base rings, but $\mathbb{Z}_p$ will suffice for our intended application.) Let $\mathcal{A} = \mathrm{Gr}_2(A \times \mathbb{Z}/p^2)$. The functoriality of Gr_2 gives $\mathcal{A}$ the structure of an algebraic group over $\mathbb{F}_p$, but $\mathcal{A}$ is not an abelian variety. Instead $\mathcal{A}$ fits into an exact sequence of algebraic groups

$$0 \to L \to \mathcal{A} \to A_s \to 0 \tag{3–1}$$

where L, the "kernel of reduction," is the vectorial group associated to the pullback of the tangent

bundle of A_s by the absolute Frobenius morphism. (This is a special case of [Buium 1996, Proposition 2.4].) We have $L \cong \mathbb{G}_a^g$ over $\mathbb{F}_p$, but the isomorphism depends on a choice of basis for $\mathrm{Lie}(A_s)$, or dually, on a choice of basis for $H^0(A_s, \Omega^1_{A_s/\mathbb{F}_p})$. In particular, $\dim \mathcal{A} = 2g$. The exact sequence (3–1) does not split in general, and the class of the extension in $\mathrm{Ext}(A_s, L)$ depends on $A \times \mathbb{Z}/p^2$, not only on A_s.

Let $\mathbb{Z}_p^{\mathrm{unr}}$ denote the valuation ring of the maximal unramified extension $\mathbb{Q}_p^{\mathrm{unr}}$ of $\mathbb{Q}_p$. Define the "mod p^2 reduction homomorphism" π as the composition

$$\pi : A(\mathbb{Q}_p^{\mathrm{unr}}) = A(\mathbb{Z}_p^{\mathrm{unr}}) \to A(\mathbb{Z}_p^{\mathrm{unr}}/p^2) \cong \mathcal{A}(\bar{\mathbb{F}}_p),$$

We obtain a similar function $\pi : X(\mathbb{Q}_p^{\mathrm{unr}}) \to \mathcal{X}(\bar{\mathbb{F}}_p)$ for any proper scheme X over $\mathbb{Z}_p$.

4. SUMMARY OF PROOF OF THE MANIN–MUMFORD CONJECTURE

We now sketch a p-adic proof of the Manin–Mumford Conjecture, mainly following [Buium 1996]. The Galois ingredient is a ramification-bounding result of Coleman [1987]. Our treatment borrows also a little from [Hrushovski $\geq$ 2001] and we paraphrase to suit our purposes.

Let X be a smooth, projective, geometrically integral curve of genus $g \geq 2$ over a field k of characteristic zero. Suppose that X is embedded in its Jacobian A using a basepoint $P_0 \in X(k)$. We write $X \cap A_{\mathrm{tors}}$ for $X(\bar{k}) \cap A(\bar{k})_{\mathrm{tors}}$. and we wish to prove that this set is finite. Eventually we hope to calculate it.

We may assume that k is finitely generated over $\mathbb{Q}$. By specialization, we may assume that $[k : \mathbb{Q}] < \infty$. We may then find a degree 1 place $k \to \mathbb{Q}_p$ for some $p > 2g$, at which X has good reduction. For most of the rest of this paper, we denote by X and A the resulting models over $\mathbb{Z}_p$. Let

$$\mathcal{X} = \mathrm{Gr}_2(X \times \mathbb{Z}/p^2), \quad \mathcal{A} = \mathrm{Gr}_2(A \times \mathbb{Z}/p^2).$$

Thanks to the embedding $X \hookrightarrow A$ and the functoriality of Gr_2 we can regard $\mathcal{X}$ as a closed subscheme of $\mathcal{A}$.

The finiteness of $X \cap A_{\mathrm{tors}}$ clearly follows from the four lemmas below. The first, which is also the hardest, is a special case of a theorem of Coleman [1987]:

Lemma 4.1. *If X is a curve of genus g over $\mathbb{Q}_p$ with good reduction and $p > 2g$, then $X \cap A_{\mathrm{tors}}$ is unramified, i.e., contained in $A(\mathbb{Q}_p^{\mathrm{unr}})_{\mathrm{tors}}$.*

Lemma 4.2. *The restriction of π to $A(\mathbb{Q}_p^{\mathrm{unr}})_{\mathrm{tors}}$ is injective.*

Lemma 4.3. *There exists a surjective homomorphism $\Phi : \mathcal{A} \to \mathbb{G}_a^g$ such that $\pi(A(\mathbb{Q}_p^{\mathrm{unr}})_{\mathrm{tors}}) \subseteq \ker \Phi$.*

Lemma 4.4. *If $\Phi : \mathcal{A} \to \mathbb{G}_a^g$ is a surjective homomorphism, then $\mathcal{X} \cap \ker \Phi$ is finite (over $\operatorname{Spec} \mathbb{F}_p$).*

Lemma 4.2 follows from formal group considerations. If $p > 2$, we have the well-known stronger result (proved in the same way; see [Katz 1981, Appendix]) that the reduction map $A(\mathbb{Q}_p^{\mathrm{unr}})_{\mathrm{tors}} \to A_s(\bar{\mathbb{F}}_p)$ on unramified torsion is injective.

We will give a short proof of Lemma 4.3 here, using an idea of Hrushovski [$\geq$ 2001]. This proof has the additional advantage of presenting Φ very explicitly. Later, for the sake of computational efficiency, we will reprove the lemma (in a manner closer to Buium's proof), giving a Φ for which the intersection in Lemma 4.4 will be much smaller.

Proof of Lemma 4.3. Let $P(x) \in \mathbb{Z}[x]$ be the characteristic polynomial of Frobenius acting on the Tate module $T_l A_s$ for some prime $l \neq p$. The fact that $P(F_{A_s}) = 0$ implies that $P(F_{\mathcal{A}}) \in \mathrm{End}\,\mathcal{A}$ maps $\mathcal{A}$ into $L \cong \mathbb{G}_a^g$. The composite map $L \hookrightarrow \mathcal{A} \to L$ is surjective, since if we write L as a product of factors isomorphic to $\mathbb{G}_a$, then $P(F_{\mathcal{A}})$ acts as a nonzero polynomial

$$x \mapsto x^{p^{2g}} + a_1 x^{p^{2g-1}} + \cdots + a_{2g} x$$

on each one.

We claim that $\Phi := P(F_{\mathcal{A}}) \in \mathrm{Hom}(\mathcal{A}, \mathbb{G}_a^g)$ satisfies the requirements. Let Frob denote the abstract group endomorphism of $A(\mathbb{Q}_p^{\mathrm{unr}})$ induced by the Frobenius automorphism in $\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{unr}}/\mathbb{Q}_p)$. Then $P(\mathrm{Frob})$ maps $A(\mathbb{Q}_p^{\mathrm{unr}})_{\mathrm{tors}}$ into the kernel of reduction. But $p > 2$ (we assumed $p > 2g$), so as remarked above, there is no nontrivial unramified torsion in the kernel of reduction. Hence $P(\mathrm{Frob})$ kills $A(\mathbb{Q}_p^{\mathrm{unr}})_{\mathrm{tors}}$, and $P(F_{\mathcal{A}})$ kills its image in $\mathcal{A}$. □

Lemma 4.4 should not be too surprising, since $\mathcal{X}$ and $\ker \Phi$ are subschemes of dimensions 2 and g respectively, in a variety of dimension $2g$.

Proof of Lemma 4.4. Dimension of maximal connected linear subgroup is additive in exact sequences of commutative algebraic groups; hence from $0 \to \ker\Phi \to \mathcal{A} \to \mathbb{G}_a^g \to 0$ we see that $\ker\Phi$ is proper over $\mathbb{F}_p$. On the other hand, since $g \geq 2$, Proposition 1.10 of [Buium 1996] shows that $\mathcal{X}$ is affine! Since $\ker\Phi$ and $\mathcal{X}$ are both closed subschemes of $\mathcal{A}$, their intersection is proper and affine, hence finite. □

5. OTHER MAPS TO THE JACOBIAN

For the computations to come, we will want p to be as small as possible. Given X over $\mathbb{Q}$, a smaller p can sometimes be used if we do not insist on the existence of a point $P_0 \in X(\mathbb{Q}_p)$. If instead we suppose an element $D \in \mathrm{Pic}(X \times \mathbb{Q}_p)$ of degree δ prime to p is given, we may use the morphism $\iota : X \to A$ that sends a point $Q \in X(\overline{\mathbb{Q}}_p)$ to the class of $\delta Q - D$. Denote also by ι the induced morphism $\mathcal{X} \to \mathcal{A}$.

We observe now that the proof of the previous section can be adapted to this situation. By [Coleman 1987, Main Theorem], the torsion packet $\iota^{-1}(A_{\mathrm{tors}})$ is contained in $X(\mathbb{Q}_p^{\mathrm{unr}})$: this is the needed extension of Lemma 4.1. Lemmas 4.2 and 4.3 do not need to be extended. We now extend Lemma 4.4 by proving that $(\Phi \circ \iota)^{-1}(O)$ is finite. Since X has good reduction, the Weil bounds and Hensel's Lemma produce $\mathbb{Q}_p$-rational divisors on X of any sufficiently large degree, and in particular, we may find $D_1 \in \mathrm{Pic}(X \times \mathbb{Q}_p)$ of degree 1. The embedding determined by D_1 induces a closed immersion $\beta : \mathcal{X} \to \mathcal{A}$. The composition $\Phi \circ \iota$ equals $\Psi \circ \beta$ where Ψ is $\delta\Phi$ followed by a translation. But $\delta\Phi$ is another surjective homomorphism $\mathcal{A} \to \mathbb{G}_a^g$, so the fibers of Ψ are proper, as in the proof of Lemma 4.4, and we conclude as before that $(\Phi \circ \iota)^{-1}(O)$ is both affine and proper, making it finite.

Remark. We will eventually be interested in the *hyperelliptic torsion packet* T of a hyperelliptic curve X: T consists of the points $P \in X(\overline{\mathbb{Q}}_p)$ such that the class of $P - P_0$ in $A(\overline{\mathbb{Q}}_p)$ is torsion, for (any) fixed Weierstrass point P_0 on X. Then T also equals $\iota^{-1}(A_{\mathrm{tors}})$, where ι is defined using the class D of $2P_0$. Because D is the pullback of the unique degree 1 element of $\mathrm{Pic}(\mathbb{P}^1)$ under the canonical map $X \to \mathbb{P}^1$, ι is defined over $\mathbb{Q}_p$ even though P_0 might not be.

6. IMPROVED HOMOMORPHISMS

As a measure of the complexity of a surjective homomorphism $\Phi : \mathcal{A} \to \mathbb{G}_a^g$, we let $\mathrm{size}(\Phi)$ denote the degree of the finite composite morphism $L \hookrightarrow \mathcal{A} \to \mathbb{G}_a^g$. For computational efficiency, it will help to find Φ for which $\mathrm{size}(\Phi)$ is as small as possible.

The homomorphism $P(F)$ used in the proof of Lemma 4.3 has size p^{2g^2}, which is too large once $g > 1$. One can reduce this to p^{g^2} by using $F^{-g}P(F) \in \mathrm{End}\,\mathcal{A}$ instead. (The divisibility of $P(F)$ by F^g in $\mathrm{End}\,A$ follows from the p-power divisibility of the low order coefficients of $P(x)$ forced by the functional equation of the zeta function.) But the size can be reduced further, at least when $g > 1$. The following bounds the size of the best possible Φ:

Lemma 6.1. *Denote by H the Zariski closure of the image $\pi(A(\mathbb{Q}_p^{\mathrm{unr}})_{\mathrm{tors}})$ in $\mathcal{A}$. Then $\mathcal{A}/H \cong \mathbb{G}_a^g$, and the quotient map $\Phi : \mathcal{A} \to \mathcal{A}/H$ has size dividing p^g.*

Proof. First we show that $p\mathcal{A}$ is a subgroup of finite index in H, and we bound the index by $p^k := \#A[p](\mathbb{Q}_p^{\mathrm{unr}})$. Multiplication-by-$p$ on $\mathcal{A}$ kills L, so the subgroup $p\mathcal{A}$ of $\mathcal{A}$ is a quotient of the abelian variety A_s. On the other hand, $p\mathcal{A}$ surjects onto $pA_s = A_s$, so $p\mathcal{A}$ must be an abelian variety isogenous to A_s. The subset $\pi(pA(\mathbb{Q}_p^{\mathrm{unr}})_{\mathrm{tors}})$ of $p\mathcal{A}$ is Zariski dense, since by Lemma 4.2 it contains l^{2g} points of order dividing l for any integer l prime to p, namely the points in $\pi(A[l](\mathbb{Q}_p^{\mathrm{unr}}))$. Any subgroup $G \subseteq (\mathbb{Q}/\mathbb{Z})^{2g}$ satisfies $\#(G/pG) \leq \#G[p]$; applying this to $A(\mathbb{Q}_p^{\mathrm{unr}})_{\mathrm{tors}} \subseteq A(\overline{\mathbb{Q}}_p)_{\mathrm{tors}}$ shows that $pA(\mathbb{Q}_p^{\mathrm{unr}})_{\mathrm{tors}}$ has index at most p^k in $A(\mathbb{Q}_p^{\mathrm{unr}})_{\mathrm{tors}}$. Applying π and taking Zariski closures, we find that $p\mathcal{A}$ is of index at most p^k in H.

Next we bound $\#\ker(L \to \mathcal{A}/p\mathcal{A})$. Verschiebung is zero on $\mathbb{G}_a$ and on L. Hence connecting two rows of (3–1) with vertical maps equal to V and applying the Snake Lemma yields an exact sequence

$$0 \to L \to \mathcal{A}[V] \to A_s[V] \to L \to \mathcal{A}/V\mathcal{A} \to A_s/VA_s = 0, \quad (6\text{–}1)$$

which, together with $V\mathcal{A} = V(F\mathcal{A}) = p\mathcal{A}$, yields

$$\#\ker(L \to \mathcal{A}/p\mathcal{A}) = \frac{\#A_s[V]}{\#\,\mathrm{image}(\mathcal{A}[V] \to A_s[V])} = \frac{p^g}{\#\,\mathrm{image}(\mathcal{A}[V] \to A_s[V])}. \quad (6\text{–}2)$$

Reduction mod p is injective on torsion, so the composition

$$A[p](\mathbb{Q}_p^{\mathrm{unr}}) \xrightarrow{\pi} \mathcal{A}[p](\overline{\mathbb{F}}_p) = \mathcal{A}[V](\overline{\mathbb{F}}_p) \to A_s[V]$$

is injective, and hence $\#\operatorname{image}(\mathcal{A}[V] \to A_s[V]) \geq p^k$. Thus (6–2) gives $\#\ker(L \to \mathcal{A}/p\mathcal{A}) \leq p^{g-k}$.

Combining the results of the previous two paragraphs we see that $\#\ker(L \to \mathcal{A}/H) \leq p^k p^{g-k} = p^g$. Also, since $pL = 0$, the order of the kernel must be a power of p.

Finally, since $\#\ker(L \to \mathcal{A}/p\mathcal{A}) < \infty$ and since L and $\mathcal{A}/p\mathcal{A}$ both have dimension g, the map $L \to \mathcal{A}/p\mathcal{A}$ is an isogeny (surjective with finite kernel). Since $p\mathcal{A}$ is of finite index in H, $L \to \mathcal{A}/H$ is an isogeny too. Over a perfect field, any geometrically integral group variety isogenous to $\mathbb{G}_a^g$ is isomorphic to $\mathbb{G}_a^g$, so $\mathcal{A}/H \cong \mathbb{G}_a^g$. □

Corollary 6.2. *There exists a homomorphism of algebraic groups $\Phi : \mathcal{A} \to \mathbb{G}_a^g$ whose kernel contains $\pi(A(\mathbb{Q}_p^{\mathrm{unr}})_{\mathrm{tors}})$, and which has size exactly p^g.*

Proof. Compose the Φ given by Lemma 6.1 with an endomorphism of $\mathcal{A}/H \cong \mathbb{G}_a^g$ of suitable degree. □

Remark. We now indicate why the bound in Lemma 6.1 cannot be reduced further for general abelian varieties of dimension g. The deformation theory of p-divisible groups and abelian varieties lets one lift an ordinary g-dimensional abelian variety A_s to an abelian scheme A over $\mathbb{Z}_p$ such that the map $A_s[V] \to L$ in (6–1) coming from the extension (3–1) is injective. In this case,

$$\#\ker(L \to \mathcal{A}/p\mathcal{A} = \mathcal{A}/V\mathcal{A}) = \#A_s[V] = p^g$$

already, so the degree of $L \to \mathcal{A}/H$ is at least p^g, hence by Lemma 6.1 equal to p^g.

On the other hand, there are special instances in which the size can be chosen much smaller. For example, if A is the canonical lift of an ordinary abelian variety over $\mathbb{F}_p$, the exact sequence (3–1) splits and the splitting map $\mathcal{A} \to L \cong \mathbb{G}_a^g$ is a homomorphism of the desired type, and of size 1.

Remark. Buium [1996] uses the bound p^{2g} on the index of $p\mathcal{A}$ in H to prove that

$$\#(X \cap A_{\mathrm{tors}}) \leq p^{4g} 3^g \left[p(2g-2) + 6g\right] g!.$$

In the course of the proof of Lemma 6.2, we bounded the index by $p^k := \#A[p](\mathbb{Q}_p^{\mathrm{unr}}) \leq \#A_s[p](\overline{\mathbb{F}}_p) \leq p^g$, and hence the p^{4g} in Buium's bound can be improved to p^{3g}. In Section 12 we will obtain an even better bound in the case $g = 2$.

7. RELATING THE HOMOMORPHISM AND COLEMAN'S INTEGRALS

Let $\varepsilon : Z \to A$ denote the zero-section of A, so Z is a closed subscheme of A isomorphic to $\operatorname{Spec}\mathbb{Z}_p$. Let $\mathcal{I} \subseteq \mathcal{O}_A$ denote the ideal sheaf of Z. Since A is smooth over $\mathbb{Z}_p$, $\varepsilon^*\Omega^1_{A/\mathbb{Z}_p} \cong \mathcal{I}/\mathcal{I}^2 \cong \tilde{M}$, where $\tilde{M}$ is the free $\mathcal{O}_Z$-module associated to a free $\mathbb{Z}_p$-module M of rank g. Fix a system of local parameters; i.e., a g-tuple of sections $t_1, \ldots, t_g$ of $\mathcal{I}$ over an open neighborhood of Z whose images in $\mathcal{I}/\mathcal{I}^2$ form a $\mathbb{Z}_p$-basis for M.

Since A is an abelian scheme, the map

$$H^0(A, \Omega^1_{A/\mathbb{Z}_p}) \xrightarrow{\varepsilon^*} H^0(Z, \varepsilon^*\Omega^1_{A/\mathbb{Z}_p})$$

is an isomorphism. The $\mathbb{Z}_p$-basis $\varepsilon^*dt_1, \ldots, \varepsilon^*dt_g$ on the right corresponds to some $\mathbb{Z}_p$-basis $\tilde{\omega}_1, \ldots, \tilde{\omega}_g$ for $H^0(A, \Omega^1_{A/\mathbb{Z}_p})$.

The functions t_i are regular on a dense open subset of $A_s \subseteq A$, so the rational map $t_i : A \dashrightarrow \mathbb{A}^1_{\mathbb{Z}_p}$ gives rise to a rational map $\mathcal{A} \dashrightarrow \mathbb{A}^2_{\mathbb{F}_p}$; i.e., to a pair of rational functions which may be interpreted as the first two Witt coordinates of t_i. Let z_i denote the second Witt coordinate of t_i. Since the t_i are regular in a neighborhood of Z, the z_i are regular on L. In fact, $(z_1, \ldots, z_g) : L \to \mathbb{G}_a^g$ is an isomorphism of group varieties over $\mathbb{F}_p$, since the t_i induce functorial isomorphisms

$$\ker\left[A(W_2(R)) \to A_s(R)\right] \to \ker\left[W_2(R) \to R\right]^g$$

for $\mathbb{F}_p$-algebras R, related to the formal group obtained by expressing the group law of A analytically in the local parameters t_i.

A short argument using [Milne 1986, Proposition 5.3(b)] shows that the morphism $\iota : X \to A$ induces an isomorphism $\iota^* : H^0(A, \Omega^1_{A/\mathbb{Z}_p}) \to H^0(X, \Omega^1_{X/\mathbb{Z}_p})$. (By considering the generic and special fibers, one can reduce this statement to the analogous one for fields; then one may assume that the field is algebraically closed, and finally, one can relate the ι^* for a degree-δ divisor to δ times the ι^* for an Albanese embedding.) Define $\omega_i = \iota^*\tilde{\omega}_i$.

We will use Coleman's p-adic abelian integrals [1985]. Let $O \in A(\mathbb{Q}_p)$ be the identity. If $Q \in$

$A(\mathbb{Q}_p^{\mathrm{unr}})$ reduces to 0 in $A_s(\overline{\mathbb{F}}_p)$, then $\int_O^Q \tilde{\omega}_i \in p\mathbb{Z}_p^{\mathrm{unr}}$, as we can see by using an analytic primitive of $\tilde{\omega}_i$. More generally, if Q reduces to a point in $A_s(\overline{\mathbb{F}}_p)$ of order n prime to p, then the same is true, since $\int_O^Q \tilde{\omega} = n^{-1}\int_O^{nQ} \tilde{\omega}$. For such Q we may define

$$\eta_i(Q) = \left(p^{-1}\int_O^Q \tilde{\omega}_i\right)^p \bmod p \quad \in \overline{\mathbb{F}}_p.$$

Lemma 7.1. *Let $Q \in A(\mathbb{Q}_p^{\mathrm{unr}})$ be a point reducing to 0 in $A_s(\overline{\mathbb{F}}_p)$, so that $\pi(Q) \in L(\overline{\mathbb{F}}_p)$. Then $\eta_i(Q) = z_i(\pi(Q))$.*

Proof. The expansion of $\tilde{\omega}_i$ in a neighborhood of Z in terms of the local parameters t_i is given by

$$\tilde{\omega}_i = dt_i + \sum_{j=1}^{g} h_j dt_j$$

where $h_j \in \mathbb{Z}_p[[t_1, \ldots, t_g]]$ has zero constant coefficient. Integrating $\tilde{\omega}_i$ formally, and noting that $p > 2$ and $t_j(Q) \equiv 0 \pmod{p}$ for each j, we find that

$$\int_O^Q \tilde{\omega}_i \equiv t_i(Q) \pmod{p^2}.$$

On the other hand, the first two Witt coordinates of $t_i(Q)$ are 0 and $z_i(\pi(Q))$, by definition of z_i, so

$$t_i(Q) \equiv p(z_i(\pi(Q)))^{1/p} \pmod{p^2}.$$

Combining these yields the result. □

As a corollary, we can use Coleman's integrals to compute values of homomorphisms $\mathcal{A} \to \mathbb{G}_a$ at many points of $\mathcal{A}$, namely those whose image in $A_s(\overline{\mathbb{F}}_p)$ are of order prime to p:

Corollary 7.2. *Let $\varphi : \mathcal{A} \to \mathbb{G}_a$ be a homomorphism, and let $\psi(z_1, z_2, \ldots, z_g)$ be the polynomial giving the restriction of φ to L. Suppose that $Q \in A(\mathbb{Q}_p^{\mathrm{unr}})$ reduces to a point in $A_s(\overline{\mathbb{F}}_p)$ of order prime to p. Then*

$$\varphi(\pi(Q)) = \psi(\eta_1(Q), \ldots, \eta_g(Q)).$$

Proof. Without loss of generality, replace Q by a prime-to-p multiple to assume that Q reduces to 0 in $A_s(\overline{\mathbb{F}}_p)$. Now apply Lemma 7.1. □

8. COMPUTING THE HOMOMORPHISM ON A HYPERELLIPTIC CURVE

We retain earlier notation, but from now on assume in addition that X is birational to the affine curve $y^2 = f(x, 1)$ where $f(x, z) \in \mathbb{Z}_p[x, z]$ is a homogeneous polynomial of degree $2g + 2$ whose mod p reduction $\bar{f}$ has no repeated factors. Then X is hyperelliptic, and we define ι and the hyperelliptic torsion packet $T = \iota^{-1}(A_{\mathrm{tors}})$ as in the remark at the end of Section 5. By changing the original $\mathbb{Z}_p$-basis for M if necessary, we may assume that $\omega_i = x^{i-1}\,dx/y$. Let x_0, x_1 denote the rational functions on $\mathcal{X}$ giving the first two Witt coordinates of the x-coordinate on X. Similarly define y_0, y_1.

Lemma 8.1. *Let φ and ψ be as in Corollary 7.2. Then as rational functions on $\mathcal{X}$,*

$$\varphi \circ \iota = \frac{G(x_0)}{y_0^{p \deg \psi}} + \psi\left(\frac{x_1}{y_0^p}, \frac{x_0^p x_1}{y_0^p}, \ldots, \frac{x_0^{(g-1)p} x_1}{y_0^p}\right) \quad (8\text{–}1)$$

for some polynomial $G \in \mathbb{F}_p[x_0]$ of degree at most $(g+1)\,p \deg \psi$.

By $\deg \psi$, we mean the total degree. Since $\psi : \mathbb{G}_a^g \to \mathbb{G}_a$ is a homomorphism, $\deg \psi = p^r$ for some $r \in \mathbb{Z}_{\geq 0}$.

Proof. We first show that the rational function

$$\xi := (\varphi \circ \iota) - \psi\left(\frac{x_1}{y_0^p}, \frac{x_0^p x_1}{y_0^p}, \ldots, \frac{x_0^{(g-1)p} x_1}{y_0^p}\right)$$

on $\mathcal{X}$ is constant on infinitely many fibers of the $\mathbb{F}_p$-morphism $\mathcal{X} \to X_s$. Let P, P' be points in $X(\mathbb{Q}_p^{\mathrm{unr}})$ reducing to the same point in $X_s(\overline{\mathbb{F}}_p)$, and assume that the latter point is affine and that it has nonzero y-coordinate. Define $Q := \iota(P') - \iota(P) \in A(\mathbb{Q}_p^{\mathrm{unr}})$. Then

$$\begin{aligned}(\varphi \circ \iota)(\pi(P')) - (\varphi \circ \iota)(\pi(P)) \\ = \varphi(\pi(Q)) = \psi(\eta_1(Q), \ldots, \eta_g(Q)),\end{aligned} \quad (8\text{–}2)$$

by Corollary 7.2, and

$$\begin{aligned}\eta_i(Q) &= \left(p^{-1}\int_O^Q \tilde{\omega}_i\right)^p \bmod p \\ &= \left(p^{-1}\int_{\iota(P)}^{\iota(P')} \tilde{\omega}_i\right)^p \bmod p \\ &= \left(p^{-1}\int_P^{P'} \omega_i\right)^p \bmod p \\ &= \left(p^{-1}\int_P^{P'} \frac{x^{i-1}\,dx}{y}\right)^p \bmod p.\end{aligned} \quad (8\text{–}3)$$

By the choice of P and P', we may expand ω_i and its integral in terms of the uniformizing parameter $x - x(P)$ at P:

$$\omega_i = \frac{x^{i-1}\,dx}{y} = \left(\frac{x(P)^{i-1}}{y(P)} + \sum_{j=1}^{\infty} c_j (x - x(P))^j\right) dx,$$

for some $c_j \in \mathbb{Z}_p$, and

$$\begin{aligned}\int_P^{P'} \omega_i &= \frac{x(P)^{i-1}}{y(P)}(x(P') - x(P)) \\ &\qquad + \sum_{j=1}^{\infty} c_j \frac{(x(P') - x(P))^{j+1}}{j+1} \\ &\equiv \frac{x(P)^{i-1}}{y(P)}(x(P') - x(P)) \pmod{p^2} \\ &\qquad \text{(since } p > 2\text{)} \\ &\equiv p\frac{\bar{x}_0^{i-1}}{\bar{y}_0}\left((\bar{x}_1')^{1/p} - \bar{x}_1^{1/p}\right) \pmod{p^2},\end{aligned}$$

where $\bar{x}_0, \bar{x}_1, \bar{y}_0$ denote the values of the functions x_0, x_1, y_0 at $\pi(P)$ (i.e., the Witt coordinates of the coordinates of P), and $\bar{x}_1'$ is the value of x_1 at $\pi(P')$. (To make sense of the previous equation, these quantities should be considered as elements of $\mathbb{Z}_p^{\mathrm{unr}}$, but it is only their residues modulo p that matter.) Substituting into (8–3) yields

$$\eta_i(Q) = \frac{\bar{x}_0^{(i-1)p}\bar{x}_1}{\bar{y}_0^p} - \frac{\bar{x}_0^{(i-1)p}\bar{x}_1'}{\bar{y}_0^p} \bmod p.$$

Substituting this into (8–2) and using the fact that ψ is a homomorphism shows that ξ is constant on each closed fiber of $\mathcal{X} \to X_s$ above an affine point with nonzero y-coordinate. Thus ξ can be expressed as a rational function in x_0 and y_0 only.

Since $\varphi \circ \iota$ is regular on all of $\mathcal{X}$, the definition of ξ shows that $y_0^{p \deg \psi}\xi$ is regular on any open set where y_0 is regular. Hence $y_0^{p \deg \psi}\xi$ can be expressed as a polynomial in x_0 and y_0. The hyperelliptic involution on X is compatible with multiplication by -1 on A. Hence the induced involution on $\mathcal{X}$ transforms both $y_0^{p \deg \psi}$ and ξ to their negatives. Thus $y_0^{p \deg \psi}\xi = G(x_0)$ for some polynomial G.

We can bound $\deg G$ by studying the behavior of (8–1) at a point $R \in \mathcal{X}(\overline{\mathbb{F}}_p)$ reducing to a point $\bar{R}$ at infinity on X_s. The function x_0^{g+1}/y_0 is nonvanishing at $\bar{R}$ if it is regular at all, since its square equals $x_0^{2g+2}/\bar{f}(x_0, 1)$ and $\deg \bar{f}(x_0, 1) \le \deg \bar{f} = 2g + 2$. Hence if $\deg G > (g+1)\,p \deg \psi$, then $G(x_0)/y_0^{p \deg \psi}$ has a pole of some order at $\bar{R}$ on X_s.

Let X_0, X_1 be the first two Witt coordinates of the rational function $1/x$. A Witt vector calculation yields $x_1 = -x_0^{2p}X_1$. Hence

$$\xi = (\varphi \circ \iota) + \psi\left(\frac{x_0^{2p}}{y_0^p}X_1, \frac{x_0^{3p}}{y_0^p}X_1, \ldots, \frac{x_0^{(g+1)p}}{y_0^p}X_1\right).$$

But X_1 and $\varphi \circ \iota$ are regular at R, so the order of the pole (if there is any at all) of ξ at the point $\bar{R}$ on X_s is at most the order of the pole of $x_0^{(g+1)\,p \deg \psi}/y_0^{p \deg \psi}$, which is strictly smaller than the order of the pole of $G(x_0)/y_0^{p \deg \psi}$. This contradicts $\xi = G(x_0)/y_0^{p \deg \psi}$. □

The degree bound in Lemma 8.1 makes it possible to compute G given φ using interpolation. Suppose, for example, that φ is the composition of $P(F_{\mathcal{A}}) : \mathcal{A} \to L$ and $z_1 : L \to \mathbb{G}_a$. Then $\psi(z_1, \ldots, z_g) = P(F)(z_1)$, where $P(F)$ should now be considered as an additive polynomial of degree p^{2g}. For many values $x_0 \in \overline{\mathbb{F}}_p$ (say, all of a given degree over $\mathbb{F}_p$ that are not roots of $f(x, 1)$), check whether x_0 is the x-coordinate of some $\bar{R} \in X_s(\overline{\mathbb{F}}_p)$ such that $\iota(\bar{R})$ is of order prime to p in $A_s(\overline{\mathbb{F}}_p)$. (In Section 11 we'll show how to check this.) If moreover $\bar{R}$ has nonzero y-coordinate, Hensel's Lemma lets us lift $\bar{R}$ to a point $R \in X(\mathbb{Q}_p^{\mathrm{unr}})$ whose x-coordinate mod p^2 equals the Teichmüller lift of x_0. Setting $Q = \iota(R)$, we may then calculate $\eta_i(Q)$ for each i (see Section 11 for details), and hence compute $\varphi(\pi(Q))$ from Corollary 7.2. On the other hand, (8–1) gives another expression for $\varphi(\pi(Q)) = (\varphi \circ \iota)(\pi(R))$, in which everything is known except the value of G. If we compute $G(x_0)$ for enough values of x_0 (more than the degree bound for G in Lemma 8.1), the polynomial G can be computed by Lagrange interpolation.

Now suppose that we wish to use the improved homomorphism Φ of Corollary 6.2 instead of $P(F_{\mathcal{A}})$. In this case, we need to get around the fact that we do not have a priori formulas for the restriction $\psi : L \to \mathbb{G}_a$ to L of the composition of Φ with a projection $\mathbb{G}_a^g \to \mathbb{G}_a$. Let I be the unknown ideal in $\mathbb{F}_p[z_1, \ldots, z_g]$ defining the subscheme $L \cap \ker \Phi$ in L. Then $\#\mathbb{F}_p[z_1, \ldots, z_g]/I = \#(L \cap \ker \Phi) = p^g$. Let W be the $2g$-dimensional $\mathbb{F}_p$-span of the z_i and z_i^p in $\mathbb{F}_p[z_1, \ldots, z_g]$. Then $\#(W \cap I) \ge p^g$. If ψ is in

$W \cap I$, then ψ kills $L \cap \ker \Phi$, so ψ factors through the restriction of Φ to L, which is a homomorphism $L \to \mathbb{G}_a^g$. Composing Φ with "the other factor", the homomorphism $\mathbb{G}_a^g \to \mathbb{G}_a$, yields a homomorphism $\mathcal{A} \to \mathbb{G}_a$ whose restriction to L is φ.

If we try to determine G for each $\psi \in W$, by interpolating several more values than the degree bound, then we will find for some ψ that the degree of G would have to *exceed* the degree bound; this means that ψ cannot possibly be the restriction of a homomorphism $\mathcal{A} \to \mathbb{G}_a$. Let W' denote the set of ψ for which the degree of the interpolated G is less than or equal to the bound; thus W' is a subspace of W containing $W \cap I$. If we find that $\dim W' \leq g$, then $W' = W \cap I$ and $\dim W' = g$, since $W \cap I$ has dimension at least g. If moreover the subgroup scheme $L[W']$ cut out by the polynomials in W' is *finite*, then its order will be at most p^g, but on the other hand it must contain $L \cap \ker \Phi$, so $L[W'] = L \cap \ker \Phi$ and the basis for W' describes $\Phi : \mathcal{A} \to \mathbb{G}_a^g$ up to an (irrelevant) automorphism of $\mathbb{G}_a^g$.

If we are not so lucky, then we can simply try a different p. Naive heuristics suggest that the method above succeeds (i.e., $\dim W' = g$ and $L[W']$ is finite) for at least a positive density of primes p, but it seems difficult to prove anything along these lines, since it is closely related to questions such as deciding, given an abelian variety A over $\mathbb{Q}$, the finiteness or co-finiteness of the set of primes p for which A mod p^2 is a canonical lift of A mod p.

(Alternatively, we could guarantee success by using $\Phi = P(F)$ instead of our improved Φ, but in practice this is usually more expensive, since the degree of G in Lemma 8.1 tends to be much larger.)

A computational improvement: instead of performing the interpolation for each of the p^{2g} elements of W, we can interpolate the η_i at points with x-coordinates that are Teichmüller lifts modulo p^2, to obtain elements of some quotient $\mathbb{F}_p[x_0]/h$ whose values at any root of $h \in \mathbb{F}_p[x_0]$ represent the value of η_i at the corresponding Teichmüller lift point, and evaluate the combinations needed in Corollary 7.2, *as elements of* $\mathbb{F}_p[x_0]/h$. Here we should interpolate enough to obtain h of degree larger than the degree bound in Lemma 8.1, and enough larger that it becomes likely that the interpolation yields a G of degree below the degree bound only when φ actually comes from a homomorphism $\mathcal{A} \to \mathbb{G}_a$.

9. ELIMINATION OF VARIABLES

Assume that we succeeded in Section 8 in computing the restriction of Φ to $\mathcal{X}$, so that we now know g regular functions on $\mathcal{X}$ (right-hand sides of (8–1)) whose common zero set is a finite subscheme containing $\pi(X \cap A_{\text{tors}})$. Multiplying each of these by a large odd power of y_0 and replacing y_0^2 by $\bar{f}(x_0)$, we obtain g polynomial equations in x_0 and x_1. It is easy to eliminate x_1 from these using p-resultants [Goss 1996, Section 1.5], since the exponents of x_1 that appear are all powers of p. We end up with a single nonzero polynomial $r(x_0) \in \mathbb{F}_p[x_0]$ whose roots (together possibly with ∞) give the x-coordinates modulo p of the residue classes on X that could possibly contain elements of T. We factor $r(x_0)$ over $\mathbb{F}_p$.

Remark. If $g > 2$, then the number of equations in x_0 and x_1 above exceeds the number of variables, so we expect heuristically that $r(x_0)$ will have very small degree.

10. LIFTING TO CHARACTERISTIC ZERO AND VERIFICATION

Now we have a list of irreducible polynomials over $\mathbb{F}_p$ whose roots in $\overline{\mathbb{F}}_p$, together with $\infty \in \mathbb{P}^1(\overline{\mathbb{F}}_p)$, contain the reductions of the x-coordinates of points of T. Let S denote the corresponding set of residue classes in $X_s(\overline{\mathbb{F}}_p)$. To finish, we need an algorithm that, given a point $\bar{R} \in S$, determines whether there exists a point $R \in X(\mathbb{Q}_p^{\text{unr}})$ in its residue class with $\iota(R)$ torsion, and if so, finds it.

The computations done so far, which have narrowed our search to a finite set of candidates for $\bar{R}$, have used only the equation of X mod p^2. For this, it did not matter whether X was defined over a number field or not. But from now on, we assume that the coefficients of the polynomial $f(x, 1)$ defining X lie in a number field $k \subseteq \mathbb{Q}_p$. Such an assumption lets us make sense of the problem of finding the points of T exactly: the answer can be the list of minimal polynomials over k satisfied by their x-coordinates.

The plan is to attempt to lift $\iota(\bar{R})$ to a torsion point $R \in A(\mathbb{Q}_p^{\text{unr}})_{\text{tors}}$ to high p-adic precision. By Lemma 4.2 there is at most one such R. Moreover, R is guaranteed to exist if $\iota(\bar{R})$ is of order prime to p. If we succeed in producing R, we check whether

it lies on $\iota(X)$ up to the computed p-adic precision. Details of computing R and determining whether it lies on $\iota(X)$ up to a certain p-adic precision will be given in Section 11.

After doing this for each non-Weierstrass point $\bar{R} \in S$, we have a list of x-coordinates in $\mathbb{P}^1(\mathbb{Q}_p^{\mathrm{unr}})$ which appear to be, to high p-adic precision, the complete list of x-coordinates of the non-Weierstrass points in T. In practice, if we go to high precision, we can be morally certain that these are approximations of the desired x-coordinates. We then construct the homogeneous polynomial $g \in \mathbb{Z}_p[x,z]$ vanishing at these points of $\mathbb{P}^1(\mathbb{Q}_p^{\mathrm{unr}})$ to high precision, scaling it so that some coordinate is 1, and try to recognize these approximate coefficients of g as elements of k of small height. This can be done using p-adic continued fractions if $k = \mathbb{Q}$; more generally, as we learned from Hendrik Lenstra, to recognize a number in $\mathbb{Z}_p$ (represented as an integer α modulo p^n for large n) as an algebraic number of degree d of small height, apply lattice basis reduction to find a short nonzero vector in the sublattice of vectors with last coordinate zero of the lattice in $\mathbb{Z}^{d+2}$ spanned by the rows of

$$\begin{bmatrix} 1 & 0 & 0 & 0 & \dots & 0 & 1 \\ 0 & 1 & 0 & 0 & \dots & 0 & \alpha \\ 0 & 0 & 1 & 0 & \dots & 0 & \alpha^2 \\ & & & & \vdots & & \\ 0 & 0 & 0 & 0 & \dots & 1 & \alpha^d \\ 0 & 0 & 0 & 0 & \dots & 0 & p^n \end{bmatrix}.$$

Finally, now that we have a homogeneous polynomial $g \in k[x,z]$ whose roots $r \in \mathbb{P}^1(\bar{k})$ we think are the x-coordinates of torsion points, for each root r let P_r be a point on X with x-coordinate r, and (using the methods of the next section) compute algebraically $n\iota(P_r)$ for $n = 1, 2, \dots$, expecting to find $0 \in A$ eventually. If so for each r, we are done; otherwise we either compute more multiples or redo the entire computation to higher p-adic precision. (In practice, we have never needed to do the latter.) At the end we have a provably correct list of the x-coordinates of the points of T.

11. THE KUMMER SURFACE

The most difficult computational ingredient in the algorithm described is an algorithm for group law computations on A and $\mathcal{A}$. Although in theory the torsion packet calculating algorithm works for any $g > 2$, we restricted our implementation to the $g = 2$ case to avoid working too hard, the work having already been done by Cassels and Flynn in this case. (See [Flynn 1993; Cassels and Flynn 1996].) Moreover our implementation assumes that the genus 2 curve is defined over $\mathbb{Q}$.

Suppose that A is the Jacobian of a curve X of genus $g = 2$ over a field k of characteristic not 2. The associated *Kummer surface* K is the quotient $A/\langle \pm 1 \rangle$ where -1 acts on A as multiplication by -1. The multiplication by -1 on A has 16 geometric fixed points (the points of order 2); some authors blow these up on A before taking the quotient in order that the quotient be smooth, but we will not. We remark that if $P \in X(k)$ is not a Weierstrass point, then the image of $\iota(P)$ in K is a nonsingular point, since otherwise $2P$ would be linearly equivalent to a sum of two Weierstrass points, and the difference of these divisors would be the divisor of a degree 2 function on X not preserved by the hyperelliptic involution, an impossibility.

A point in $K(k)$ corresponds to a $\mathrm{Gal}(\bar{k}/k)$-stable pair $\{P, Q\}$ of points in $A(\bar{k})$ satisfying $P = -Q$. For $n \in \mathbb{Z}$, multiplication by n on A induces a morphism $m_n : K \to K$ taking $\{P, -P\}$ to $\{nP, -nP\}$. The addition $A \times A \to A$ does not induce a morphism $K \times K \to K$. But instead there is a "addition-and-subtraction" morphism $\varphi : K \times K \to \mathrm{Sym}^2(K)$ taking $(\{P, -P\}, \{Q, -Q\})$ to

$$\{\{P+Q,\ -(P+Q)\},\ \{P-Q,\ -(P-Q)\}\}.$$

Cassels and Flynn observed that equations for the basic computations on K can be written down in a reasonable amount of space. These equations include: an explicit projective embedding for K, equations for the morphism $\iota' : \mathbb{P}^1 \to K$ induced by $\iota : X \to A$ ($\mathbb{P}^1$ being the x-line), equations defining φ and recursive formulas defining m_n for $n \geq 1$. These equations are *much* simpler than the analogous equations for A. Hence we will try to use computations with K in place of A wherever possible.

The variety K can be presented as a surface in $\mathbb{P}^3$ with homogeneous coordinates k_1, k_2, k_3, k_4. If $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$, the map $X \times X \to K$ taking (P_1, P_2) to the image of the divisor $P_1 + P_2 - \kappa$,

κ being the canonical divisor, is given by $[1, x_1+x_2, x_1x_2, h]$, where the final projective coordinate h is a rational function in all the variables x_1, y_1, x_2, y_2.

We recall what is needed.

1. *Evaluating p-adic integrals* (Section 8): Given $x_0 \in \overline{\mathbb{F}}_p$ with $f(x_0, 1) \neq 0$, check if a point $\bar{R} \in X_s(\overline{\mathbb{F}}_p)$ is such that $\iota(\bar{R})$ has order prime to p in $A_s(\overline{\mathbb{F}}_p)$, and if so, lift $\bar{R}$ to $R \in X(W_2(\overline{\mathbb{F}}_p))$ and compute $\eta_i(\iota(R)) \in \overline{\mathbb{F}}_p$ for $i = 1, 2, \ldots, g$.
2. *Lifting to torsion points* (Section 10): Given $\bar{R} \in X_s(\overline{\mathbb{F}}_p)$ and a moderately large integer r (e.g. 30), either lift $\iota(\bar{R})$ to a point $R \in A(W_r(\overline{\mathbb{F}}_p))$ of the same order (a potential approximation to a torsion point), or prove that no such R exists.
3. *Deciding whether a point on the Jacobian lies on the image of the curve* (Section 10): Given a point in $A(W_r(\overline{\mathbb{F}}_p))$ determine whether it lies on the image $\iota(X(W_r(\overline{\mathbb{F}}_p)))$ of the curve (to p-adic precision p^r).
4. *Verifying torsion points* (Section 10): If k is a number field, $R \in X(k)$, and $n \geq 1$, determine whether $n\iota(R) = 0$ in $A(k)$.

Before describing the algorithms for these particular routines, we remark that elements of $W_r(\mathbb{F}_{p^d})$ are represented by polynomials of degree less than d in $(\mathbb{Z}/p^r)[x]$ modulo a fixed monic polynomial in $(\mathbb{Z}/p^r)[x]$ of degree d whose mod p reduction is irreducible. The characteristic polynomial $P(x)$ (of Section 4) is computed from $X(\mathbb{F}_p)$ and $X(\mathbb{F}_{p^2})$, which are computed naively by checking all possible x-coordinates. Then $\#A(\mathbb{F}_{p^d})$ is the norm from $\mathbb{Z}[x]/(P(x))$ to $\mathbb{Z}$ of the image of $x^d - 1$. Similarly the order of the subgroup $A(\mathbb{F}_{q^{2d}})^-$ of $A(\mathbb{F}_{q^{2d}})$ on which F^d acts as -1 is the norm of the image of $x^d + 1$.

Evaluating p-adic Integrals

Let d be the degree of x_0 over $\mathbb{F}_p$. First compute $f(x_0)$ and raise it to the $(p^d - 1)/2$ power to determine whether the y-coordinate y_0 of a point $\bar{R} \in X_s(\overline{\mathbb{F}}_p)$ with x-coordinate x_0 lies in $\mathbb{F}_{p^d}$ or in its quadratic extension. Let $N = \#A(\mathbb{F}_{p^d})$ in the first case, and let $N = \#A(\mathbb{F}_{p^{2d}})^-$ in the second case, so that the order of $\iota(\bar{R})$ divides N. Let N' be the largest prime-to-p divisor of N. Let $N'' = 2N'$ if $N' \equiv 2 \pmod{p}$, and let $N'' = N'$ otherwise. Calculate $m_{N''+1}(\iota'(x_0))$, the image of $(N''+1)\,\iota(\bar{R}) \in A_s(\overline{\mathbb{F}}_p)$ in K. If the order of $\bar{R}$ in $A_s(\overline{\mathbb{F}}_p)$ is prime to p, then $N\bar{R} = 0$, implying that $(N''+1)\bar{R} = \bar{R}$ and $m_{N''+1}(\iota'(x_0)) = \iota'(x_0)$. Conversely, if

$$m_{N''+1}(\iota'(x_0)) = \iota'(x_0),$$

then $(N''+1)\bar{R} = \pm\bar{R}$, but N'' and $N''+2$ are both prime to p, so $\bar{R}$ is of order prime to p.

We now assume we are in the case where $\bar{R}$ is of order prime to p. The Teichmüller lift $x_0' \in W_2(\mathbb{F}_{p^d})$ of x_0 is computed by choosing an arbitrary lift and raising it to the p^d power. By Hensel's Lemma, there is a point $R \in X(\mathbb{Q}_p^{\mathrm{unr}})$ with x-coordinate reducing to x_0' mod p^2. To compute $\eta_i(\iota(R))$, we need to evaluate

$$\int_0^{\iota(R)} \tilde{\omega}_i = \frac{1}{N''} \int_{\iota(R)}^{(N''+1)\iota(R)} \tilde{\omega}_i.$$

Since we know $(N''+1)\iota(R)$ only through its image in K, we must relate the latter integral to one on K.

Consider the sequence of morphisms

$$X \xrightarrow{\Delta} X \times X \xrightarrow{\beta} A \xrightarrow{\gamma} K$$

where Δ is the diagonal, β maps (P, Q) to the class of $P + Q - \kappa$, and γ is the canonical quotient map. Since $\beta^*\tilde{\omega}_1$ is a 1-form on $X \times X$ symmetric under interchange of coordinates, such that α^* pulls it back to dx/y, we must have

$$\beta^*\tilde{\omega}_1 = \frac{1}{2}\left(\frac{dx_1}{y_1} + \frac{dx_2}{y_2}\right).$$

Similarly

$$\beta^*\tilde{\omega}_2 = \frac{1}{2}\left(\frac{x_1\,dx_1}{y_1} + \frac{x_2\,dx_2}{y_2}\right).$$

In particular, β^* is injective on meromorphic 1-forms. On the other hand the 1-forms $\mu_1 := d(k_2/k_1)$ and $\mu_2 := d(k_3/k_1)$ pull back to $d(x_1 + x_2) = dx_1 + dx_2$ and $d(x_1x_2) = x_2dx_1 + x_1dx_2$ on $X \times X$, respectively. Abusing notation by identifying each 1-form with its pullback to $X \times X$, and solving for $\tilde{\omega}_1$ and $\tilde{\omega}_2$ in terms of μ_1 and μ_2, we obtain

$$\tilde{\omega}_1 = \frac{1}{2y_1y_2}\left(y_1 - x_1\frac{y_2 - y_1}{x_2 - x_1}\right)\mu_1 + \frac{1}{2y_1y_2}\frac{y_2 - y_1}{x_2 - x_1}\mu_2, \quad (11\text{–}1)$$

and

$$\tilde{\omega}_2 = \frac{1}{2y_1y_2}\left((x_1+x_2)y_1 - x_1^2\frac{y_2-y_1}{x_2-x_1}\right)\mu_1 + \frac{1}{2y_1y_2}\left(-y_1 + x_1\frac{y_2-y_1}{x_2-x_1}\right)\mu_2. \quad (11\text{–}2)$$

To evaluate the integral μ_1 and μ_2 on K from the image of $\iota(R)$ to the image of $(N''+1)\iota(R)$, as elements of $p\mathbb{Z}_p^{\mathrm{unr}}$ modulo p^2, is trivial, because we know the projective coordinates k_1, k_2, k_3, k_4 of those two images, using the explicit map $\mathbb{P}^1 \to K$ and the recursively computed map $m_{N''+1} : K \to K$. Hence in order to compute $\int_{\iota(R)}^{(N''+1)\iota(R)} \tilde{\omega}_i$, it suffices to know the values mod p at $(\bar{R}, \bar{R})$ of the four functions appearing as coefficients of μ_1 and μ_2 in the change of variable formulas (11–1) and (11–2). These functions can be evaluated directly, once we observe that

$$\frac{y_2-y_1}{x_2-x_1} = \frac{y_2^2-y_1^2}{(x_2-x_1)(y_1+y_2)} = \frac{f(x_2)-f(x_1)}{(x_2-x_1)(y_1+y_2)}$$

evaluates to $f'(x)/(2y)$ at an affine point satisfying $(x_1, y_1) = (x_2, y_2) = (x, y)$ and $y \neq 0$ modulo p.

Lifting to Torsion Points

Define N as in the previous subsection, and suppose that p^m is the highest power of p dividing N. The 1-form calculations of the previous section show that k_2/k_1 and k_3/k_1 with constants subtracted serve as local parameters at the image of $\iota(\bar{R})$ on K, and they induce a bijection between the set of points of its residue disk in $K(W(\overline{\mathbb{F}}_p))$ and $(pW(\overline{\mathbb{F}}_p))^{\oplus 2}$. We will find the image of a torsion point in this disk, if it exists, by a Newton-like method. Choose R_1 in this residue disk, corresponding to (a_1, b_1). (Of course, the coordinates of R_1 are given only to some finite p-adic precision.) By definition of N, $m_{N+1}(R_1)$ maps to the same residue class; suppose it corresponds to (a_{N+1}, b_{N+1}). Let $R_0 \in K(W(\overline{\mathbb{F}}_p))$ denote the point corresponding to

$$\left(a_1 - \frac{a_{N+1}-a_1}{N}, b_1 - \frac{b_{N+1}-b_1}{N}\right),$$

provided that these coordinates belong to $pW(\overline{\mathbb{F}}_p)$. We claim that iterating this construction $R_1 \mapsto R_0$ either terminates in failure if at some point the coordinates are no longer in $pW(\overline{\mathbb{F}}_p)$, in which case the conclusion is that there is no torsion point of $A(W(\overline{\mathbb{F}}_p))$ in the desired residue class, or else the sequence of iterates converges to the image of the desired torsion point. This follows from applying the following lemma with $m = m_{N+1}$ and h the conversion to the formal coordinates obtained by integrating regular 1-forms.

Lemma 11.1. *Let $V_1 = V_2 = (pW(\overline{\mathbb{F}}_p))^{\oplus 2}$. Let $h : V_1 \to V_2$ be an analytic isomorphism. Under h, an endomorphism $m : V_1 \to V_1$ corresponds to an affine linear function $v \mapsto (N+1)v - \varepsilon$ on V_2. If $\varepsilon/N \in V_2$, then m has a unique fixed point v_0 and for any starting point $v \in V_1$, iteration of $\varphi(v) := v - (m(v)-v)/N$ converges to v_0. If $\varepsilon/N \notin V_2$, then for any $v \in V_1$, $(m(v)-v)/N \notin V_1$.*

Proof. Let $|\cdot|$ denote the p-adic absolute value on $W(\overline{\mathbb{F}}_p)$, and also the sup norm on

$$V_1 = V_2 = (pW(\overline{\mathbb{F}}_p))^{\oplus 2}.$$

For $u, u' \in (pW(\overline{\mathbb{F}}_p))^{\oplus 2}$, we write $u \sim u'$ if $|u-u'| < |u|$.

The fixed points of m correspond under h to the fixed points of $v \mapsto (N+1)v - \varepsilon$; there is at most one, and one exists if and only $\varepsilon/N \in V_2$. We have

$$\begin{aligned} |m(v)-v| &= |h(m(v)) - h(v)| \\ &= |(N+1)h(v) - \varepsilon - h(v)| \\ &= |N(h(v) - \varepsilon/N)|. \end{aligned}$$

Therefore φ is well-defined at v if and only if ε/N is in V_2.

It remains to show that if $\varepsilon/N \in V_2$, then iteration of φ converges to the fixed point v_0 of m. Because the valuation on $W(\overline{\mathbb{F}}_p)$ is discrete, it suffices to prove $|\varphi(v)-v_0| < |v-v_0|$ for $v \neq v_0$. Composing the isomorphism h by translations on both sides, we may assume $v_0 = \varepsilon = 0$. The derivative of h modulo p is a constant nonsingular matrix in $GL_2(\overline{\mathbb{F}}_p)$; by a linear change of variable, we may assume that it is the identity matrix mod p. The Taylor expansion of h around u shows that $h(u') - h(u) \sim u' - u$ for all $u, u' \in V_1$.

Given $v \neq 0$, let $w = h(v)$, so

$$h(m(v)) = (N+1)\,w.$$

Then $m(v) - v \sim h(m(v)) - h(v) = Nw$, so that $(m(v)-v)/N \sim w \sim v$. Thus $|\varphi(v)| < |v|$ as desired. □

Deciding Whether a Point on the Jacobian Lies on the Image of the Curve

This is simple to do with the Kummer surface: the image of the curve in K is the subvariety cut out by the equation $k_2^2 - k_1 k_3 = 0$. In practice, one can check this relation as one goes along in the successive approximation of the previous subsection, to higher and higher precision, in hope of terminating the successive approximation early, as soon as one discovers that the torsion point (if it exists at all) is not on the curve.

Verifying Torsion Points

Apply ι' to the x-coordinate of R to obtain the image of R in K, apply m_n, and see if the result is $[0,0,0,1]$, which is the image of $0 \in A$ in K.

12. THEORETICAL BOUNDS FOR GENUS-TWO CURVES

Now that we have finished describing the implementation, we will use the method to prove a bound for $\#T$ when $g = 2$. In the next section, we will show how this bound enables one to combine p-adic information for different primes p to speed up the computation.

Lemma 12.1. *Let K be a subgroup scheme of $\mathbb{G}_a^2 = \operatorname{Spec} \mathbb{F}_p[z_1, z_2]$ of order p^2. Then there exist elements a, b, c, d of $\mathbb{F}_p$ such that K is defined by one of three systems of equations*:

I. $z_1^p + az_1 + bz_2 = z_2^p + cz_1 + dz_2 = 0$,
II. $z_1^{p^2} + az_1^p + bz_1 = z_2 + cz_1 = 0$, *or*
III. $z_2^{p^2} + az_2^p + bz_2 = z_1 + cz_2 = 0$.

Proof. For $i = 1, 2$, denote by K_i the scheme-theoretic image of K under the i-th projection $\mathbb{G}_a^2 \to \mathbb{G}_a$. Clearly K_i is a subgroup scheme of $\mathbb{G}_a$ of order at most p^2.

Case 1: $\#K_1 \le p$ and $\#K_2 \le p$. Since $K \subseteq K_1 \times K_2$, we have $(\#K_1)(\#K_2) \ge p^2$, so the only possibility is $\#K_1 = \#K_2 = p$ and $K = K_1 \times K_2$. Every subgroup scheme of $\mathbb{G}_a$ of order p^k is cut out by an additive polynomial, so K is cut out by

$$z_1^p + az_1 = z_2^p + dz_2 = 0$$

for some $a, d \in \mathbb{F}_p$, which is of type I.

Case 2: $\#K_1 > p$. Then $\#K_1 = p^2$, K_1 is cut out by an equation

$$z_1^{p^2} + az_1^p + bz_1 = 0, \tag{12–1}$$

and K is the graph of a homomorphism $K_1 \to \mathbb{G}_a$. The homomorphism K_1 is the restriction of a homomorphism $\mathbb{G}_a \to \mathbb{G}_a$, which is an additive polynomial, but since we may reduce this polynomial modulo (12–1), we may take it to be of the form $cz_1^p + dz_1$, with $c, d \in \mathbb{F}_p$, and K is defined by (12–1) together with

$$z_2 = cz_1^p + dz_1. \tag{12–2}$$

If $c = 0$, we are in type II.

Otherwise (12–2) expresses z_1^p as a combination of z_1 and z_2 while if we replace $z_1^{p^2}$ in (12–1) by $\left(c^{-1}(z_2 - dz_1)\right)^p$ and use (12–2) again to eliminate the z_1^p, we express z_2^p as a combination of z_1 and z_2. The subgroup scheme K' cut out by these two expressions, which are of type I, contains K but has order p^2, so $K' = K$, and we are done.

Case 3: $\#K_2 > p$. This is the same as Case 2, but with coordinates reversed. □

Theorem 12.2. *Let $p \ge 5$ be prime. Let X be a curve of genus 2 over $\mathbb{Q}_p$ with good reduction at p. Then there are at most $p^3 + p^2 + p + 7$ distinct x-coordinates of points in $X(\overline{\mathbb{Q}}_p)$ in the hyperelliptic torsion packet T.*

Proof. Let φ_1 and φ_2 be the components of the homomorphism Φ given by Corollary 6.2. Let ψ_1 and ψ_2 be their restrictions to L. Let K be the kernel of (ψ_1, ψ_2). Let ψ_1' and ψ_2' denote the homomorphisms $\mathbb{G}_a^2 \to \mathbb{G}_a$ given by Lemma 12.1. Since (ψ_1', ψ_2') has the same kernel as (ψ_1, ψ_2), each can be obtained from the other by composing with an endomorphism of the target $\mathbb{G}_a^2$. Hence, by composing Φ with an automorphism of $\mathbb{G}_a^2$, we may assume that ψ_1 and ψ_2 are of one of the types in Lemma 12.1.

For $i = 1, 2$, let $\mathcal{F}_i$ be the regular function $\varphi_i \circ \iota$ on $\mathcal{X}$, which by Lemma 8.1 is of the form

$$\mathcal{F}_i = H_i + \psi_i(w, x_0^p w)$$

where H_i is a rational function in x_0, y_0 only, and $w = x_1/y_0^p$. Then the hyperelliptic torsion packet maps into the finite subscheme $\mathcal{F}_1 = \mathcal{F}_2 = 0$ of $\mathcal{X}$.

We now eliminate w from the equations $\mathcal{F}_1 = \mathcal{F}_2 = 0$, as in Section 9. Suppose that ψ_1 and ψ_2

are of type I in Lemma 12.1. Then for some polynomials A, C, D in x_0 of degrees at most p, p, p^2 respectively, we have

$$\begin{aligned}\mathcal{F}_1 &= H_1 + Aw + w^p,\\ \mathcal{F}_2 &= H_2 + Cw + Dw^p,\\ \mathcal{F}_1^p &= H_1^p + A^p w^p + w^{p^2},\\ \mathcal{F}_2^p &= H_2^p + C^p w^p + D^p w^{p^2}.\end{aligned}$$

This can be rewritten in terms of matrices:

$$\begin{pmatrix} H_1 - \mathcal{F}_1 & A & 1 & 0\\ H_2 - \mathcal{F}_2 & C & D & 0\\ H_1^p - \mathcal{F}_1^p & 0 & A^p & 1\\ H_2^p - \mathcal{F}_2^p & 0 & C^p & D^p \end{pmatrix} \begin{pmatrix} 1\\ w\\ w^p\\ w^{p^2}\end{pmatrix} = 0,$$

so the 4×4 matrix has zero determinant, and

$$\det \begin{pmatrix} H_1 & A & 1 & 0\\ H_2 & C & D & 0\\ H_1^p & 0 & A^p & 1\\ H_2^p & 0 & C^p & D^p \end{pmatrix} = \det \begin{pmatrix} \mathcal{F}_1 & A & 1 & 0\\ \mathcal{F}_2 & C & D & 0\\ \mathcal{F}_1^p & 0 & A^p & 1\\ \mathcal{F}_2^p & 0 & C^p & D^p \end{pmatrix}.$$

The entries of the second, third, and fourth columns are polynomials in x_0 of degree at most p, p^2, and p^3, respectively. Expanding the right-hand side in minors along the first column shows that it is a combination of the regular functions $\mathcal{F}_1$, $\mathcal{F}_2$, $\mathcal{F}_1^p$, $\mathcal{F}_2^p$ on $\mathcal{X}$ weighted by polynomials in x_0 of degree at most $p^3 + p^2 + p$. In particular it is regular wherever x_0 is, and $x_0^{-(p^3+p^2+p)}$ is regular along the polar divisor of x_0 on $\mathcal{X}$. But the left-hand side is a rational function in x_0, y_0 only, and is odd with respect to the hyperelliptic involution. Combining these observations shows that both sides equal $I(x_0)y_0$ for some polynomial I of degree at most $p^3 + p^2 + p$. The nonvanishing of I follows from the finiteness of the subscheme F of $\mathcal{X}$ cut out by $\mathcal{F}_1 = \mathcal{F}_2$ and the theory of p-resultants.

But by the right-hand side definition of $I(x_0)y_0$, I vanishes on the image of $F(\overline{\mathbb{F}}_p)$ in $X_s(\overline{\mathbb{F}}_p)$, except possibly at points where x_0 fails to be regular or where y_0 vanishes. Hence, since $X \cap A_{\text{tors}}$ injects into $X_s(\overline{\mathbb{F}}_p)$, the number of distinct x-coordinates in $X(\overline{\mathbb{Q}}_p)$ of torsion points on X is at most p^3+p^2+p+7, where the $+7$ comes from the six Weierstrass x-coordinates, and $x_0 = \infty$. □

Remark. The same proof, with the same bound, can be made to work for smooth genus 2 curves X over $W(\overline{\mathbb{F}}_p)$. Also, with a little more work, we could improve the bound slightly, by studying more carefully the valuation of I at ∞, and at the Weierstrass x-coordinates. But the main term, p^3, would be the same.

Corollary 12.3. *Under the hypotheses of Theorem* 12.2, *the hyperelliptic torsion packet T contains at most $2p^3 + 2p^2 + 2p + 8$ torsion points.*

Proof. There are at most p^3+p^2+p+1 non-Weierstrass x-coordinates (possibly including ∞), each giving rise to at most two points of the hyperelliptic torsion packet; there are also six Weierstrass points. □

Remark. The bound in Corollary 12.3 is a significant improvement over the bound $\#T \le 36p^9 + 216p^8$ obtained by applying the general Theorem A of [Buium 1996] to the case $g = 2$ with a Weierstrass point as basepoint.

13. COMBINING p-ADIC INFORMATION FOR DIFFERENT PRIMES p

As we will discuss in the next section, the running time of the algorithm varies widely with the curve. In the cases where the algorithm is slow, most of the time is spent in lifting to torsion points (page 459), where one has a large degree factor of the polynomial $r(x_0)$, and tries to lift the corresponding point in $A_s(\overline{\mathbb{F}}_p)$ (or rather its image in the Kummer surface) to a torsion point in $A(\mathbb{Q}_p^{\text{unr}})$ to higher p-adic precision.

There is sometimes a way to prove *a priori* that the roots of these large degree factors of $r(x_0)$ cannot lift to x-coordinates of points in T, using the bound of Theorem 12.2 for a smaller prime l. We illustrate this through an example.

Let X be the genus 2 modular curve $X_0(31)$. Although X has good reduction at 5, the algorithm with the improved homomorphism fails for $p = 5$ because it turns out that $\dim W'$ (see Section 8) is 3 instead of 2.

We try again using $p = 7$. This time the interpolation shows that $\dim W' = 2$ and $L[W']$ is finite, so the method will succeed, in theory. The degrees of the irreducible factors of the polynomial $r(x_0) \in \mathbb{F}_7[x_0]$ of Section 9 turn out to be 3, 3, 8, 67, and 272. The first two factors are from the Weierstrass points. A few seconds of computation show

that a point in $A_s(\overline{\mathbb{F}}_p)$ corresponding to the degree 8 factor does not lift to a torsion point, and a 50-minute computation shows that the same holds for the degree 67 factor, but we run out of memory trying to prove the same for the degree 272 factor. If there actually were a point of T whose x-coordinate reduced modulo 7 to a root of this degree 272 factor, its degree over $\mathbb{Q}$ would be at least 272, however, and then the number of distinct x-coordinates of points in T would be at least 272, contradicting the bound $5^3+5^2+5+7=162$ given by Theorem 12.2 for the prime 5. Thus the 5-adic bound lets us finish the 7-adic computation without examining the degree 272 factor.

14. EXAMPLES

Table 1 lists some genus 2 curves X over $\mathbb{Q}$, specified by giving a separable quintic or sextic polynomial $f(x) \in \mathbb{Q}[x]$ such that X is birational to $y^2 = f(x)$. For each, we give the smallest prime $p > 2g = 4$ for which the method with the improved homomorphism worked, the number of points in the hyperelliptic torsion packet T, and a list of irreducible polynomials in $\mathbb{Q}[x]$ whose roots are a complete list of the x-coordinates of the non-Weierstrass points in T. We include ∞ in the latter list, if there are non-Weierstrass points in T with $x = \infty$. When there is more than one prime p listed, the algorithm was run using the first one, but using the Theorem 12.2 bound for the second prime to weed out large degree factors, as discussed in Section 13.

It is hard to predict in advance how long the program will take to compute T for a given curve. The running time depends on the size of the smallest usable p, but also can be dramatically reduced in certain favorable cases, for instance when the reduction X_s is superspecial, i.e., when the Cartier operator acts as zero on the space of regular differentials. The curves in the table taking the most and least time, respectively, were $y^2 = x^5 + 1$ (over 4 hours) and $y^2 = x^6 + 1$ (under 14 seconds). These timings were on a 300 MHz Sun Ultra 2.

Modular Curves

The curve $X_0(N)$ is the smooth projective model of the coarse moduli space over $\mathbb{Q}$ parameterizing pairs (E, C) where E is an elliptic curve and C is a cyclic subgroup of E of order N. The curve $X_1(N)$ is the same, except parameterizing pairs (E, P) where P is a point on E of order N. For prime N, $X_0^+(N)$ is the quotient of $X_0(N)$ by the Atkin-Lehner involution W_N; it is the smooth projective model of the coarse moduli space parameterizing unordered pairs of N-isogenous elliptic curves. Many of the explicit equations for these modular curves are classical; in any case, we copied them from [Hasegawa 1995], with a change of variables in a few cases.

By [Ogg 1974], $X_0(N)$ is hyperelliptic (of genus at least 2) if and only if $N \in \{22, 23, 26, 28, 29, 30, 31, 33, 35, 37, 39, 40, 41, 46, 47, 48, 50, 59, 71\}$; but, as was known much earlier, the only curves $X_0(N)$ of genus 2 are the eight listed in Table 1. By [Ishii and Momose 1991], $X_1(N)$ is hyperelliptic if and only if $N \in \{13, 16, 18\}$; in each case the genus is 2. All the $X_0^+(N)$ of genus 2 with N prime are listed in Table 1. Drinfel'd [1973] generalized a result of Manin [1972] to prove that the cusps on the quotient of the extended upper half plane by any congruence subgroup of $SL_2(\mathbb{Z})$ lie in a single torsion packet. (For other proofs of this "Manin-Drinfel'd theorem," see [Elkik 1990] or [Kubert and Lang 1981, Chapter 5, Theorem 3.1].) We call this packet the *cuspidal torsion packet*; it coincides with the hyperelliptic torsion packet for all the $X_0(N)$ and $X_1(N)$ in the table except $X_0(37)$, and for *none* of the $X_0^+(N)$ in the table.

Suppose $X = X_0(N)$ is of genus 2, and N is prime. Let C denote the set of cusps, and let H be the set of Weierstrass points (points fixed by the hyperelliptic involution) if $X_0(N)$ is hyperelliptic and $N \neq 37$, and let $H = \varnothing$ otherwise. Coleman, Kaskel, and Ribet [Coleman et al. 1999] conjectured that the cuspidal torsion packet of $X_0(N)$ equals $C \cup H$. This was proved independently by M. Baker [2000] and A. Tamagawa [2001]. Hence the only new results in the entries for $X_0(N)$ in Table 1 are for composite N, and for $N = 37$. The paper [Coleman et al. 1999] gives several proofs that the cuspidal torsion packet for $X_0(37)$ consists of only the two cusps, while our computation shows that the hyperelliptic torsion packet consists only of the six Weierstrass points.

Coleman remarked [1985, p. 155] that $X_1(13)$ has $\#T \geq 22$, because T contains at least 12 cusps, 6 Weierstrass points, and 4 points fixed by the or-

curve	$f(x)$	p	$\#T$	minimal polynomials of x-coordinates
$X_0(22)$	$x^6-4x^4+20x^3-40x^2+48x-32$	7	10	∞, $x-2$
$X_0(23)$	$x^6-8x^5+2x^4+2x^3-11x^2+10x-7$	5	8	∞
$X_0(26)$	$x^6-8x^5+8x^4-18x^3+8x^2-8x+1$	5	10	∞, x
$X_0(28)$	$x^6+10x^4+25x^2+28$	5	16	∞, $x-1$, $x+1$, x^2+3
$X_0(29)$	$x^6-4x^5-12x^4+2x^3+8x^2+8x-7$	5	8	∞
$X_0(31)$	$x^6-8x^5+6x^4+18x^3-11x^2-14x-3$	7, 5	8	∞
$X_0(37)$	$x^6+8x^5-20x^4+28x^3-24x^2+12x-4$	5	6	
$X_0(50)$	$x^6-4x^5-10x^3-4x+1$	7	20	∞, x, $x+1$, $x^4-x^3+x^2-x+1$
$X_1(13)$	$x^6+2x^5+x^4+2x^3+6x^2+4x+1$	5	22	∞, x^3+4x^2+x-1, x^2+x+1, $x+1$, x
$X_1(16)$	$-x^5+2x^4+2x^2+x$	7	14	$x-1$, $x+1$, x^2+2x-1
$X_1(18)$	$x^6+2x^5+5x^4+10x^3+10x^2+4x+1$	5	22	∞, x^3-3x-1, x^2+x+1, $x+1$, x
$X_0^+(67)$	$x^6-4x^5+6x^4-6x^3+9x^2-14x+9$	5	6	
$X_0^+(73)$	$x^6-4x^5+6x^4+2x^3-15x^2+10x+1$	7, 5	6	
$X_0^+(103)$	$x^6-10x^4+22x^3-19x^2+6x+1$	5	6	
$X_0^+(107)$	$x^6-4x^5+10x^4-18x^3+17x^2-10x+1$	5	6	
$X_0^+(167)$	$x^6-4x^5+2x^4-2x^3-3x^2+2x-3$	5	6	
$X_0^+(191)$	$x^6+2x^4+2x^3+5x^2-6x+1$	7, 5	6	
C	x^5+1	19	18	x, x^5-4
V	x^6+1	5	10	∞, x
BG_1	x^5+x	5	22	x^4-4x^2+1, x^4+4x^2+1
BG_2	x^5+5x^3+x	5	6	
P	x^5-x+1	5	6	
B_{277}	$x^6-2x^5-x^4+4x^3+3x^2+2x+1$	7, 5	10	∞, x
L_{29}	$4x^6-4x^5+x^4-8x^3+20x^2-16x+4$	5	12	∞, $x-1$, x
HLP_{63}	$897x^6-197570x^4+79136353x^2-146398496$	11, 5	6	

TABLE 1. Hyperelliptic torsion packets of genus 2 curves $y^2 = f(x)$. The column headed p shows the smallest prime for which the method with the improved homomorphism worked; the next column gives the number of points in the hyperelliptic torsion packet, and the last one gives irreducible polynomials in $\mathbb{Q}[x]$ whose roots are a complete list of the x-coordinates of the non-Weierstrass points in T.

der 3 diamond operator $\langle 3\rangle \in \mathrm{Aut}(X_1(13))$. This was apparently the only known result on the torsion packets on $X_1(N)$ before the present paper. Our program shows that T for $X_1(13)$ contains no other points. For $X_1(16)$, T equals the set of 14 cusps, which include the Weierstrass points. And for $X_1(18)$, T is the union of the 16 cusps and the 6 Weierstrass points.

Baker [2000] also proved that for all prime N, the cuspidal torsion packet of $X_0^+(N)$ consists of only the one cusp. In the genus 2 cases, all of which are in Table 1, we find that the hyperelliptic torsion packet contains only the six Weierstrass points. In particular, the cuspidal and hyperelliptic torsion packets are distinct, so ι sends the cusp to a rational point of infinite order on the Jacobian.

Other Curves of Genus Two

The literature contains a few other computations of T for genus 2 curves over $\mathbb{Q}$. We succeeded in verifying all we could find, and we computed T for a few other curves.

Coleman [1986, end] worked 11-adically to prove that a curve isomorphic over $\overline{\mathbb{Q}}$ to $C : y^2 = x^5+1$ has $\#T = 18$. Voloch [1997] showed that $V : y^2 = x^6+1$ has $\#T = 10$. He used a 7-adic method which can be viewed as a simplification of ours: it is simpler because he exploited the fact that its Jacobian modulo 7^2 is a canonical lift, and that the Jacobian is isoge-

nous over $\mathbb{Q}$ to a product of (equal) elliptic curves. Boxall and Grant [2000], in addition to giving a new calculation of T for C, determined T for the curves BG_1 and BG_2 in Table 1, by using the Galois action on torsion points. The curve P has no particularly special properties we know of; in addition to having trivial hyperelliptic torsion packet, its Jacobian A satisfies

$$A(\mathbb{Q})_{\text{tors}} = \{0\} \quad \text{and} \quad \text{End}(A_{\bar{\mathbb{Q}}}) = \mathbb{Z}$$

(as computing the zeta functions over $\mathbb{F}_3$ and $\mathbb{F}_7$ shows), the typical situation. The smallest prime known to occur as the conductor of the Jacobian of a genus 2 curve over $\mathbb{Q}$ so far is 277; we learned of the existence of this curve from a talk of Brumer, and hence name it B_{277}. The largest positive integer (respectively, prime integer) known to occur as the order of a rational torsion point on a 2-dimensional Jacobian over $\mathbb{Q}$ so far is 63 (respectively, 29); the corresponding curves are HLP_{63} and L_{29}, from [Howe et al. 2000] and [Leprévost 1993].

The one curve we tried for which our algorithm failed was the curve

$$y^2 = 278271081x^6 - 5238713058x^4 + 22999624761x^2 - 229833600 \quad (14\text{–}1)$$

having 588 rational points [Keller and Kulesz 1995], the current record for a genus 2 curve over $\mathbb{Q}$. It was not the large coefficients that created the difficulty: the algorithm does not even see this for much of the time, while doing computations modulo p^2 for a small prime p. (Indeed, adding 1 to the right-hand side of (14–1) resulted in a curve for which T could be readily computed using $p = 7$.) Instead, the problem was that none of the first few primes was good for our method.

Remark 1. There are infinitely many genus 2 curves over $\mathbb{C}$ having $\#T = 22$ [Poonen 2000] , but it is not known whether there is a single genus 2 curve over $\mathbb{C}$ with larger $\#T$. It seems likely that there exists a uniform bound for $\#T$ for all genus 2 curves over $\mathbb{C}$, but this too is not known.

Remark 2. Table 1 shows that every even integer between 6 and 22 inclusive occurs as $\#T$ for a curve of genus 2 over $\mathbb{Q}$.

ACKNOWLEDGEMENTS

I thank E. V. Flynn for making his Kummer surface routines, written in Maple, available electronically, and Michael Stoll for translating them from Maple into GP–PARI, the software package used to implement the algorithm of this paper.

REFERENCES

[Baker 2000] M. H. Baker, "Torsion points on modular curves", *Invent. Math.* **140**:3 (2000), 487–509.

[Bosch et al. 1990] S. Bosch, W. Lütkebohmert, and M. Raynaud, *Néron models*, Ergebnisse der Mathematik (3) **21**, Springer, Berlin, 1990.

[Boxall and Grant 2000] J. Boxall and D. Grant, "Examples of torsion points on genus two curves", *Trans. Amer. Math. Soc.* **352**:10 (2000), 4533–4555.

[Buium 1996] A. Buium, "Geometry of p-jets", *Duke Math. J.* **82**:2 (1996), 349–367.

[Cassels and Flynn 1996] J. W. S. Cassels and E. V. Flynn, *Prolegomena to a middlebrow arithmetic of curves of genus* 2, London Math. Soc. Lecture Note Series **230**, Cambridge Univ. Press, Cambridge, 1996.

[Coleman 1985] R. F. Coleman, "Torsion points on curves and p-adic abelian integrals", *Ann. of Math.* (2) **121**:1 (1985), 111–168.

[Coleman 1986] R. F. Coleman, "Torsion points on Fermat curves", *Compositio Math.* **58**:2 (1986), 191–208.

[Coleman 1987] R. F. Coleman, "Ramified torsion points on curves", *Duke Math. J.* **54**:2 (1987), 615–640.

[Coleman 1989] R. F. Coleman, "Torsion points on abelian étale coverings of $\mathbb{P}^1 - \{0, 1, \infty\}$", *Trans. Amer. Math. Soc.* **311**:1 (1989), 185–208.

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

[Coleman et al. 1999] R. Coleman, B. Kaskel, and K. A. Ribet, "Torsion points on $X_0(N)$", pp. 27–49 in *Automorphic forms, automorphic representations, and arithmetic* (Fort Worth, TX, 1996), vol. 1, Proc. Sympos. Pure Math. **66**, Amer. Math. Soc., Providence, RI, 1999.

[Drinfel'd 1973] V. G. Drinfel'd, "Two theorems on modular curves", *Funkcional. Anal. i Priložen.* **7**:2 (1973), 83–84. In Russian; translation in *Functional Anal. Appl.* **7** (1973), 155–156.

[Elkik 1990] R. Elkik, "Le théorème de Manin–Drinfel'd", pp. 59–67 in *Séminaire sur les pinceaux de courbes elliptiques* (Paris, 1988), Astérisque **183**, Soc. math. France, Paris, 1990.

[Flynn 1993] E. V. Flynn, "The group law on the Jacobian of a curve of genus 2", *J. Reine Angew. Math.* **439** (1993), 45–69.

[Goss 1996] D. Goss, *Basic structures of function field arithmetic*, Ergebnisse der Mathematik (3) **35**, Springer, Berlin, 1996.

[Greenberg 1961] M. J. Greenberg, "Schemata over local rings", *Ann. of Math.* (2) **73** (1961), 624–648.

[Greenberg 1963] M. J. Greenberg, "Schemata over local rings, II", *Ann. of Math.* (2) **78** (1963), 256–266.

[Hasegawa 1995] Y. Hasegawa, "Table of quotient curves of modular curves $X_0(N)$ with genus 2", *Proc. Japan Acad. Ser. A Math. Sci.* **71**:10 (1995), 235–239.

[Hindry 1988] M. Hindry, "Autour d'une conjecture de Serge Lang", *Invent. Math.* **94**:3 (1988), 575–603.

[Howe et al. 2000] E. W. Howe, F. Leprévost, and B. Poonen, "Large torsion subgroups of split Jacobians of curves of genus two or three", *Forum Math.* **12**:3 (2000), 315–364.

[Hrushovski ≥ 2001] E. Hrushovski, "The Manin–Mumford conjecture and the model theory of difference fields", *Ann. Pure Appl. Logic*. To appear.

[Ishii and Momose 1991] N. Ishii and F. Momose, "Hyperelliptic modular curves", *Tsukuba J. Math.* **15**:2 (1991), 413–423.

[Katz 1981] N. M. Katz, "Galois properties of torsion points on abelian varieties", *Invent. Math.* **62**:3 (1981), 481–502.

[Keller and Kulesz 1995] W. Keller and L. Kulesz, "Courbes algébriques de genre 2 et 3 possédant de nombreux points rationnels", *C. R. Acad. Sci. Paris Sér. I Math.* **321**:11 (1995), 1469–1472.

[Kubert and Lang 1981] D. S. Kubert and S. Lang, *Modular units*, Grundlehren der Math. Wissenschaften **244**, Springer, New York, 1981.

[Leprévost 1993] F. Leprévost, "Points rationnels de torsion de jacobiennes de certaines courbes de genre 2", *C. R. Acad. Sci. Paris Sér. I Math.* **316**:8 (1993), 819–821.

[Manin 1972] J. I. Manin, "Parabolic points and zeta functions of modular curves", *Izv. Akad. Nauk SSSR Ser. Mat.* **36** (1972), 19–66. In Russian; translated in *Math. USSR Izv.* **6** (1972), 19–64.

[Milne 1986] J. S. Milne, "Jacobian varieties", pp. 167–212 in *Arithmetic geometry* (Storrs, CT, 1984), edited by G. Cornell and J. H. Silverman, Springer, New York, 1986.

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

[Poonen 1999] B. Poonen, "Mordell–Lang plus Bogomolov", *Invent. Math.* **137**:2 (1999), 413–425.

[Poonen 2000] B. Poonen, "Genus-two curves with 22 torsion points", *C. R. Acad. Sci. Paris Sér. I Math.* **330**:7 (2000), 573–576.

[Raynaud 1983] M. Raynaud, "Courbes sur une variété abélienne et points de torsion", *Invent. Math.* **71**:1 (1983), 207–233.

[Ribet 1999] K. A. Ribet, "Almost rational torsion points", May 1999. Lectures at the University of Arizona.

[Szpiro et al. 1997] L. Szpiro, E. Ullmo, and S. Zhang, "Équirépartition des petits points", *Invent. Math.* **127**:2 (1997), 337–347.

[Tamagawa 2001] A. Tamagawa, "Ramification of torsion points on curves with ordinary semistable Jacobian varieties", *Duke Math. J.* **106**:2 (2001), 281–319.

[Tzermias 2000] P. Tzermias, "The Manin-Mumford conjecture: a brief survey", *Bull. London Math. Soc.* **32**:6 (2000), 641–652.

[Ullmo 1998] E. Ullmo, "Positivité et discrétion des points algébriques des courbes", *Ann. of Math.* (2) **147**:1 (1998), 167–179.

[Voloch 1997] J. F. Voloch, "Torsion points on $y^2 = x^6 + 1$", 1997. See http://www.ma.utexas.edu/users/voloch/preprint.html.

Bjorn Poonen, Department of Mathematics, University of California, Berkeley, CA 94720-3840, United States (poonen@math.berkeley.edu)

Received November 3, 2000; accepted in revised form February 26, 2001