TORSION POINTS ON $X_0(N)$

Robert Coleman, Bruce Kaskel and Kenneth A. Ribet

University of California, Berkeley

To professor Goro Shimura

Abstract. Let N be a prime number, and let X be the modular curve $X_0(N)$, considered over the field of complex numbers. Suppose that the genus of X is at least 2, i.e., that N is at least 23. Using the cusp at infinity on X, we identify X with a subvariety of positive codimension of the Jacobian of X. The set of points on X which map to torsion points on the Jacobian is a finite set (Manin-Mumford conjecture) which always contains the two cusps on X and which contains the hyperelliptic branch points on X in the special case where X is hyperelliptic and N is different from 37. We conjecture that this set contains no other points, and verify our conjecture when $N = 37$. For general N, we accumulate information about this set in the direction of the conjecture. With this information in hand, M. Baker has been able to prove the conjecture for certain other values of N.

1. Introduction

Let X be a complex algebraic curve of genus > 1. Choosing a base point $x_0 \in X$, we view X as a subvariety of its Jacobian $J = J(X)$ via the Albanese map which sends each $x \in X$ to the class of the divisor $(x) - (x_0)$. Let J_{tor} be the group of torsion points on J. The Manin-Mumford conjecture states that the intersection

$$\mathcal{S} := X \cap J_{\text{tor}}$$

is finite.

This conjecture was studied first by S. Lang [18], who showed that is implied by a statement about the action of $\text{Gal}(\overline{K}/K)$ on J_{tor}, where K is a finitely generated subfield of $\mathbf{C}$ over which X and x_0 are defined. Lang's hypothesis states that the image of $\text{Gal}(\overline{K}/K)$ in $\text{Aut}\, J_{\text{tor}}$ contains an open subgroup of the homothety group $\hat{\mathbf{Z}}^* \subseteq \text{Aut}\, J_{\text{tor}}$. The statement remains unproved, despite partial results by Bogomolov [1] and Serre [32]. (See also [14], which may be regarded as a sequel to [18].)

Meanwhile, the Manin-Mumford conjecture was proved by M. Raynaud in a 1983 article [28]. Subsequently, a second proof of the conjecture was given by R. Coleman in [4]. Generalizations and strengthenings of the Manin-Mumford conjecture have been proposed in various quarters. For example, a recent article by E. Ullmo [34] studies points on X which map to points of J with small canonical height. (See also [24].)

This work was partially supported by grants from the National Science Foundation. The authors thank M. Baker for helpful feedback to preliminary drafts of our manuscript and for compiling the list of errata to [4] which appears at the end of this article.

This article concerns the intersection $X \cap J_{\text{tor}}$ in the special case where X is a modular curve. More specifically, we limit our attention to the curve $X = X_0(N)$ where N is a prime number. The requirement that X have genus > 1 becomes the condition $N \geq 23$, which we now impose. We take x_0 to be the standard "cusp at ∞," which we call C_∞.

A general theorem of Manin-Drinfeld implies that $\mathcal{S}$ contains the set of cusps on X. There are two cusps, the standard cusp C_∞, which maps to 0 in $J_0(N)$, and a second cusp, C_0, which maps to a point on $J_0(N)$ of order $n := \text{num}\,\frac{N-1}{12}$. (See [21, Ch. II, §11] for a discussion of the group C generated by C_0 on $J_0(N)$; this group is called the cuspidal subgroup of $J_0(N)$. Theorem 1.2 of [21, Ch. III] states that C is the torsion subgroup of the Mordell-Weil group of J.) The inclusion $\{C_0, C_\infty\} \subseteq \mathcal{S}$ is the first piece of information about $\mathcal{S}$ at our disposal. Because of it, we describe $\mathcal{S}$ as the "cuspidal torsion packet" on X. (As the reader may recall, Coleman uses the term "torsion packet" to refer to $X \cap J_{\text{tor}}$ in [2, 4].)

A second constraint on $\mathcal{S}$ arises from the fixed points of the hyperelliptic involution of X if $X = X_0(N)$ is a hyperelliptic curve:

Proposition 1.1. *Suppose that X is hyperelliptic, and let P be a fixed point of the hyperelliptic involution of X. Then we have $P \in \mathcal{S}$ if and only if N is different from 37. In this latter case, $2P$ belongs to the cuspidal subgroup of J.*

Proof. Let h be the hyperelliptic involution. Since h operates on $J = J_0(N)$ as -1, the images in J of the divisors $(P) - (C_\infty)$ and $\big(h(C_\infty)\big) - (P)$ are equal. Adding $(P) - (C_\infty)$, we find that $2\big((P) - (C_\infty)\big)$ and $\big(h(C_\infty)\big) - (C_\infty)$ are equal on J. Hence we have $P \in \mathcal{S}$ if and only if the point $h(C_\infty)$ has finite order in J. A theorem of Ogg states that X is hyperelliptic if and only if N is either 37 or one of the seven primes 23, 29, 31, 41, 47, 59 and 71. (See [26, Th. 2] and the article [27].) For the last seven primes on the list, h is the Atkin-Lehner involution $w = w_N$ of X and hence $h(C_\infty)$ is the cusp C_0. In particular, $h(C_\infty)$ has finite order on J, so that P belongs to $\mathcal{S}$. Further, the point $2P$ on J is the class of the divisor $(C_0) - (C_\infty)$, which is a generator of the cuspidal group C. For the exceptional case $N = 37$, Mazur and Swinnerton-Dyer [23, §5] have observed that $h(C_\infty)$ has infinite order on J. Hence P is not an element of $\mathcal{S}$. ∎

Let $\mathcal{S}_0$ be the set which is defined as follows: If X is not hyperelliptic or if $N = 37$, $\mathcal{S}_0 = \{C_0, C_\infty\}$; if X is hyperelliptic and $N \neq 37$, $\mathcal{S}_0$ is the set consisting of the two cusps of X and the hyperelliptic fixed points on X. We then have in all cases

$$\mathcal{S}_0 \subseteq \mathcal{S}.$$

It seems plausible to us that this inclusion is an equality, i.e., that one has

$$\mathcal{S} \stackrel{?}{=} \mathcal{S}_0$$

for all $N \geq 23$*. Despite the somewhat ad hoc definition of $\mathcal{S}_0$, the equality $\mathcal{S} = \mathcal{S}_0$ has a simple restatement:

---

* Through the efforts of Matt Baker we now know this equality is true for N a prime number in the set $\{23, 29, 37, 41, 47, 59\}$. Note that $X_0(N)$ is hyperelliptic in each of these cases.

Proposition 1.2. *We have $\mathcal{S} = \mathcal{S}_0$ if and only if $2P$ is a rational point of J for all $P \in \mathcal{S}$.*

Proof. Assume that $\mathcal{S} = \mathcal{S}_0$, and let P be an element of $\mathcal{S}$. If P is one of the two cusps of $X_0(N)$, then P is rational. If P is not a cusp, then P is a hyperelliptic branch point of $X_0(N)$ and N is different from 37. We have seen in this case that $2P$ lies in the cuspidal group C; in particular, $2P$ is rational. Assume now that $2P$ is rational for each $P \in \mathcal{S}$. Take $P \in \mathcal{S}$ and suppose first that P is not itself a rational point. Then there is a $g \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ such that $gP \neq P$. The difference $gP - P$, computed on J, is then a 2-division point because $2P$ is rational. This means that the non-zero divisor $2(gP) - 2(P)$ is the divisor of a rational function on $X_0(N)$. This function defines a degree-two map $X_0(N) \to \mathbf{P}^1$ for which P is a ramified point. We find then that P is a hyperelliptic branch point of $X_0(N)$. Since P lies in $\mathcal{S}$, we must have $N \neq 37$; thus P is a point in $\mathcal{S}_0$. The second possibility is that P is a rational point of $X_0(N)$. In that case, P lies in the intersection $C \cap X_0(N)$, in view of Mazur's theorem [21, p. 33] that C is the torsion subgroup of the Mordell-Weil group of $J_0(N)$. We need to know that this intersection consists of the two cuspidal points C_0 and C_∞ of J. One way to proceed is to cite the well-known theorem of Mazur [22, Th. 7.1] which states for all but four prime numbers $N \geq 23$ that $X_0(N)(\mathbf{Q}) = \{C_0, C_\infty\}$. The four exceptional primes are $N = 37$, 43, 67, and 163. For the first of these primes, the equality $X_0(N) \cap C = \{C_0, C_\infty\}$ is proved by Mazur and Swinnerton-Dyer [23, §5, Prop. 2]. For the primes 43, 67, and 163, there is a unique non-cuspidal point of $X_0(N)$, which arises from elliptic curves with complex multiplication by $\mathbf{Q}(\sqrt{N})$. By uniqueness, this point is fixed by the Atkin-Lehner involution w of $X_0(N)$. Since w operates on C by multiplication by -1 [21, p. 99], and since $n = \mathrm{num}\,\frac{N-1}{12}$ is odd when $N = 43$, 67 and 163, the desired statement follows. ∎

In this article, we present an assortment of results about $\mathcal{S}$. These include theorems proved by the p-adic techniques of the first author [2, 4] and an inequality (proved in §4) which is presented "in the spirit of Lang [18]."

To illustrate the scope of our results, we will state a theorem which is valid for all $N \geq 23$ and a complement which concerns the special case $N = 37$. Before presenting these results, we introduce some notation: First, we let $\mathbf{T}$ be the ring of endomorphisms of $J_0(N)$, i.e., the ring of Hecke operators acting on the space of weight-two cusp forms on $\Gamma_0(N)$. (See [21, Ch. II, Prop. 9.5].) Further, we write P_p for the "p-primary part" of P, whenever P is a torsion point on J and p is a prime number. Thus P is the sum of its p-primary parts (as p ranges over the set of primes) and P_p has p-power order. Using [21, Ch. III, Th. 1.2], we may restate Proposition 1.2 as follows: the equality $\mathcal{S} = \mathcal{S}_0$ holds if and only if $2P_p$ lies in the cuspidal group C for all primes p and all $P \in \mathcal{S}$.

Theorem 1.3. *Let P be an element of $\mathcal{S}$, and let $p \neq 2, 3$ be a prime for which P_p does not belong to the cuspidal group C. Then at least one of the following holds: (i) $p = N$; (ii) p satisfies $5 \leq p < 2g$, $X_0(N)$ does not have ordinary reduction at p, and p is ramified in $\mathbf{T}$ in the sense that $\mathbf{T}/p\mathbf{T}$ is not a product of fields. Further, suppose that $p = N$ and that N is not ramified in $\mathbf{T}$. Then there is some $\ell \neq N$ such that $P_\ell \notin C$.*

Theorem 1.4. *The intersection $X_0(37) \cap J_0(37)_{\mathrm{tor}}$ consists of the two cusps C_0 and C_∞.*

We prove the latter theorem by combining results such as Theorem 1.3 with some facts which are specific to the case and $N = 37$. In particular, we lean heavily on results which were proved by B. Kaskel in [15]; these involve a detailed description of the image of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ in $\mathrm{Aut}\, J_0(37)_{\mathrm{tor}}$. To obtain this description, Kaskel employs many of the techniques pioneered by Serre [31] and Lang-Trotter [20] in the case where $X_0(N)$ has genus one. To the best of our knowledge, no analogous description is available in general for $J_0(N)$; it would certainly be of considerable interest to find such a description.

It strikes us that the general results at our command, when augmented by the description of [15], seem to represent overkill: they allow us to prove Theorem 1.4 in several, closely related, ways. Because of our interest in the general case, we will present three proofs of the theorem in §6.

2. Ramification

Let P be a torsion point on $J = J_0(N)$. We wish to study the set of primes which ramify in the extension $\mathbf{Q}(P)/\mathbf{Q}$. First, we record the following statement, which follows directly from the main results of [4] and [2, Th. 5.5].

Theorem 2.1. *Suppose that P lies in $\mathcal{S}$. Then the extension $\mathbf{Q}(P)/\mathbf{Q}$ can be ramified only at the bad prime N, the two very small primes 2 and 3, and the primes p satisfying $5 \leq p < 2g$. Further, if $\mathbf{Q}(P)/\mathbf{Q}$ is ramified at $p = 3$, then the ramification at 3 is tame. Finally, if $\mathbf{Q}(P)/\mathbf{Q}$ is ramified at p and p satisfies $5 \leq p < 2g$, then X does not have ordinary reduction at p.*

For each prime number p, we again write P_p for the "p-primary component of P." Further, we again use the symbol $\mathbf{T}$ to denote the ring of endomorphisms of $J_0(N)$, i.e., the ring of Hecke operators acting on the space of weight-two cusp forms on $\Gamma_0(N)$. Finally, we recall that a prime number p is said to be *Eisenstein* if it divides the order of the cuspidal subgroup C of J.

Theorem 2.2. *Suppose that the field extension $\mathbf{Q}(P)/\mathbf{Q}$ is unramified at p. Then either $p = 2$, or P_p belongs to the cuspidal group C.*

Proof. Assume, to the contrary, that p is an odd prime and that P_p is not contained in the cuspidal group C. Let M be the $\mathbf{T}[\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})]$-submodule of $J_0(N)(\overline{\mathbf{Q}})_{\mathrm{tor}}$ which is generated by P_p. Then M is a finite abelian group of p-power order which is not contained in C. As a module for the Galois group $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, M is unramified at p.

As explained in [21, Ch. II, §14], the Jordan-Hölder constituents of M can only be of the following three forms: (i) the constant group $\mathbf{Z}/p\mathbf{Z}$; (ii) the group μ_p; (iii) an irreducible module of the form $J_0(N)[\mathfrak{m}]$, where $\mathfrak{m}$ is a non-Eisenstein maximal ideal of $\mathbf{T}$ with residue characteristic p. Types (i) and (ii) occur only if p is an Eisenstein prime, i.e., if p divides the integer n introduced above. However, since p is odd, the modules of types (ii) and (iii) are visibly ramified at p: note that the determinant of $J_0(N)[\mathfrak{m}]$ is the mod p cyclotomic character. In view of our supposition that M is unramified at p, M is a successive extension of copies of $\mathbf{Z}/p\mathbf{Z}$, so that p is a divisor of n. In particular p and N are distinct.

We view M as an extension of $Q := M/M_C$ by M_C, where M_C is the intersection $M \cap C$. Since M is not contained in C, Q is non-zero. Let $Q' \cong \mathbf{Z}/p\mathbf{Z}$ be a minimal sub-module of Q, and let M' be the inverse image of Q' in M. Thus we have a

tautological exact sequence

$$0 \to M_C \to M' \to Q' \to 0$$

in which the groups M_C and Q' are trivial $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-modules.

We claim that M' is unramified at N. This claim follows from an argument due to Mazur [21, Ch. II, Lemma 16.5], which we shall now recapitulate. Let σ be an element of an inertia group for the prime N in $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, and let m be an element of M'. Let p^r be the order of m. Grothendieck's theory of semistable reduction (together with the Deligne-Rapoport theorem [11] that $J_0(N)$ has multiplicative reduction at N) shows that $\sigma m - m$ belongs to the "toric part" of $J_0(N)[p^r](\overline{\mathbf{Q}}_N)$. The displayed exact sequence forces $\sigma m - m$ to be an element of C. However, reduction mod N induces an isomorphism between C and the group of connected components of the Néron model for $J_0(N)$ in characteristic N; this yields in particular that the intersection of C and the toric part of $J_0(N)[p^r](\overline{\mathbf{Q}}_N)$ is zero. Hence $\sigma m - m = 0$, which proves what was claimed.

Now M' can be ramified a priori only at p and at N. We have just seen that M' is unramified at N, and the hypothesis to the theorem implies that it is unramified at p. It is therefore everywhere unramified, so that the action of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ on M' must be trivial. In other words, we have $M' \subseteq J_0(N)(\mathbf{Q})_{\mathrm{tor}}$. On the other hand, one of the main results of [21] asserts that $C = J_0(N)(\mathbf{Q})_{\mathrm{tor}}$. We thus have $M' = M_C$ and $Q' = 0$, which is a contradiction. ∎

Corollary 2.3. *Let P be an element of $\mathcal{S}$, and assume that P_p does not belong to the cuspidal group C. Then at least one of the following holds: (i) $p = 2$ or $p = 3$; (i) $p = N$; (ii) p satisfies $5 \leq p < 2g$ and X does not have ordinary reduction at p.*

This corollary results directly from the two results above. We have stated it in order to record our progress toward proving Theorem 1.3.

Theorem 2.4. *Suppose that $P \in \mathcal{S}$ and that the order of P is even but not divisible by N. Assume that N is not congruent to 1 mod 8. Then P belongs to $\mathcal{S}_0$.*

Proof. It will be convenient to write the order of P as $2d$. Let R be the 2-division point dP. We claim that the extension $\mathbf{Q}(R)/\mathbf{Q}$ is ramified at the prime N.

For this, let M be the $\mathbf{T}[\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})]$-submodule of $J_0(N)(\overline{\mathbf{Q}})_{\mathrm{tor}}$ which is generated by R; further, let V be a minimal submodule of M. Thus V is a constituent of $J_0(N)[2]$ which belongs to a maximal ideal $\mathfrak{m}$ of $\mathbf{T}$ of residue characteristic 2. (See [21, Ch. II, §14] for the terminology.) In view of the hypothesis $N \not\equiv 1 \bmod 8$, $\mathfrak{m}$ cannot be an Eisenstein ideal; this means that V is an irreducible 2-dimensional representation of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ over $\mathbf{T}/\mathfrak{m}$. By a theorem of Tate [33], the representation V is ramified at N. This proves the claim.

Equivalently: there is an inertia group I for N in $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ and a $\sigma \in I$ such that $\sigma R \neq R$. It follows that $\sigma R - R$ has order 2.

Consider the action of σ on $J_0(N)[2d]$. By Grothendieck's semistable reduction theorem (and the results of Deligne-Rapoport [11]), σ acts as the sum $1 + A$, where 1 represents the identity operator and A an endomorphism satisfying $A^2 = 0$. Using the binomial theorem, we find

$$\sigma^d(P) - P = (1 + dA)P - P = AdP = \sigma(R) - R.$$

Hence if $g = \sigma^d$, then g is an element of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ such that $gP - P$ has order 2. As we have seen in the proof of Proposition 1.2, it follows that P lies in $\mathcal{S}_0$. ∎

3. Ramified torsion points revisited

As we indicated above, this article concludes with a list of errata to [4]. In particular, we point out that the proofs of cases (ii) and (iii) of [4, Theorem 20] are incorrect. These cases concern the primes $p = 2$ and $p = 3$. Although those statements are not needed for the main theorem of [4], we hope that appropriately modified versions of them may be quite useful. Accordingly, we provide in this section some results for the primes $p = 2$ and $p = 3$. In addition, we will complete the proof of Theorem 1.3.

Fix a prime p, and let $\mathbf{C}_p$ be the completion of an algebraic closure of $\mathbf{Q}_p$. Let v be the valuation of $\mathbf{C}_p$ such that $v(p) = 1$. Let K^{ur} be the completion of the maximal unramified extension of $\mathbf{Q}_p$ and let K be a complete subfield of K^{ur}. Let R be the ring of integers of K and let k be the residue field of R. Also let R^{ur} be the ring of integers of K^{ur}, $\mathbf{F}$ the residue field of R^{ur} and σ the Frobenius automorphism of K^{ur}.

Let A be an Abelian scheme over R. Define a pairing

$$(\ , \ ) : \Omega^1_{A/R^{\mathrm{ur}}}(A) \times A(\mathbf{F}) \to K^{\mathrm{ur}}/pR^{\mathrm{ur}}$$

as follows: Given $\omega \in \Omega^1_{A/R^{\mathrm{ur}}}(A)$ and $P \in A(\mathbf{F})$, let $\tilde{P}$ be a lifting of P to $A(K^{\mathrm{ur}})$ and set

$$(\omega, P) = \int_0^{\tilde{P}} \omega \bmod pR^{\mathrm{ur}}.$$

It is easy to check that (ω, P) is independent of the choice of $\tilde{P}$: when $P = 0$, $\int_0^{\tilde{P}} \omega \in pR^{\mathrm{ur}}$. We note that $(\ , \ )$ is a Galois-invariant bilinear form and that (ω, P) is trivial when the order of P is prime to p.

Remark 3.1. We can relate $(\ , \ )$ to the Serre-Tate parameters when A is ordinary. Recall that there is a natural pairing

$$q\colon \operatorname{Ta}_p A(\mathbf{F}) \times \operatorname{Ta}_p \hat{A}(\mathbf{F}) \to 1 + pR.$$

(See Katz [17].) There is also a natural map $\operatorname{Ta}_p \hat{A}(\mathbf{F}) \to \Omega^1_{A/R^{\mathrm{ur}}}(A)$, $\alpha \mapsto \omega_\alpha$. Then one can show:

Proposition 3.2. *Suppose* $\alpha = (\alpha_n) \in \operatorname{Ta}_p \hat{A}(\mathbf{F})$ *and* $\beta = (\beta_n) \in \operatorname{Ta}_p A(\mathbf{F})$. *Then*

$$(\omega_\alpha, \beta_n) \equiv \frac{1}{p^n} \log q(\alpha, \beta) \bmod pR^{\mathrm{ur}}.$$

We say that a quadruple (H, W, F, V) is an F-T-crystal over R if H is free R module of finite rank, W is a direct summand of H and F and V are σ and σ^{-1}-linear endomorphisms of H, respectively, such that

$$FV = VF = p, \qquad VH = W + pH.$$

(This was called an F-crystal in [4].) If S is a smooth complete scheme of finite type over R, the first de Rham cohomology of S over R has a natural structure of an F-T-crystal where $H = H^1_{\mathrm{DR}}(S/R)$ and $W = H^0(S, \Omega^1)$ and we call a sub-F-T-crystal of this a *de Rham F-T-crystal* on S.

Suppose (H, W) is a de Rham F-T-crystal on A. Let P be a point of $A(\mathbf{F})$. For a coset B of pR^{ur} in $\mathbf{C}_p$ we set $v(B) = \min\{v(x)\colon x \in B\}$. Let

$$M_P(H) := 1 - \min\{v(\omega, P)\colon \omega \in W\}.$$

Let H be the first de Rham cohomology group of A over R thought of as an F-T crystal. Suppose $P \in A(\mathbf{F})$. We have in general,

$$M_{pP}(H) + 1 \geq M_P(H) \geq M_{pP}(H) \tag{1}$$

and if $M_P(H) \geq 1$

$$M_{pP}(H) + 1 = M_P(H). \tag{2}$$

It follows, from (1) and (2), that if $M_{pP}(H) \geq 1$

$$M_{pP}(H) + 1 = M_P(H). \tag{3}$$

Lemma 3.3. *Suppose $H = H^1_{\mathrm{DR}}(A, R)$. Let $P \in A(\mathbf{F})$. Then $M_P(H) = 0$ if and only if there is a torsion point of $A(K^{\mathrm{ur}})$ lying over P.*

Proof. If there is such a torsion point, $\overline{P}$, then

$$\int_O^{\overline{P}} \omega = 0,$$

for all $\omega \in W$. It follows that $v(\omega, P) = 1$ for all $\omega \in W$ and so $M_P(H) = 0$.

Now suppose $M_P(H) = 0$. Let $U(P)$ be the residue class above P. Let $\omega_1, \ldots, \omega_g$ be a basis for W over R. Let $\omega = (\omega_1, \ldots, \omega_g)$. Define a function on $U(P)$ into $\mathbf{C}_p^g$ by

$$F(X) = \int_0^X \omega,$$

for $X \in U(P)$. Now let $z_1, \ldots, z_g$ be a set of local parameters on $U(P)$ defined over R and let $Z = (z_1, \ldots, z_g)$ be the corresponding multivariable. We may use Z to identify $U(P)$ with $B(0,1)^g$. Having done this the R^{ur}-valued points of $U(P)$ become identified with $p(R^{\mathrm{ur}})^g$. Also we may now write F as a series in Z,

$$F(Z) = (\sum_I A_{1,I} Z^I, \ldots, \sum_I A_{g,I} Z^I),$$

where I runs over $\mathbf{N}^g$. Since $dF = \omega$, it follows that

$$G(Z) := (F(pZ) - F(0))/p \in R[[Z]].$$

Also since $\omega, \ldots, \omega_g$ is a basis for W, $G'(0)$ is an invertible matrix. Since $\mathbf{F}$ is algebraically closed, it follows that as a function from $(R^{\mathrm{ur}})^g$ to itself, G is surjective. Now $M_P(H) = 1 - \max\{1, v(F(0))\}$, so since $M_P(H) = 0$, $F(0) \in pR^g$. Thus, there exists a $z \in (R^{\mathrm{ur}})^g$ such that $G(z) = -F(0)/p$ and so there exists an $x \in U(P)(R^{\mathrm{ur}})$ such that $F(x) = 0$. It follows from [2, Theorem 2.11] that x is a torsion point. ∎

Corollary 3.4. *Suppose $P \in A(\mathbf{F})$ and $k \in \mathbf{Z}_{>0}$. Then $M_P(H) = k$ if and only if there exists a torsion point in $U(p^kP)(R^{\mathrm{ur}})$ but not in $U(p^{k-1}P)(R^{\mathrm{ur}})$.*

Proof. Suppose $M_P(H) = k$. Then it follows from (2) that $M_{p^{k-1}P}(H) = 1$ and $M_{p^kP}(H) = 0$ and so from the lemma there exists a torsion point in $U(p^kP)$ but not in $U(p^{k-1}P)$. Now assume there exists a torsion point in $U(p^kP)(R^{\mathrm{ur}})$ but not in $U(p^{k-1}P)(R^{\mathrm{ur}})$. Then it follows from the lemma that $M_{p^kP}(H) = 0$ and $M_{p^{k-1}P}(H) \neq 0$. It follows from (1) that $M_{p^{k-1}P}(H) = 1$. Now apply (3) repeatedly to deduce the corollary. ∎

Now suppose Y is a smooth complete curve over R and that (H, W) is a de Rham F-T-crystal on Y, which we may equally well think of as a de Rham F-T crystal on its Jacobian J. We will use a great deal of the notation of [4, §3].

We will say that H is *special* if it is either ordinary or superspecial in the language of [4]. In the ordinary case, as explained in [4] we have bijective σ^{-1} and σ-linear operators operators $\mathcal{C}$ and $\mathcal{C}^*$ on $\overline{W} := W/pW$ and $\overline{W}^* := \mathrm{Hom}(\overline{W}, k)$ satisfying

$$(\mathcal{C}w, v)^\sigma = (w, \mathcal{C}^* v)$$

for $w \in \overline{W}$ and $v \in \overline{W}^*$, where $(\ ,\ )$ is the natural pairing. (Caution: in [4, §3], the superscript "*" has a different meaning.) In the superspecial case, there are analogous operators, again called $\mathcal{C}$ and $\mathcal{C}^*$, with similar properties. In both cases, we obtain an operator on $\mathbf{P}(\overline{W})$ which we call $\mathbf{P}(\mathcal{C})$.

Let $O \in Y(K)$ and suppose (H, W) is a special de Rham F-T-crystal on Y. Let $q = p$ if H is ordinary and p^2 if H is superspecial. Let

$$\lambda_\nu(Q) = \int_O^Q \nu.$$

That H is special implies that for $P \in Y(\mathbf{F})$ there exists $g_\nu \in T\mathcal{O}_Y(U(P))$ such that

$$dg_\nu \equiv \nu \bmod T^{q-1}\Omega_Y(U(P)).$$

Here, T is a uniformizing parameter for $U(P)$. Also, $\overline{g}_\nu$ is the reduction of g_ν modulo p. Set

$$k_P(H) = \min\{q, \mathrm{ord}_P\, \overline{g}_\nu \colon \nu \in W\}.$$

We note that $k_P(H) \leq 1 + \min\{\mathrm{ord}_P\, \bar{\nu} \colon \nu \in W\}$ if the minimum is strictly less than q, with equality if it is strictly less than p. The following two propositions refine Proposition 15 of [4].

Proposition 3.5. *Suppose H is special. Let $P \in Y(\mathbf{F})$, $U = U(P)$ and T be a uniformizing parameter on U over K^{ur}. Assume $k_P(H) < q$. Suppose $b \in U(\mathbf{C}_p)$ is a common zero of $\Lambda = \{\lambda_\nu \,|\, \nu \in W\}$. Let $k = k_P(H)$ and $M = M_P(H)$ and $v = v(T(b))$. Then one of the following holds:*

(i) $M = 0$, $v = \infty$ or r/s where r and s are positive integers and $s \leq k$ or
(ii) $M > 0$, $v = 1/kq^M$ or
(iii) $v = 1/(kq^n(q-1))$ for some integer n such that $q^n(q-1) > q^M$.

For S a uniformizing parameter on U and let h_S be the element of $\overline{W}^*$

$$\omega \to \frac{\omega}{dS}(P)$$

and let $j(P)$ be the image of h_S in $\mathbf{P}(\overline{W})$. (This is independent of the choice of S.) If $M > 0$, we also define $e(P)$ to be the image in $\mathbf{P}(W)$ of the element $d(P)$ in W^* which is given by $\omega \mapsto p^{M-1}(\omega, P)$.

Proposition 3.6. *In addition to the hypotheses of the last proposition suppose $k_P(H) = 1$ (i.e., that P is not a base point of W). Then we have:*

In case (i), $b \in U(K^{\mathrm{ur}})$.

In case (ii), every differential in W which vanishes at P vanishes at least $q-2$ times. Moreover, if $q \geq 3$,*

$$\mathbf{P}(\mathcal{C})(j(P)) = j(P) = e(P). \tag{$*$}$$

If $q = 2$, choose a 2^Mth root of 2, let r be the image of $T(b)/2^{2^{-M}}$ in the residue field of $K(b)$ and let $h_b = rh_T \in \overline{W}^*$. Then

$$\mathcal{C}^{*M+1}(h_b) + \mathcal{C}^{*M}(h_b) = d(P).$$

In case (iii), every differential in W which vanishes at P vanishes at least $q-2$ times if $n = M$ and $q-1$ times if $n > M$; further,

$$\mathbf{P}(\mathcal{C})(j(P)) = j(P).$$

We note that the element h_b defined above is independent of choices.

Proof of Propositions 3.5 and 3.6. The main ingredient of the proof of these propositions, as discussed in the proof of Proposition 15 of [4], is the fact that for each $\omega \in W$ there exists $f_{\omega,m}(T) \in TR^{\mathrm{ur}}[[T]]$ such that

$$df_{\omega,m} \equiv \mathcal{C}^m\omega \bmod (p, T^q dT/T), \tag{4}$$

and for $x \in U$,

$$\lambda_\omega(x) = c_\omega + f_{\omega,0}(T(x)) + \frac{f^\sigma_{\omega,1}(T(x)^q)}{p} + \cdots + \frac{f^{\sigma^m}_{\omega,m}(T(x)^{q^m})}{p^m} + \cdots, \tag{5}$$

where $c_\omega = \lambda_\omega(T^{-1}(0))$. Call the series on the right $L_\omega(T(x))$. What we do is consider the lower convex hull of the Newton polygons of the series $L_\omega(T)$ for $\omega \in W$. This is the lower convex hull of the set of points

$$S \cup \{(kq^i, -i)\}_{i \geq 0},$$

where S is $\{(0, 1-M)\}$ if $M > 0$ and if $M = 0$ is some set of points of the form (x, y) with x-coordinate a non-negative integer at most $k-1$ and y-coordinate an integer at least 1. From this and Lemma 14 of [4], Proposition 3.5 follows.

Since, the proof of parts (i) and (iii) of Proposition 3.6 is contained in that of Proposition 15 of [4] and in that proposition the same assertion as the first sentence in (ii) was claimed, but not proved, with $q-2$ replaced by $q-1$ and the first equation of $(*)$ as well as the statement for $q = 2$ are new, we give the proof of part (ii) now.

Assume $M > 0$, $k = 1$.

---

* *In fact, using the results proven below, Matt Baker has shown that when $q \geq 3$ this case can only occur if* $\dim W = 1$.

First suppose $q \geq 3$. Let $a = T(b)$. Then the assertion $\lambda_\omega(b) = 0$ implies

$$c_\omega + \frac{f_{\omega,M-1}^{\sigma^{M-1}}(a^{q^{M-1}})}{p^{M-1}} + \frac{\big(f'_{\omega,M}(0)\big)^{\sigma^M} a^{q^M}}{p^M} \equiv 0 \bmod p^{2-M}. \qquad (**)$$

As

$$f'_{\omega,M}(0) \equiv \big(\mathcal{C}^M \bar{\omega}/dT\big)|_P \bmod p,$$

we obtain $\mathbf{P}(\mathcal{C})^M(j(P)) = e(P)$ immediately. Hence, to prove $(*)$, we only have to establish the first equality. It also follows from $(**)$ that $\mathcal{C}^M\bar{\omega}$ vanishes at P implies c_ω is congruent to 0 modulo $a^{q^{M-1}}p^{1-M}$ and hence modulo p^{2-M} as $c_\omega \in K^{\mathrm{ur}}$. Hence

$$f_{\omega,M-1}(a^{q^{M-1}}) \equiv 0 \bmod p,$$

which together with (4) implies $\mathcal{C}^{M-1}\bar{\omega}$ vanishes $q-2$ times at P as $v(a^{q^{M-1}}) = 1/q$. In particular, using the facts that $\mathcal{C}$ is bijective on $\bar{W}$ and is σ^{-1} linear we see that the hyperplane of differentials which vanish at P is stable under $\mathcal{C}$ which is equivalent to the first equation of $(*)$. The fact that ω vanishes $q-2$ times at P follows from the above with ω replaced by an element $\nu \in W$ such that $\mathcal{C}^{1-M}\bar{\omega} = \bar{\nu}$ as we now know such a ν vanishes at P.

Suppose now $q = 2$. Then we see from (5) that, in the residue field of $K(b)$,

$$2^{M-1}c_\omega + \Big(r\big(\frac{d}{dT}f_{\omega,M}\big)(0)\Big)^{\sigma^M} + \Big(r\big(\frac{d}{dT}f_{\omega,M+1}\big)(0)\Big)^{\sigma^{M+1}} = 0.$$

The assertion now follows from (4) and the definitions.

■

If $Q \in Y(\mathbf{C}_p)$ and T is a uniformizing parameter defined over K^{ur} on the residue disk containing Q, let $v(Q) = v(T(Q) + pR^{\mathrm{ur}}) = \min\{1, v(T(Q))\}$. This is independent of the choice of T.

Corollary 3.7. *Suppose that we are in the situation of Proposition 3.6. In cases (i) or (ii), Λ has exactly q^M common zeroes c such that $v(c) = q^{-M}$ unless $q = 2$, in which case it has either 2^M or 2^{M+1} zeroes; in the latter case, $\mathbf{P}(\mathcal{C})(j(P)) = j(P)$. In case (iii), Λ has exactly $q^n(q-1)$ common zeroes c such that $v(c) = (q^n(q-1))^{-1}$.*

Proof. Lemma 10 of [4] together with the proofs of Proposition 15 of [4] when $q \geq 3$ and 3.6 when $q = 2$, we see, that Λ has at most the numbers of common zeroes claimed. That it has at least this number follows from Galois theory. The statement about $j(P)$ when $q = 2$ follows by an examination of the proof of Proposition 3.6.

■

The following proposition summarizes most of what we know about $p = 2$ and 3 in the ordinary case.

Proposition 3.8. *Suppose Y is embedded in its Jacobian J so that O is the origin. Suppose Q is a ramified torsion point on Y and $\bar{Y}$ is ordinary. Then p equals 2 or 3. Moreover:*

(i) Suppose $p = 2$. Then $\bar{Q}$ either does not lift to an unramified torsion point of J or $\bar{Y}$ is hyperelliptic and $\bar{Q}$ is a hyperelliptic branch point.

(ii) Suppose $p = 3$. Then: (a) $\mathbf{P}(\mathcal{C})(j(\bar{Q})) = j(\bar{Q})$. (b) If $3|(1/v(Q))$, $\bar{Q}$ does not lift to an unramified torsion point on J. (c) If $\bar{Y}$ is hyperelliptic, then $g(Y) = 2$. Moreover, in this case, if $y^2 = f(x)$ is an equation for Y, where $f(x)$ is a polynomial of degree 6 in $R[x]$ such that $(\overline{f}(x), \overline{f'}(x)) = 1$ and $\overline{f'}(x)$ has degree 4, then

$$\overline{f'(Q)} = 0.$$

(d) If $g(Y) = 2$ and $v(Q) = 1/2$, then $\bar{Q}$ lifts to an unramified torsion point on J. Moreover, there are an even number, at most 16, such torsion points on Y.

Note that, by Corollary 3.7, in situation (ii) of the Proposition, $v(Q)$ is either of the form $1/3^n$, $n > 0$ or of the form $1/(2 \cdot 3^n)$, $n \geq 0$.

Proof. Suppose $p = 2$. Then, if $M_{\bar{Q}}(H) > 0$, $\bar{Q}$ does not lift to an unramified torsion point by Lemma 3.3. Suppose $M_{\bar{Q}}(H) = 0$. Then we must be in case (iii), so $\mathbf{P}(\mathcal{C})(j(\bar{Q})) = j(\bar{Q})$ and we can apply the argument in the proof of Theorem 5.5 of [2] for $p = 2$.

Now suppose $p = 3$. Then (a) is contained in Proposition 3.6. If $v(Q) = 1/3^n$, then we are in case (ii) of this proposition and (b) follows from Lemma 3.6. Now suppose $v(Q) = 1/2 \cdot 3^n$ and $n > 0$. Then it follows from this Proposition that every differential which vanishes at $\bar{Q}$ must vanish at least 2 times. Thus, $\bar{Y}$ is hyperelliptic and $\bar{Q}$ is a hyperelliptic branch point. By the argument in the proof of Theorem 5.5 of [2], this is impossible, so also in this case we may conclude that $\bar{Q}$ does not lift to an unamified torsion point. Now (c) follows from (a) and the proof of Theorem 5.5 of [2]. Finally, if $v(Q) = 1/2$, then $M_{\bar{Q}}(H) = 0$, so $\bar{Q}$ does lift to an unramified torsion point on J. By (c), $\bar{Q}$ is a zero of a function on $\bar{Y}$ of degree 8 and by Corollary 3.7 there are 0 or 2 such Q's in any residue class. ■

Note. Theorem 19 of [4] has the appealing corollary:

Proposition 3.9. *Let C be a smooth curve of genus $g > 1$ with good reduction, embedded in its Jacobian J over R. If $p > 2g$ and P is a non-trivial torsion point in the kernel of reduction of $J(\mathbf{C}_p)$, then*

$$C(\mathbf{C}_p) \cap (P + J(K)) = \emptyset.$$

This is, in fact, equivalent to the theorem when the crystalline cohomology of C has no unit root part.

Now fix p and let

$$H_1 = \bigcap_{n \geq 0} T_p^n H^1_{\mathrm{DR}}(X_0(N), \mathbf{Z}_p), \quad H_2 = \{\, h \in H^1_{\mathrm{DR}}(X_0(N), \mathbf{Z}_p) \mid \lim_{n \to \infty} T_p^n h = 0 \,\}.$$

Set

$$W_1 = H_1 \cap H^0(X_0(N), \Omega^1_{X_0(N)/\mathbf{Z}_p}), \qquad W_2 = H_2 \cap H^0(X_0(N), \Omega^1_{X_0(N)/\mathbf{Z}_p}).$$

If I is an ideal of $\mathbf{T}$, we let $\mathbf{T}_I$ denote the completion of $\mathbf{T}$ at I. We write $\mathbf{T}_p$ for $\mathbf{T}_{(p)}$.

Proposition 3.10. *Assume that $p \neq N$. Then the pairs $H_1 := (H_1, W_1)$ and $H_2 := (H_2, W_2)$ are de Rham F-T-crystals, H_1 is ordinary and*

$$H_1 + H_2 = H^1_{\mathrm{DR}}(X_0(N), \mathbf{Z}_p)$$
$$W_1 + W_2 = H^0(X_0(N), \Omega^1_{X_0(N)/\mathbf{Z}_p}).$$

Further, suppose that $\mathbf{T}$ is unramified at p, or more generally that T_p is divisible by p in $\mathbf{T}_\mathfrak{m}$ for each maximal ideal $\mathfrak{m}$ of $\mathbf{T}$ such that $\mathfrak{m}|p$ and $T_p \in \mathfrak{m}$. Then H_2 is superspecial.

Proof. Let V and F be the Verschiebung and Frobenius endomorphisms acting on $H^1_{\mathrm{DR}}(X_0(N), \mathbf{Z}_p)$. Since these endomorphisms commute with T_p, it follows immediately that (H_i, W_i) is a sub-F-T-crystal. Since $T_p = V + F$ we see that H_1 is ordinary. Because $\mathbf{T}_p$ is Gorenstein, we have an isomorphism

$$W_2 \approx \oplus \mathbf{T}_\mathfrak{m}$$

of $\mathbf{T}_p$-modules in which the sum runs over those maximal ideals $\mathfrak{m}$ of $\mathbf{T}$ which lie over p and contain T_p. Since $FW_2 \equiv 0 \bmod p$, it follows from the hypotheses of the proposition that $VW_2 \equiv 0 \bmod p$. The fact that T_p is self-adjoint and W_2 is self-orthogonal with respect to the cup product implies that $h := \operatorname{rk} H_2 = 2 \operatorname{rk} W_2$. We also know $VH_2 = W_2 + pH_2$. Let $\bar{V}$ and $\bar{F}$ be the reductions of V and F mod p, $\operatorname{rk} \bar{V} = h/2$. Thus the sequence

$$0 \to W_2/pW_2 \to H_2/pH_2 \xrightarrow{\bar{V}} W_2/pW_2 \to 0$$

is exact. Together with the equation $VF = p$, this implies that $FH_2 \subseteq W_2 + pH_2$ and $\operatorname{rk} \bar{F} = h - \operatorname{rk} \bar{V} = h/2$. We conclude that $FH_2 = W_2 + pH_2$, i.e., that H_2 is superspecial. ∎

Remarks. (i) It is easy to see that H_2 is not superspecial if $\mathbf{T}$ does not satisfy the hypothesis of the proposition which concerns local divisibilities of T_p by p. (ii) This hypothesis fails to be satisfied in the particular case $N = 37$, $p = 2$. In this case T_2 lies in the unique maximal ideal $\mathfrak{m}$ of $\mathbf{T}$ which divides 2, but T_2 does not lie in $2\mathbf{T}_\mathfrak{m}$.

Lemma 3.11. *Suppose that ω is an element of W_2 and that P lies in $J_0(N)(\mathbf{F})$. Then we have $(\omega, P) = 0$. In particular, $M_P(H_2) = 0$.*

Proof. This follows from the identity

$$(\omega, T_p Q) = (T_p \omega, Q),$$

for $\omega \in \Omega^1_{J_0(N)/R^{ur}}(J_0(N))$ and $Q \in J_0(N)(\mathbf{F})$, which is evident from the definitions and the fact that the T_p acts bijectively on the p-power torsion points of $J_0(N)(\mathbf{F})$. ∎

Proposition 3.12. *Suppose $p \geq 5$, $p \neq N$, H_2 is superspecial and $Q \in \mathcal{S}$. Then the extension $\mathbf{Q}(Q)$ of $\mathbf{Q}$ is unramified above p.*

Proof. We may work locally at p. Let P be an element of $X_0(N)(\mathbf{F})$ and let T be a uniformizing parameter on $U(P)$ defined over R^{ur}. Let $H_i^{\mathrm{ur}} = H_i \otimes R^{\mathrm{ur}}$. Suppose

$Q \in U(P)$ and Q is ramified. For $k \in \{1,2\}$, let $M_k = M_P(H_k^{\mathrm{ur}})$ and $q_k = p^k$. Note that $M_k = 0$ for $k = 2$ by the Lemma above. Then since P is not a base point for $H^0(X_0(N), \Omega^1_{X_0(N)/\mathbf{F}})$, it is not a base point for $W_j \otimes \mathbf{F}$ for some $j \in \{1,2\}$. Suppose $\{1,2\} = \{i,j\}$. Then $k_P(H_j^{\mathrm{ur}}) = 1$, and Proposition 3.6, Proposition 3.5 and the Lemma above imply that either (a) $j = 1$, $M_1 > 0$, $v(Q) = 1/p^{M_1}$ and every differential in $W_1 \otimes \mathbf{F}$ which vanishes at P vanishes $p-2$ times or (b) $v(Q) = 1/q_j^n(q_j - 1)$ where $n \geq M_j$ and all differentials in $W_j \otimes \mathbf{F}$ which vanish at P vanish at least $q_j - 2$ times (or $q_j - 1$ times if $n > M_j$). If $k_P(H_i^{\mathrm{ur}}) \geq p$, every differential in $W_i \otimes \mathbf{F}$ vanishes at least $p-1$ times at P. If $1 \leq k_P(H_i^{\mathrm{ur}}) < p$ then Proposition 3.5 applies, but none of its conclusions are consistent with what we have concluded above. Thus every differential in $W_i \otimes \mathbf{F}$ vanishes at least $p-1$ times at P.

Thus every differential in $H^0(X_0(N), \Omega^1_{X_0(N)/\mathbf{F}})$ which vanishes at P vanishes at least $p-2$ times. This is impossible for $p \geq 5$ since $g > 1$. ∎

In view of Theorem 2.2, Proposition 3.12 completes the proof of Theorem 1.3 for primes p which are different from N. To prove Theorem 1.3, we need only prove that $P_N \notin C$ implies $P - P_N \notin C$, when $\mathbf{T}$ is unramified at N. This question will be addressed below.

The proof of Proposition 3.12 yields:

Corollary 3.13. *Suppose $p = 2$ or 3 and $\mathbf{Q}(Q)$ is ramified at some prime $\mathfrak{p}$ above p. Suppose that $\{1,2\} = \{i,j\}$ and the reduction P of Q modulo $\mathfrak{p}$ is not a base point for W_j. Then P is a base point for W_i. Moreover, if $p = 3$ every non-zero differential in W_i must vanish at least two times at P and if at a prime $\mathfrak{p}$ above 3 $j = 2$ or $v(Q) < \left(p^{M_1}(p-1)\right)^{-1}$ and $j = 1$ then $X_0(N) \bmod 3$ is hyperelliptic and P is a hyperelliptic branch point.*

We next prove:

Proposition 3.14. *Suppose $Q \in \mathcal{S}$ and N divides the order of Q. Then for all embeddings $\overline{\mathbf{Q}}$ into $\overline{\mathbf{Q}}_N$, the image of Q in $X_0(N)(\overline{\mathbf{Q}}_N)$ reduces to a singular point of the reduction of the Deligne-Rapoport model* [11] *of $X_0(N)$ over $\mathbf{Q}_N$.*

Proof. Let $\mathcal{N}$ be the Néron model of $J_0(N)$ and let $\mathcal{X}$ be the complement of the singular locus in the minimal regular model of $X_0(N)$. The Néron property of $\mathcal{N}$ implies that the map from $X_0(N)$ to $J_0(N)$ extends to a map from $\mathcal{X}$ to $\mathcal{N}$. The reduction of $\mathcal{X}$ differs from the non-singular locus of the reduction of Deligne-Rapoport model only by at most three components, which correspond to supersingular elliptic curves with complex multiplication by the fourth or third roots of unity. (See [21, Appendix, §1].)

Let M be the $\mathbf{Z}_N$-submodule of $H^0(X_0(N), \Omega^1_{X_0(N)/\mathbf{Q}_N})$ consisting of differentials which correspond to weight-two cusp forms with integral q-expansions at the two cusps of $X_0(N)$. Let D be the special fiber of the Deligne-Rapoport model of $X_0(N)$ over $\mathbf{Z}_N$, and let $X^\times$ represent the irreducible component of D which contains the cusp C_∞, endowed with log-structure at the supersingular points. (See [16].) Let W_∞ and W_0 be the wide opens in $X_0(N)$ whose points reduce to the irreducible components of D containing C_∞ and C_0. (See [5].) Then the natural map from M into $H^1_{\mathrm{DR}}(W_\infty, \mathbf{Q}_N)$ is an injection. Its image is $H := H^1_{\mathrm{cris}}(X^\times, \mathbf{Z}_N)$. (See [7, §3].) Indeed, let $\mathcal{Y}_\infty$ and $\mathcal{Y}_0$ be the connected components of C_∞ and C_0 in the formal completion of $\mathcal{X}$ along its reduction. Then $\mathcal{Y}_\infty \otimes \mathbf{Q}_N$ may be identified with the underlying affinoid (ibid.) of W_∞, $W_\infty \setminus W_0$, and the natural map of

$\mathcal{Y}_\infty$ into the formal completion of $\mathcal{N}$ along its reduction takes $\mathcal{Y}_\infty$ into the connected component of the origin, $\mathcal{N}^0$. Further, the map $\bar{\mathcal{Y}}_\infty \to \bar{\mathcal{N}}^0$ is an Albanese morphism into the generalized Jacobian of X relative to the modulus SS of supersingular points ($\bar{\mathcal{Y}}_\infty$ may naturally be identified with $X - \mathrm{SS}$). (See also [13, §8] and Theorem 3.1 and Corollary A2.3 of [7].) Now H has natural endomorphisms F and V so that if $W = H$, the quadruple (H, W, F, V) is an ordinary F-T-crystal. It follows by a direct translation of the proof of Theorem 20(i) of [4] as $g = \mathrm{rk}_{\mathbf{Z}_N}(W)$ that as soon as $g > 1$, $\sigma(\mathcal{S}) \cap \mathcal{Y}_\infty(\mathbf{C}_N) \subset \mathcal{Y}_\infty(\mathbf{Q}_N^{\mathrm{ur}})$ for any embedding σ of $\bar{\mathbf{Q}}$ into $\bar{\mathbf{Q}}_N$. Exploiting the Atkin-Lehner involution, we see similarly that if $g > 1$, $\sigma(\mathcal{S}) \cap \mathcal{Y}_0(\mathbf{C}_N) \subset \mathcal{Y}_0(\mathbf{Q}_N^{\mathrm{ur}})$ for any embedding σ of $\bar{\mathbf{Q}}$ into $\bar{\mathbf{Q}}_N$.

The proposition follows since every torsion point of order N is ramified at all primes above N in view of Theorem 2.2 and the fact that the order of cuspidal group is prime to N. ∎

Our aim now is to prove the following result, which will complete the proof of Theorem 1.3:

Theorem 3.15. *Suppose N does not divide the discriminant of the Hecke algebra $\mathbf{T}$. Let P be an element of $\mathcal{S}$, written as usual as the sum $\sum P_p$. Assume that $P_p \in C$ for all $p \neq N$. Then $P_N = 0$.*

Our proof of Theorem 3.15 exploits a recent unpublished theorem of B. Edixhoven which concerns the special fibre $\overline{\mathcal{N}}$ of $\mathcal{N}$. In its statement, the horizontal bar denotes the reduction map to characteristic N and the points 0 and ∞ are the cusps C_0 and C_∞:

Theorem 3.16. *Let $\overline{C}$ be the image of C in $\overline{\mathcal{N}}$. Then $\overline{C} \cap \overline{\mathcal{X}} = \{\overline{0}, \overline{\infty}\}$.*

We recall also a simple result from [29] which concerns the action of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ on the ℓ-power torsion points of $J = J_0(N)$, i.e., the ℓ-adic representation of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ attached to J. This result has been proved only under the hypothesis that ℓ is different from 2 and 3 and is prime to the discriminant of $\mathbf{T}$. We apply it in the case $\ell = N$, which explains the presence of the discriminant hypothesis in the statement of Theorem 3.15. When the hypothesis is satisfied, $\mathbf{T}_N = \mathbf{T} \otimes \mathbf{Z}_N$ is the product of discrete valuation rings; thus, Mazur's theorem [21, Ch. II, §14–§15] to the effect that the N-adic Tate module $\mathrm{Ta}_N(J)$ of J is free of rank 2 over $\mathbf{T}_N$ is especially easy to prove. Choosing a basis for $\mathrm{Ta}_N(J)$ over $\mathbf{T}_N$, we view the N-adic representation of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ defined by J as a continuous homomorphism

$$\rho_N \colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{GL}(2, \mathbf{T}_N).$$

We obtain from [29]:

Proposition 3.17. *Suppose that N is prime to the discriminant of $\mathbf{T}$. Then the image of ρ_N contains the group $\mathbf{SL}(2, \mathbf{T}_N)$.*

Here is our proof of Theorem 3.15:

Proof. Using Proposition 3.17, one shows that there is a $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ such that $\sigma(P_N)$ lies in the kernel of the reduction map to characteristic N. Replacement of P by $\sigma(P)$ preserves the hypothesis that $P_p \in C$ for all $p \neq N$ and does not affect the question of whether P_N is non-zero. We may thus assume that P and $P - P_N$ have the same image in characteristic N. It follows that P is a point on $\mathcal{N}^{\mathrm{rig}}$,

the generic fiber of the formal completion of $\mathcal{N}$ along its reduction. The connected components of this rigid space are in one-to-one correspondence with the connected components of the reduction of the Néron model, which in turn are in one-to-one correspondence, via reduction, with the elements of C. Thus the reduction of P is a point in $\overline{C} \cap \overline{\mathcal{X}}$. Now it will be shown in [10] that the intersection of $\mathcal{N}^{\mathrm{rig}}$ with $X_0(N)$ is the rigid space associated to the formal completion of the minimal model of this curve along its reduction (this is a general phenomenon that occurs when the reduction of the minimal model is semistable and every edge in its graph is contained in a cycle). Thus it follows from Edixhoven's theorem that $P - P_N$ is either 0 or ∞. But now Proposition 3.14 implies that $P_N = 0$. ■

4. Lang's Approach

We proceed in the spirit of Lang [18]:

Lemma 4.1. *Suppose X is a curve of genus $g > 1$ embedded in its Jacobian and n an integer such that $|n| > 1$. Then $\#(nX \cap X) \leq gn^2$.*

Proof. Let $W_n = X + X + \cdots + X$, where the sum is over $|n|$ copies of X. If $a \in W_{g-2}$, then $X \subseteq W_{g-1} - a$. It follows from Lemma 5.4 of [2] that there exists an $a \in W_{g-2}$ such that $(W_{g-1} - a) \cap nX$ is finite. (Note that condition (ii) in the proof of this lemma should be replaced by the condition: D is not special.) Hence

$$\#(X \cap nX) \leq \deg(W_{g-1} \cdot nX),$$

where $(\ \cdot\ )$ is the intersection pairing. By Theorem 5 of [19, Ch. 4, §3],

$$\deg(W_{g-1} \cdot n(X)) = \deg\left(n^{-1}(W_{g-1}) \cdot X\right).$$

We see from the discussion following Proposition 4 of §3 that $n^{-1}(W_{g-1})$ is numerically equivalent to $n^2 \cdot W_{g-1}$. The result now follows from the fact that $\deg(W_{g-1} \cdot X) = g$. (Proof: We actually compute $W_{g-1} \cdot -X$. Suppose the divisor $Q_1 + \cdots + Q_g$ is not special. Let A be the point on J equal to $\sum Q_i$. Then if $P \in X$ and $-P$ lies in $W_{g-1} - A$, we see that $P = Q_i$ for some i.) ■

Proposition 4.2. *Suppose X and the embedding into its Jacobian are defined over $\mathbf{Q}$ and there exists a $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ which acts on $J[M](\overline{\mathbf{Q}})$ via the homothety n, where n is an integer satisfying $|n| > 1$. Then*

$$\#\left(X(\overline{\mathbf{Q}}) \cap J[M](\overline{\mathbf{Q}})\right) \leq gn^2.$$

Proof. The proposition follows immediately from the lemma, since the indicated intersection lies both in X and nX. ■

Proposition 4.2 and the results of [2] can be combined to deduce consequences in other contexts. For example, let p be a prime, and for each triple of integers (a, b, c) with abc prime to p, let

$$F^p_{a,b,c} : y^p = (-1)^c x^a (1 - x)^b$$

denote the indicated quotient of the degree-p Fermat curve $F^p : X^p + Y^p + Z^p = 0$. (See, e.g., [8, §3] for background on Fermat quotients.) The cusps on F^p are the

images of points on the Fermat curve for which one of the projective coordinates X, Y, Z is 0; the cusps on $F^p_{a,b,c}$ are the points where the coordinate z is 0, 1 or ∞. According to well-known results of Rohrlich [30], the cusps of F^p lie in a common torsion packet; i.e., their differences form degree-zero divisors whose images on the Jacobian of F_p are torsion. The corresponding statement then holds for the quotients $F^p_{a,b,c}$. One can ask whether the cusps form a complete torsion packet on Fermat curves F^p and $F^p_{a,b,c}$ of genus > 1. (This question is discussed in [3] and especially in [6].) For instance, let x_0 a cusp of $F^p_{a,b,c}$, and use it to embed $F^p_{a,b,c}$ in its Jacobian J. Does the cuspidal torsion packet $\mathcal{S} := F^p_{a,b,c} \cap J_{\rm tor}$ contain only the cusps?

To prove statements of this sort, it has proved helpful to show first that $\mathcal{S}$ has small cardinality. As an application of Proposition 4.2, we obtain:

Proposition 4.3. *Assume that $F^p_{a,b,c}$ is not hyperelliptic and that $p \geq 5$. Then the cuspidal torsion packet of $F^p_{a,b,c}$ has at most $(p-1)/2 \cdot (1+p)^2$ elements.*

Suppose now that p is a prime ≥ 5. Then Coleman, Tamagawa and Tzermias [9] have shown, using the proposition and results of Coleman [6] and Greenberg [12], that the cusps on F^p form a complete torsion packet.

5. Galois action on torsion points of $J_0(37)$

We next present some results of [15] about the action of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ on the group of torsion points of $J_0(37)$.

The space of weight-two cusp forms on $\Gamma_0(37)$ is two dimensional; it is spanned by the eigenforms with integral coefficients which arise from the two isogeny classes of rational elliptic curves with conductor 37. The action of the Hecke ring $\mathbf{T}$ on these forms induces an inclusion $\mathbf{T} \subseteq \mathbf{Z} \times \mathbf{Z}$. It is well known that the image of $\mathbf{T}$ in $\mathbf{Z} \times \mathbf{Z}$ is the order consisting of pairs of integers (a, b) which satisfy $a \equiv b \bmod 2$. Using the results of [21, Ch. II], one sees that the adelic Tate module

$$\mathrm{Ta_f}\, J := \varprojlim J[n]$$

of $J = J_0(37)$ is free of rank 2 over $\mathbf{T} \otimes \hat{\mathbf{Z}}$. Equivalently: for each prime p, the p-adic Tate module $\mathrm{Ta}_p\, J = \mathrm{Ta}_p\left(J(\overline{\mathbf{Q}})\right)$ is free of rank two over the ring $\mathbf{T}_p := \mathbf{T} \otimes \mathbf{Z}_p$.

The image G of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ in $\mathrm{Aut}\, J(\overline{\mathbf{Q}})_{\rm tors}$ is the image of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ in

$$\mathrm{Aut}_{\mathbf{T}\otimes\hat{\mathbf{Z}}}\, \mathrm{Ta_f} \approx \mathbf{GL}(2, \mathbf{T} \otimes \hat{\mathbf{Z}}).$$

Since the determinant of the representation $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{GL}(2, \mathbf{T}\otimes\hat{\mathbf{Z}})$ is the adelic cyclotomic character $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \hat{\mathbf{Z}}^*$, the image of this representation lies in the group

$$A := \{\, M \in \mathbf{GL}(2, \mathbf{T} \otimes \hat{\mathbf{Z}}) \mid \det M \in \hat{\mathbf{Z}}^* \,\}.$$

In other words, we have

$$G \subseteq A \subset \mathbf{GL}(2, \mathbf{T} \otimes \hat{\mathbf{Z}}).$$

For each prime p, let G_p and A_p be the images of G and A in the group $\mathbf{GL}(2, \mathbf{T}_p)$. One has $G \subseteq \prod_p G_p$. More generally, if S is a set of primes (possibly infinite), let G_S be the image of G in $\mathbf{GL}(2, \prod_{p\in S} \mathbf{T}_p)$, i.e., in the product $\prod_{p\in S} G_p$. Further,

let G^S be the image of G in $\prod_{p\notin S} G_p$, and make similar definitions with G replaced by A. For each S, one has trivially $A = A_S \times A^S$, but the analogous decomposition for G is by no means automatic. If $p_1, \dots, p_n$ are distinct primes, we sometimes write $G(p_1, \dots, p_n)$ in place of $G_{\{p_1,\dots,p_n\}}$ and make similar use of $A(p_1, \dots, p_n)$.

The main result of [15] is a description of G as a subgroup of A.

Proposition 5.1. *For all $p \geq 5$, one has*

$$G_p = A_p = \{\, M \in \mathbf{GL}(2, \mathbf{Z}_p \times \mathbf{Z}_p) \mid \det M \in \mathbf{Z}_p^* \,\}.$$

Further, let S be the set $\{2, 3, 37\}$. The natural inclusion $G \hookrightarrow G_S \times G^S$ is an isomorphism.

In the displayed equation, the second equality, which asserts that A_p is a $\mathbf{GL}(2)$, results from the circumstance that $2 = (\mathbf{Z} \times \mathbf{Z} \colon \mathbf{T})$ is prime to p. The first equality is not too difficult to establish, even in the more general case where 37 is replaced by an arbitrary prime number [29]. The equation $G = G_S \times G^S$ may be summarized by the statement that each group G_p with $p \neq 2, 3, 37$ is a subgroup of G. One can prove it by the methods of Serre [31, §6.2]. ∎

Proposition 5.1 reduces the determination of G to a determination of its quotient G_S, where $S = \{2, 3, 37\}$. On the other hand, it is the quotient G_S, as opposed to the full group G, which intervenes in our proof of Theorem 1.4. The group G_S is a subgroup of $G_2 \times G_3 \times G_{37}$ which turns out to have index 3 in the product $G_2 \times G_3 \times G_{37}$. In order to describe G_S, it is convenient to discuss first the individual factors G_2, G_3, and G_{37}. The last of the three factors has already been determined: it coincides with its overgroup A_{37}. (One can say that G_{37} is "as large as possible.") The following consequence of this fact will be useful below:

Corollary 5.2. *Let P be a torsion point on $J_0(37)$ whose order is divisible by 37. Then P has at least $37^2 - 1 = 1368$ conjugates.*

We next describe G_2. To do this, we shall introduce a certain homomorphism

$$\theta \colon A_2 \to \mathbf{F}_2.$$

View A_2 as the group

$$\{\, (\alpha, \beta) \in \mathbf{GL}(2, \mathbf{Z}_2) \times \mathbf{GL}(2, \mathbf{Z}_2) \mid \det(\alpha) = \det(\beta) \text{ and } \alpha \equiv \beta \bmod 2 \,\}.$$

Let $\mathfrak{sl}_2(\mathbf{F}_2)$ be the lie algebra of 2×2 matrices over $\mathbf{F}_2$ with trace 0. The adjoint action $(\alpha, \beta) : M \mapsto aMa^{-1}$, where $a = \alpha \bmod 2 = \beta \bmod 2$, makes $\mathfrak{sl}_2(\mathbf{F}_2)$ into an A_2-module. We regard $\mathbf{F}_2$ as an A_2-module with trivial action. One may verify explicitly that the map

$$\mathfrak{sl}_2(\mathbf{F}_2) \to \mathbf{F}_2, \qquad \begin{pmatrix} a & b \\ c & a \end{pmatrix} \longmapsto a + b + c$$

is a non-zero map of A_2-modules. Meanwhile, it is well known, and not hard to check by direct calculation, that the association

$$A_2 \to \mathfrak{sl}_2(\mathbf{F}_2), \qquad (\alpha, \beta) \mapsto \frac{\alpha\beta^{-1} - I}{2} \bmod 2$$

is a 1-cocycle on A_2 with values in $\mathfrak{sl}_2(\mathbf{F}_2)$. On composing this cocycle with the map $\mathfrak{sl}_2(\mathbf{F}_2) \to \mathbf{F}_2$ we have exhibited, we obtain the desired homomorphism θ.

For later use, we define a second non-trivial homomorphism

$$\epsilon\colon A_2 \to \mathbf{F}_2$$

as the composite of the surjection $A_2 \to \mathbf{GL}(2, \mathbf{F}_2)$ defined by $(\alpha, \beta) \mapsto \alpha \bmod 2$ and the unique non-zero homomorphism $\mathbf{GL}(2, \mathbf{F}_2) \to \mathbf{F}_2$. This latter map is the "sign" function $S_3 \to \{\pm 1\}$, viewed as taking values in the additive group $\mathbf{F}_2$. It is clear that ϵ is non-trivial on G_2, since G_2 maps onto $\mathbf{GL}(2, \mathbf{F}_2)$.

Proposition 5.3. *The group G_2 is the kernel of $\theta\colon A_2 \to \mathbf{F}_2$.*

For the proof of this Proposition, see [15]. In what follows, we we will present a concrete explanation for the inclusion $G_2 \subseteq \ker \theta$.

View G_2 as the Galois group of the extension K of $\mathbf{Q}$ gotten by adjoining all 2-power division points on the two strong modular elliptic curves of conductor 37. Call these curves E and E'; order them so that the discriminants of E and E' are $\Delta = 37$ and $\Delta' = 37^3$, respectively. The field K contains $\mathbf{Q}(\sqrt{\Delta}) = \mathbf{Q}(\sqrt{\Delta'})$: this field is the quadratic subfield of the S_3-extension of $\mathbf{Q}$ gotten by adjoining the 2-division points on E or E'. On the other hand, K contains $\mathbf{Q}(\sqrt{-1}, \sqrt[4]{\Delta})$ and $\mathbf{Q}(\sqrt{-1}, \sqrt[4]{\Delta'})$: these are subfields of the field of 4-division points of $E \times E'$. In particular, K contains the biquadratic field $\mathbf{Q}(\sqrt{-1}, \sqrt[4]{\Delta'/\Delta})$. Here we note that Δ'/Δ is a perfect square because of the isomorphism $E[2] \approx E'[2]$, so that $\sqrt[4]{\Delta'/\Delta}$ is either rational or a quadratic irrationality. Thus the subfield $\mathbf{Q}(\sqrt{-1}, \sqrt[4]{\Delta'/\Delta}, \sqrt{\Delta})$ of K is a $(2, \ldots, 2)$-extension of $\mathbf{Q}$ whose degree over $\mathbf{Q}$ could a priori be as large as 8. In fact, however, the quantities $\sqrt[4]{\Delta'/\Delta}$ and $\sqrt{\Delta}$ are equal, so that the degree of this field over $\mathbf{Q}$ is at most 4.

Corollary 5.4. *Let P be a non-zero point on $J_0(37)$ of 2-power order. Then there is a $g \in G_2$ such that $\epsilon(g) = 0$ and such that $gP - P$ has order 2.*

This result may be deduced from the equality $G_2 = \ker \theta$ by straightforward calculation. Alternatively, we can proceed somewhat more intrinsically as in the proof of Theorem 2.4, considering the action of an inertia subgroup I of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ for the prime 37. Composing ϵ with the projection $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to G_2$, we will regard ϵ as a map $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{F}_2$. We must find a $g \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ in the kernel of ϵ with the property that $gP - P$ has order two.

Suppose first that P itself has order 2. Then it suffices to find a g in the kernel of ϵ which does not fix P. For this, it is helpful to recall the structure of $J_0(37)[2]$ as a $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-module. Let $J = J_0(37)$ and let $\mathfrak{m}$ be the unique maximal ideal of $\mathbf{T}$ with residue characteristic 2. The kernel $J[\mathfrak{m}]$ is isomorphic to $E[2]$ (and also to $E'[2]$), and the quotient $J[2]/J[\mathfrak{m}]$ is again isomorphic to $J[\mathfrak{m}]$ (cf. [21, p. 112]). The group $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ acts on $E[2]$ via its quotient $\mathbf{GL}(2, \mathbf{F}_2)$, which is the symmetric group on three letters. The image in $\mathrm{Aut}\, E[2]$ of the kernel of ϵ is the alternating group on three letters, which permutes transitively the three non-zero elements of $E[2]$. An element g in the kernel of ϵ which maps non-trivially to this alternating group can fix no non-zero element of $J[2]$. Indeed, such elements g fix no non-zero elements of the quotient $E[2]$ and no non-zero elements of the submodule $E[2]$.

Suppose now that P has order 2^n, with $n \geq 2$. Then $Q = 2^{n-1}P$ is a point of $J_0(37)$ of order 2. As we have noted, the action of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ on $E[2]$ cuts

out an S_3-extension of $\mathbf{Q}$. This extension is ramified at 37; indeed, it contains the quadratic field $\mathbf{Q}(\sqrt{37})$. For each non-zero R in $E[2]$, we may find an inertia subgroup $I \subset \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ for the prime 37 and a $\sigma \in I$ such that $\sigma R \neq R$. (Indeed, the image of each I in S_3 has order 2; some conjugate of this element will move R.) Using again that $J[2]$ is an extension of $E[2]$ by $E[2]$, we may find an inertia group I for 37 and a $\sigma \in I$ such that $\sigma Q \neq Q$. Now consider the action of σ on $J_0(37)[2^n]$. As in the proof of Theorem 2.4, σ acts as the sum $1 + A$, where 1 represents the identity operator and A an endomorphism satisfying $A^2 = 0$. Since

$$\sigma Q = Q + A\, 2^{n-1} P,$$

the quantity $2^{n-1}AP$ has order 2. Also

$$\sigma^{2^{n-1}} P = (1 + A)^{2^{n-1}} P = P + 2^{n-1} AP$$

by the binomial theorem. It thus suffices to take $g = \sigma^{2^{n-1}}$: this element is automatically in the kernel of ϵ because it is the square of an element of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. ■

We now describe

$$G_3 = \mathrm{Gal}\,(\mathbf{Q}(E[3^\infty], E'[3^\infty])/\mathbf{Q}) \hookrightarrow \mathrm{Aut}(\mathrm{Ta}_3\, E) \times \mathrm{Aut}(\mathrm{Ta}_3\, E').$$

As noted by Serre [31, 5.5.8], G_3 maps onto the first factor $\mathrm{Aut}(\mathrm{Ta}_3\, E)$. Let X be the image of G_3 in the second factor $\mathrm{Aut}(\mathrm{Ta}_3\, E') \approx \mathbf{GL}(2, \mathbf{Z}_3)$. Since $E'[3]$ may be regarded as $J_0(37)[\mathfrak{m}]$, where $\mathfrak{m}$ is the unique Eisenstein prime of $\mathbf{T}$, the module $E'[3]$ is isomorphic to the direct sum $\mu_3 \oplus \mathbf{Z}/3\mathbf{Z}$. In particular, the image of X mod 3 has order 2. Let $\overline{X}$ be the image of X in $\mathbf{GL}(2, \mathbf{Z}/9\mathbf{Z})$, i.e., in $\mathrm{Aut}\, E[3^2]$. Then the order of $\overline{X}$ is a divisor of $2 \cdot 81$ which is divisible by 2. According to [15], $\overline{X}$ has order $54 = 2 \cdot 27$; thus, $\overline{X}$ is of index 3 in the inverse image in $\mathbf{GL}(2, \mathbf{Z}/9\mathbf{Z})$ of the image of $\overline{X}$ mod 3. On the other hand, X is the full inverse image of $\overline{X}$ in $\mathrm{Aut}(\mathrm{Ta}_3\, E') \approx \mathbf{GL}(2, \mathbf{Z}_3)$. Concretely, with respect to a suitable basis of $\mathrm{Ta}_3\, E'$ one has:

$$X = \left\{ \begin{pmatrix} 1+3e & 3f \\ 3g & h \end{pmatrix} \in \mathbf{GL}(2, \mathbf{Z}_3) \;\middle|\; g \equiv -fh \bmod 3 \right\}.$$

For later use, we introduce the surjective homomorphism

$$X \to \mathbf{Z}/9\mathbf{Z}, \qquad \begin{pmatrix} 1+3e & 3f \\ 3g & h \end{pmatrix} \mapsto e + 3(e^2 - g^2) \bmod 9.$$

Composing this map with the projection $G_3 \to X$, we obtain a surjection

$$F\colon G_3 \to \mathbf{Z}/9\mathbf{Z}.$$

The group G_3 is contained in the group of pairs $(g, x) \in \mathbf{GL}(2, \mathbf{Z}_3) \times X$ which satisfy the condition $\det g = \det x$. As Kaskel shows in [15], G_3 has index 3 in this latter group; this additional constraint on the elements of G_3 may be traced to the fact that both $\mathbf{Q}(E[3^\infty])$ and $\mathbf{Q}(E'[3^\infty])$ contain the field $\mathbf{Q}(\sqrt[3]{37})$.

Proposition 5.5. *With respect to suitable bases, G_3 is the group of pairs*

$$\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} 1+3e & 3f \\ 3g & h \end{pmatrix} \right) \in \mathbf{GL}(2, \mathbf{Z}_3) \times X$$

which satisfy the determinant condition $ad - bc = (1+3e)h - 9fg$ and the supplementary condition

$$(ac + bd)(c^2 + d^2) \equiv g \equiv -fh \bmod 3.$$

Corollary 5.6. *The homothety -2 belongs to G_3.*

We now state without proof a description of the full Galois group G. This description involves the homomorphisms $\epsilon\colon G_2 \to \mathbf{Z}/2\mathbf{Z}$ and $F\colon G_3 \to \mathbf{Z}/9\mathbf{Z}$ which were introduced above.

Theorem 5.7. *The group G is the subgroup of $\prod_\ell G_\ell$ consisting of all elements $(\dots, g_\ell, \dots)$ which are related by the identity*

$$\det(g_{37})^2 \equiv 2^{20F(g_3)+18\epsilon(g_2)} \bmod 37$$

in $\mathbf{F}_{37}^*$.

The reader will remark that the groups $G_{\{2,3,37\}}$ and $G^{\{2,3,37\}}$ are "independent" in the sense that G is the product of these two factors of G; we have already noted this point above. In the crucial quotient $G_{\{2,3,37\}}$, the two factors G_2 and G_3 are independent of each other: the group $G_{\{2,3\}}$ is the product of its quotients G_2 and G_3. On the other hand, G_{37} is linked to each of G_2 and G_3. See [31, Prop. 22] for a related observation.

The following consequence of Theorem 5.7 can be seen by inspection.

Corollary 5.8. *The homothety -5 belongs to $G_{\{2,3,37\}}$.*

6. Torsion points on $X_0(37)$

We now prove Theorem 1.4, which states that $\mathcal{S} = X_0(37) \cap J_0(37)_{\mathrm{tor}}$ contains only the two cusps C_∞ and C_0.

Let P be an element of $\mathcal{S}$. Recall that we may decompose P as the sum of its primary components P_p. According to Corollary 2.3, all P_p are zero except perhaps for $p = 2$, $p = 3$, and $p = 37$:

$$P = P_2 + P_3 + P_{37}.$$

We may thus view $\mathcal{S}$ as a subset of $J[M]$, where M is the product of suitable powers of 2, 3, and 37. (With the appropriate definition, one can take $M = 2^\infty 3^\infty 37^\infty$.) As we have just seen, there is an element of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ which acts on $J[M]$ as the homothety -5. By Proposition 4.2, we get

$$\#\mathcal{S} \leq 2(-5)^2 = 50,$$

since the genus of $X_0(37)$ is two. On the other hand, any element of $\mathcal{S}$ for which P_{37} is non-zero must have at least 1368 conjugates by Corollary 5.2. Thus each $P \in \mathcal{S}$ may be decomposed as the sum $P_2 + P_3$.

We claim next that $P_2 = 0$, i.e., that $P = P_3$. If not, there is a $g \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ such that $gP_2 - P_2$ has order 2 by Corollary 5.4. Because of the independence of G_2 and G_3, we may assume that g fixes P_3. Therefore, $gP - P$ has order two on J. As we saw in §1, it follows that P is a hyperelliptic branch point of $X_0(37)$. Indeed, the divisor $2\big((gP) - (P)\big)$ is the divisor of a non-constant function, and the point P is forced to ramify in the corresponding degree-two covering of $\mathbf{P}^1$. However, we have seen in Proposition 1.1 that the hyperelliptic branch points of $X_0(37)$ do not belong to $\mathcal{S}$.

Knowing that $\mathcal{S} \subseteq J_0(37)[3^\infty]$, we apply Corollary 5.6 and Proposition 4.2 and deduce the bound $\#\mathcal{S} \leq 8$. To conclude, we consider the degree-two covering $\pi\colon X_0(37) \to E$ which is obtained by dividing $X_0(37)$ by its Atkin-Lehner involution. This covering may be viewed as the composite of the Albanese map $X_0(37) \to J_0(37)$ sending C_∞ to 0 with a homomorphism of abelian varieties $J_0(37) \to E$ whose kernel is E' (regarded as an abelian subvariety of $J_0(37)$). As we have remarked, the image of G_3 in $\mathrm{Aut}(E[3^\infty])$ is all of $\mathbf{GL}(2, \mathbf{Z}_3)$. Hence any non-zero element of $E[3^\infty]$ has at least eight conjugates. It follows that the image of $\mathcal{S}$ in $E[3^\infty]$ is the single element 0. Indeed, $\mathcal{S}$ contains the two rational points C_∞ and C_0 and consists of at most eight elements. Therefore, it can contain no point with more than six conjugates. Thus $\mathcal{S}$ is contained in the set $\pi^{-1}(\{0\})$; since π has degree two, $\mathcal{S}$ can have no more than two elements. ∎

With an eye to possible generalizations, we present two variants of the proof of Theorem 1.4. In the first variant, we begin as before, writing $P \in \mathcal{S}$ as $P_2 + P_3 + P_{37}$, but noting that $P_{37} = 0$ because of Proposition 4.2. Thus $P = P_2 + P_3$.

Proposition 6.1. *The point P_3 belongs to the cuspidal subgroup of $J_0(37)$.*

Proof. We consider the two normalized newforms

$$F_1(q) = q + 0q^2 + \ q^3 + \cdots$$
$$F_2(q) = q - 2q^2 - 3q^3 + \cdots$$

of weight two on $\Gamma_0(37)$ and let ω_1 and ω_2 be the corresponding regular differentials on $X_0(37)$.

Lemma 6.2. *If p is an odd prime, neither ω_1 nor ω_2 has a double zero modulo p.*

Proof. Let w be the Atkin-Lehner involution of $X_0(37)$. Then

$$w^*\omega_1 = -\omega_1$$
$$w^*\omega_2 = \ \ \omega_2.$$

It follows, from this and the fact that $X_0(37)$ is hyperelliptic of genus 2, that both of these differentials are pullbacks of invariant differentials on elliptic curves by degree two morphisms. From this and the Riemann-Hurwitz theorem, the lemma follows. ∎

Continuing the proof of Proposition 6.1, we work in the context of §3, taking $p = 3$. After glancing at the displayed q-expansions, we see that $W_1 = \mathbf{Z}_p\omega_1$

and $W_2 = \mathbf{Z}_p\omega_2$ in that setting. In view of the Lemma we have just proved and Corollary 3.13, we find that the extension $\mathbf{Q}(P)/\mathbf{Q}$ is unramified at 3. The desired conclusion now follows from Theorem 2.2. ■

Our second proof of Theorem 1.4 now concludes as follows. We claim as before that $P_2 = 0$. Indeed, if P_2 is non-zero, then we may find as before a $g \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ such that $gP_2 - P_2$ has order 2. Because P_3 lies in $J_0(37)(\mathbf{Q})$, g fixes P_3. Therefore, $gP - P$ has order two on J, and we have seen that this is not the case. Thus we have $P = P_3 \in C$, where C is the cuspidal subgroup of $J_0(37)$. However, one knows that $X_0(37) \cap C$ consists precisely of the two cusps on $X_0(37)$ [23, §5, Prop. 2].

To make a third proof, we again write $P \in \mathcal{S}$ as the sum $P_2 + P_3 + P_{37}$. As we saw in the second proof, P_3 belongs to C. Once we know that P_{37} is zero, we can conclude as before. To see that this is the case, we argue by contradiction, supposing that P_{37} is not zero. Then P_{37} cannot belong to C, a group of order three. Thus, by Theorem 1.3, P_2 must be non-cuspidal, and hence non-zero. By Theorem 5.4, there is a $g_2 \in G_2$ with $\epsilon(g_2) = 0$ such that $g_2P_2 - P_2$ has order two. In view of Theorem 5.7, there is a $g = (\dots, g_\ell, \dots) \in G$ whose component at 2 is the given g_2 and whose component at 37 is 1. We then have

$$gP - P = (g_2P_2 - P_2) + (g_3P_3 - P_3) + (P_{37} - P_{37}) = (g_2P_2 - P_2).$$

In computing $gP - P$, we have used that P_3 is rational, so that $g_3P_3 = P_3$ for any choice of g_3. (Of course, we could have taken $g_3 = 1$.) Thus $gP - P$ has order two, and we have seen that this is impossible.

References

1. F. A. Bogomolov, *Sur l'algébricité des représentations l-adiques*, CRAS Paris, série A **290** (1980), 701–703.
2. R. F. Coleman, *Torsion points on curves and p-adic Abelian integrals*, Annals of Math. **121** (1985), 111–168.
3. ———, *Torsion points on Fermat curves*, Compositio Math. **58** (1986), 191–208.
4. ———, *Ramified torsion points on curves*, Duke Math. J. **54** (1987), 615–640.
5. ———, *Reciprocity laws on curves*, Compositio Math. **72** (1989), 205–235.
6. ———, *Torsion points on abelian étale coverings of* $\mathbf{P}^1 \setminus \{0, 1, \infty\}$, Trans. AMS **311** (1989), 185–208.
7. ———, *On a p-adic Inner Product on Elliptic Modular Forms*, Barsotti Symposium in algebraic geometry, Academic Press, New York, 1984, pp. 125–151.
8. R. Coleman and W. McCallum, *Stable reduction of Fermat curves and Jacobi sum Hecke characters*, J. reine angew. Math. **385** (1988), 41–101.
9. R. Coleman, A. Tamagawa and P. Tzermias, *The cuspidal torsion packet on Fermat curves* (To appear in Crelle.).
10. R. Coleman, The Monodromy Pairing (To appear.).
11. P. Deligne and M. Rapoport, *Les schémas de modules de courbes elliptiques*, Lecture Notes in Math., vol. 349, Springer-Verlag, Berlin and New York, 1973, pp. 143–316.
12. R. Greenberg, *On the Jacobian variety of some algebraic curves*, Compositio Math. **42** (1991), 345–359.
13. B. H. Gross, *A tameness criterion for Galois representations associated to modular forms* mod p, Duke Math. J. **61** (1990), 445–517.
14. M. Hindry, *Autour d'une conjecture de Serge Lang*, Invent. Math. **94** (1988), 575–603.
15. B. Kaskel, *The adelic representation associated to* $X_0(37)$, PhD. thesis, UC Berkeley, May, 1996.
16. K. Kato, *Logarithmic structures of Fontaine-Illusie*, Algebra, Analysis, Geometry and Number Theory (J.-I. Igusa, ed.), Johns Hopkins University Press, Baltimore, 1989, pp. 191–224.

17. N. M. Katz, *Serre-Tate local moduli*, Lecture Notes in Math., vol. 868, Springer-Verlag, Berlin and New York, 1981, pp. 138–202.
18. S. Lang, *Division points on curves*, Ann. Mat. Pura Appl. **70** (1965), 229–234.
19. ———, *Abelian varieties*, Springer-Verlag, Berlin and New York, 1983.
20. S. Lang and H. Trotter, *Frobenius distributions in* $\mathbf{GL}_2$*-extensions*, Lecture Notes in Math., vol. 504, Springer-Verlag, Berlin and New York, 1976.
21. B. Mazur, *Modular curves and the Eisenstein ideal*, Publ. Math. IHES **47** (1977), 33–186.
22. ———, *Rational isogenies of prime degree*, Invent. Math. **44** (1978), 129–162.
23. B. Mazur and P. Swinnerton-Dyer, *Arithmetic of Weil curves*, Invent. Math. **25** (1974), 1–61.
24. P. Michel and E. Ullmo, *Points de petite hauteur sur les courbes modulaires* $X_0(N)$ (to appear).
25. T. Miyake, *Modular forms*, Springer-Verlag, Berlin and New York, 1989.
26. A. Ogg, *Hyperelliptic modular curves*, Bull. Soc. Math. France **102** (1974), 449–462.
27. ———, *Automorphismes de courbes modulaires*, Sém. Delange-Pisot-Poitou (1974/1975, exposé 7).
28. M. Raynaud, *Courbes sur une variété abélienne et points de torsion*, Invent. Math. **71** (1983), 207–233.
29. K. Ribet, *Images of semistable Galois representations* (Preprint, 1996).
30. D. Rohrlich, *Points at infinity on Fermat curves*, Invent. Math. **39** (1977), 95–127.
31. J-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259–331.
32. ———, *Course at the Collège de France, 1985–1986.*
33. J. Tate, *The non-existence of certain Galois extensions of* $\mathbf{Q}$ *unramified outside 2*, Contemporary Mathematics **174** (1994), 153–156.
34. E. Ullmo, *Positivité et discretion des points algébriques des courbes*, Annals of Math. (to appear).

Errata for [4]

This list of errata for Coleman's article "Ramified torsion points on curves" was compiled by Matt Baker:

— p. 615 Conjecture B, part (ii): should read "$K/\mathbb{Q}$ is unramified at $\mathfrak{p}$."
— p. 620 line 3: should read " ... we get $p^k w = F^n h_n$ for all $n \geq k$."
— p. 623 fifth line from bottom: should read "$\omega_i = \frac{\phi^* \omega_{i+1}^{\sigma}}{p} + df_i$."
— p. 623 fourth line from bottom: "Let $0 < n_0 < n_1 < \cdots$" should read "Let $0 \leq n_0 < n_1 < \cdots$."
— p. 623 third line from bottom: "$\tilde{\omega_i} \in \tilde{\Omega}$" should be "$[\omega_i]^* \in \tilde{\Omega}$."
— p. 624 line 2: the p^{a_i} in the denominator should be a p.
— p. 624 line 3: should read "Let $h_i = g_i - g_i(Q) \in A^0(Y) \otimes R^u$."
— p. 624 line 5: should read "$dL(T) = \nu$ on U."
— p. 624 line 8 : should read "Let $k_i = \mathrm{ord}_U \tilde{\nu_i} + 1$."
— p. 624 Theorem 10: When $p = 2$ in part (iii), one can conclude from the proof that $i = M = 0, k_i = 1, Q_i = (1, 0), Q_{i+1} = (2, -1)$.
— p. 625 line 6: should read "$s(k_1 p - h) \leq (1 + s)(k_0 - h)$."
— p. 625 third line from bottom: p^h should be p^n.
— p. 627 fifth line from bottom: replace sentence beginning "To finish ..." with "To finish the proof of the proposition, we will eliminate all but one of the above possibilities for D."
— p. 628 line 7: "$n_{i+1} - n_i > 1$" should be "$n_{i+1} - n_i \geq 1$."
— p. 628 line 11: v^{n_i} should be V^{n_i}.
— p. 628 line 12: "for all $\eta \in \tilde{W}^*$" should be "for all $\eta \in W$."
— p. 629 line 4: "$k_0 \omega)$" should be "$k_0(\omega)$."
— p. 630 seventh line from bottom: should read "$\omega \in \tilde{W} \mapsto (\frac{\omega}{d\tilde{T}})(U)$."

— p. 630 fourth line from bottom: "let $e = e(a)$" should be "let $e = e(A)$."
— p. 631 line 2: should read "$b \in U(\mathbb{C}_p)$."
— p. 631 line 13: Proposition 10 should be Theorem 10.
— p. 631, Prop. 15, part (ii): $q - 1$ should be replaced by $q - 2$.
— p. 631 line 15: "when $p = 2, A = 1$" should be "when $q = 2, A \leq 1$."
— p. 631 middle: "for some $g_{\omega,i}T$)" should read "for some $g_{\omega,i}(T)$."
— p. 631 fifth line from bottom: replace "$g_{\omega,i}(0)$" by "$\frac{d}{dT}g_{\omega,i}(0)$."
— p. 632 line 3: replace "$a_n = a^{q^n}$" by "$a_n = a^{q^{n-1}}$."
— p. 632 line 4: replace "Theorem 4.2.1 of [C-1]" by "Theorem 4.1 of [C-1]."
— p. 632 middle: replace "$\frac{1}{p^{n'_{i+1}} - p^{n'_j}}$" by "$\frac{1}{p^{n'_{j+1}} - p^{n'_j}}$."
— p. 633 line 10: should say "$\omega \in W$."
— p. 633 proof of Theorem 18: reference to Cor. 13.1 should be to Cor. 13.3.
— p. 633 proof of Theorem 19: reference to Prop. 10 should be to Prop. 13.
— p. 634 Theorem 20: when $p = 2$ or 3, the theorem is incorrect. The present article contains corrected version.
— p. 635 proof of Theorem 20: reference to Prop. 19 should be to Prop. 15.

UC Mathematics Department, Berkeley, CA 94720-3840 USA