ACTA ARITHMETICA
120.2 (2005)

On torsion in $J_1(N)$

by

S. Kamienny (Los Angeles, CA)

1. The modular curves. Let N be a prime ≥ 13, and let $X_1(N)$ denote the non-singular projective curve over $\mathbb{Q}$ associated to the *moduli problem*:

> Classify, up to isomorphism, pairs (E, P) where E is an elliptic curve, and P is a point of E of order N.

We let $X_0(N)$ denote the non-singular projective curve over $\mathbb{Q}$ classifying isomorphism classes of pairs (E, C) where E is an elliptic curve, and C is a cyclic subgroup of E of order N.

The complex points of $X_0(N)$ may be viewed as the points of the compact Riemann surface $\Gamma_0(N)\backslash\mathbf{H}^*$, where $\mathbf{H}^* = \mathbb{P}^1(\mathbb{Q}) \cup \mathbf{H}$ is the completed upper half plane upon which

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PSL}_2(\mathbb{Z}) : c \equiv 0 \pmod{N} \right\}$$

acts via fractional linear transformations. Similarly the complex points of $X_1(N)$ are the points of the compact Riemann surface $\Gamma_1(N)\backslash\mathbf{H}^*$ where

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) : a \equiv d \equiv 1 \pmod{N} \right\}.$$

From either point of view it is clear that $X_1(N)$ is a cyclic cover of $X_0(N)$ with covering group $\triangle$ isomorphic to $(\mathbb{Z}/N\mathbb{Z})^*/(\pm 1)$. The covering map $\pi : X_1(N) \to X_0(N)$ is given, on non-cuspidal points, by $\pi(E, P) = (E, C_P)$ where C_P is the subgroup of E generated by P. We denote by $\langle a \rangle$ the element of $\triangle$ which acts on a non-cuspidal point (E, P) by $\langle a \rangle (E, P) = (E, aP)$.

The curve $X_0(N)_{/\mathbb{Q}}$ has two cusps 0 and ∞, each rational over $\mathbb{Q}$. The cusps are unramified in the cover $X_1(N) \to X_0(N)$, so there are $(N-1)/2$ cusps of $X_1(N)$ lying above the cusp $0 \in X_0(N)$. We call these the 0-*cusps*. Similarly there are $(N-1)/2$ cusps lying above ∞. We call

2000 *Mathematics Subject Classification*: 11G18, 14G35.

these the ∞-*cusps* of $X_1(N)$. We work with a model of $X_1(N)$ in which the 0-cusps are $\mathbb{Q}$-rational, and the ∞-cusps are rational in $\mathbb{Q}(\zeta_N)^+$.

2. The jacobians and Hecke operators. We denote by $J_1(N)$ (respectively, $J_0(N)$) the jacobian of the modular curve $X_1(N)_{/\mathbb{Q}}$ (resp., $X_0(N)_{/\mathbb{Q}}$). The abelian variety $J_0(N)$ is semi-stable over $\mathbb{Q}$, and has bad reduction only at the prime N. The abelian variety $J_1(N)_{/\mathbb{Q}}$ also has good reduction away from the prime N, but we can say even more. Let $S = \operatorname{Spec}\mathbb{Z}[1/N]$, and regard all of our varieties as schemes over S. The maximal étale cover $X_2(N) \to X_0(N)$ that is intermediate for the cover $X_1(N) \to X_0(N)$ has covering group D isomorphic to the unique quotient of $\triangle$ of order $n = \operatorname{num}((N-1)/12)$. The map $\pi : X_1(N) \to X_0(N)$ induces, via Pic° functoriality, a map $\pi^* : J_0(N) \to J_1(N)$ whose kernel is Cartier dual to D (regarded as a constant group scheme over S). The quotient abelian variety $A = J_1(N)/\pi^* J_0(N)$ attains everywhere good reduction over $\mathbb{Q}(\zeta_N)^+$.

We embed $X_1(N)$ into $J_1(N)$, sending a 0-cusp to $0 \in J_1(N)$. The divisor classes supported only at the 0-cusps form a finite subgroup C of $J_1(N)(\mathbb{Q})$ of order $M = N \cdot \Pi\left(\frac{1}{4}\mathbb{B}_{2,\varepsilon}\right)$ (see [3]), where the product is taken over all even characters ε of $(\mathbb{Z}/N\mathbb{Z})^*$. The odd primes p in the support of some $\mathbb{B}_{2,\varepsilon}$ are precisely the odd prime divisors of M. We call these p the *cuspidal primes*.

The automorphism group of $X_1(N)$ is isomorphic to the dihedral group D_{N-1} of order $N-1$. It is generated by the covering group $\triangle$, and any lift w_ζ of the Atkin–Lehner involution w (of $X_0(N)$) to $X_1(N)$. The involutions w_ζ switch the 0-cusps and the ∞-cusps, so the latter also generate a subgroup of order M in $J_1(N)$. The points of this subgroup are rational in $\mathbb{Q}(\zeta_N)^+$.

The standard Hecke operators T_l (l a prime $\neq N$) and U_N act as correspondences on the curve $X_1(N)_{/\mathbb{Q}}$. As such they induce endomorphisms of the jacobian $J_1(N)$. We define the *Hecke algebra* $\mathbb{T}$ to be the algebra of endomorphisms of $J_1(N)$ generated over $\mathbb{Z}$ by the T_l ($l \neq N$), U_N, and $\triangle$. It is a commutative ring of finite type over $\mathbb{Z}$, and all of its elements are defined over $\mathbb{Q}$. The Hecke algebra $\mathbb{T}$ preserves $\pi^* J_0(N)$, and induces an algebra (again denoted by $\mathbb{T}$) of endomorphisms of the quotient A.

Since $J_1(N)$ and A have good reduction away from N their Néron models $J_{/S}$ and $A_{/S}$ over S are abelian schemes. We denote their fibers at l by $J_{/\mathbb{F}_l}$ and $A_{/\mathbb{F}_l}$, respectively. The fibers $J_{/\mathbb{F}_l}$ and $A_{/\mathbb{F}_l}$ inherit an action of the appropriate Hecke algebra $\mathbb{T}$ from the induced action of $\mathbb{T}$ on the Néron models. The Eichler–Shimura relation

$$T_l = \operatorname{Frob}_l + \frac{l\langle l\rangle}{\operatorname{Frob}_l}$$

holds in $\operatorname{End}(J_{/\mathbb{F}_l})$ (resp., $\operatorname{End}(A_{/\mathbb{F}_l})$). We can lift this relation to the p-divisible group $J_p(\overline{\mathbb{Q}})$ (resp., $A_p(\overline{\mathbb{Q}})$) where p is any prime $\neq l, N$, as well as to any étale subgroup of $J_l(\overline{\mathbb{Q}})$ (resp., $A_l(\overline{\mathbb{Q}})$). Of course, in the original equation Frob_l is the Frobenius endomorphism of the group scheme $J_{/\mathbb{F}_l}$ (resp., $A_{/\mathbb{F}_l}$), while in the lift Frob_l is any l-Frobenius automorphism in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

3. Rational torsion in A and maximal ideals of the Hecke algebra. Let K be a degree d Galois extension of $\mathbb{Q}$ with Galois group $G = \mathrm{Gal}(K/\mathbb{Q})$. We suppose that K is disjoint from $\mathbb{Q}(\zeta_N)^+$, and that there exists a K-rational point $P \in A(K)$ of odd prime order p. We also suppose that $p > d+1$, and that $p \neq N$.

We let V be the $(\mathbb{T}/p\mathbb{T})[G]$ span of P, and fix an irreducible submodule W of V. Since W is irreducible its annihilator (in $\mathbb{T}$) is a maximal ideal $\mathcal{M}$. We write k for the residue field $\mathbb{T}/\mathcal{M}$, and note that k is a finite field of characteristic p. Finally, we let $A[\mathcal{M}]$ denote the kernel of the ideal $\mathcal{M}$ acting on A, i.e., $A[\mathcal{M}] = \bigcap_{\alpha\in\mathcal{M}} \mathcal{A}[\alpha]$.

PROPOSITION 3.1. *$A[\mathcal{M}]^{\text{ét}}_{/\mathbb{F}_p}$ is a k-vector group scheme of rank one.*

Proof. Let O be the ring of integers of the completion of K at a prime of residue characteristic p, and let $R = \mathrm{Spec}\, O$. Since $p \neq N$ the Néron model $A_{/R}$ of A over R is an abelian scheme, and the Zariski closure $W_{/R}$ of W in $A_{/R}$ is a finite flat group scheme. Moreover, since $d < p-1$ we see immediately that $W_{/R}$ is an étale group scheme (see [7]), and so $A[\mathcal{M}]^{\text{ét}}_{/\mathbb{F}_p}$ is non-zero.

Now following [5], we recall that there is a canonical isomorphism

$$\delta : J_1(N)[p](\overline{\mathbb{F}}_p) \to H^\circ(X_1(N)_{/\mathbb{F}_p}, \Omega^1)^{\mathcal{C}}$$

where the right hand side consists of those elements fixed by the Cartier operator $\mathcal{C}$. This isomorphism induces an injection

$$J_1(N)[\mathcal{M}](\overline{\mathbb{F}}_p) \otimes_{\mathbb{F}_p} \overline{\mathbb{F}}_p \hookrightarrow H^\circ(X_1(N)_{/\overline{\mathbb{F}}_p}, \Omega^1)[\mathcal{M}].$$

The q-expansion principle (see [2]) shows that the right hand side injects into the module B of q-expansions of weight two cusp forms with coefficients in $\overline{\mathbb{F}}_p$. The submodule $B[\mathcal{M}]$ is a one-dimensional k-vector space. The proposition follows immediately.

As a corollary we obtain

COROLLARY 3.2. *$W_{/S}$ is a one-dimensional k-vector group scheme.*

It follows from Corollary 3.2 that the $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ representation on W is given by a character

$$\psi : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to k^*$$

that is unramified away from p and N. Let $O_{\mathbb{Q}(\zeta_N)^+}$ denote the integer ring of $\mathbb{Q}(\zeta_N)^+$, and let $T = \mathrm{Spec}\, O_{\mathbb{Q}(\zeta_N)^+}$. The Galois representation on $W_{/T}$ is ramified only at primes above p, so ψ is a product $\psi = \chi\varepsilon$ of a character ε of $\mathrm{Gal}(\mathbb{Q}(\zeta_N)^+/\mathbb{Q})$ with a character $\chi : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to k^*$ that is ramified only at p. We twist W by tensoring with $(\mathbb{Z}/p\mathbb{Z} \otimes k)[\varepsilon^{-1}]$ to obtain a rank one k-vector group scheme $X = W \otimes (\mathbb{Z}/p\mathbb{Z} \otimes k)[\varepsilon^{-1}]$ that is ramified only at p. Applying [7] (or even [6]), and using the fact that p is unramified in $\mathbb{Q}(\zeta_N)^+$, we see that $X_{/T}$ must be either $\mathbb{Z}/p\mathbb{Z} \otimes k$ or $\mu_p \otimes k$. However, since W is étale the latter is clearly impossible, and so $X_{/T} \approx (\mathbb{Z}/p\mathbb{Z} \otimes k)_{/T}$ and $W_{/S} \approx (\mathbb{Z}/p\mathbb{Z} \otimes k)[\varepsilon]$. Finally, we note that $(\mathbb{Z}/p\mathbb{Z} \otimes k)[\varepsilon]$ does not have its points rational over K unless $\varepsilon = 1$.

THEOREM 3.3. *Let K be a degree d Galois number field that is disjoint from $\mathbb{Q}(\zeta_N)^+$, and let P be a K-rational point of A of order p. If $p > d + 1$, and $p \neq N$, then the prime p is cuspidal.*

Proof. The covering group $\triangle$ acts on the submodule W via an even character η of $(\mathbb{Z}/N\mathbb{Z})^*$. The Eichler–Shimura relation shows that the elements $T_l - (1 + l\eta(l))$ (for $l \neq N$) annihilate W, and so lie in $\mathcal{M}$. Write T_N for U_N, and let $\varphi = \sum_{n>0} T_n q^n \in \mathbb{T}[[q]]$ be the q-expansion of the weight two cusp form (on $\Gamma_1(N)$ over $\mathbb{T}$) whose existence follows from the q-expansion principle (see [1]). We also let

$$g = \frac{-\mathbb{B}_{2,\eta}}{2} + \sum_{n>0} \Big(\sum_{d|n} \eta(d) \cdot d \Big) q^n$$

be the usual weight two Eisenstein series on $\Gamma_0(N, \eta)$. Then

$$\varphi - g \equiv \frac{\mathbb{B}_{2,\eta}}{2} + h(q^N) \pmod{\mathcal{M}},$$

i.e., the right hand side is a function $\widetilde{f}$ of q^N. The modular form $\widetilde{f}$ is the push-up of a weight two holomorphic modular form on $\Gamma_1(1)$ over k. Since $p > 3$ such a modular form must be zero (see [2], [4], [5], [9]). Thus, modulo $\mathcal{M}$, all Hecke operators are congruent to elements in $\mathbb{Z}[\eta]$, and $\mathbb{B}_{2,\eta}$ must lie in the ideal $\mathcal{M}$. It follows that p is a cuspidal prime.

4. The exceptional cases and the case $d = 2$. If $p = N$ then much of what we have done will often still work. For our group scheme arguments we need to assume that the ramification degree of N in $K \cdot \mathbb{Q}(\zeta_N)^+$ is $< N - 1$. Thus, we assume either that N is unramified in K or that $K \subseteq \mathbb{Q}(\zeta_N)^+$. Lemma 5.3 of [1], together with the arguments of §3, shows that if P has order N then P is annihilated by the Eisenstein ideal of $\mathbb{T}$. Theorem 7.2 of [10], in place of Proposition 3.1, may then be used to show that P actually lies in the cuspidal divisor class group of $J_1(N)$. In particular, N must be an irregular prime.

Finally, we restrict our attention to the case where $d = [K : \mathbb{Q}] = 2$. We let σ be the non-trivial element of $\mathrm{Gal}(K/\mathbb{Q})$ and suppose that there exists a K-rational p-torsion point P on A for some prime $p \neq 2, 3$. Either $P + P^\sigma$ is 0, or $P + P^\sigma$ is a non-trivial p-torsion point in $A(\mathbb{Q})$. In the latter case our arguments, applied to $P + P^\sigma$, show that the point $P + P^\sigma$ actually lies in the cuspidal group C as long as $p \neq 2$. If $P + P^\sigma$ is 0 then P generates a $\mathrm{Gal}(K/\mathbb{Q})$-invariant submodule Y of $A(K)$ of order p. Applying our arguments to Y in place of W shows that p is cuspidal.

We have thus far excluded points on $\pi^* J_0(N)$. In order to study these we recall that the isogeny

$$J_0(N) \to \pi^* J_0(N)$$

has kernel of order $n = \mathrm{num}((N-1)/12)$. This is also the order of the cuspidal group on $J_0(N)$. We regard $\mathbb{T}$ as an algebra of endomorphisms of $J_0(N)$, and let $\mathcal{M}$ be a maximal ideal of $\mathbb{T}$. Mazur [5] has shown that $\ker \mathcal{M}$ is a two-dimensional $k = \mathbb{T}/\mathcal{M}$-vector space. Ribet [8] has shown that if $\mathcal{M}$ is a non-Eisenstein maximal ideal then the image of the $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-representation on $\ker \mathcal{M}$ contains $\mathrm{SL}_2(k)$. We suppose that, for some prime p not dividing n, there exists a K-rational p-torsion point P on $J_0(N)$. As before, we let V be the $\mathbb{T}/p\mathbb{T}[G]$-module spanned by P, W an irreducible submodule, and $\mathcal{M}$ the annihilator (in $\mathbb{T}$) of W. Then the image of the $\mathrm{Gal}(\overline{K}/K)$-representation on $\ker \mathcal{M}$ is, for a suitable choice of basis, of the form

$$\begin{pmatrix} 1 & * \\ 0 & \chi \end{pmatrix}.$$

It follows that K must be an extension of $\mathbb{Q}$ of degree $d > p + 1$. Thus, if, as we assumed, $d < p - 1$ the point P cannot exist.

Remark. The techniques of §3 can be used to show that the kernel of any non-Eisenstein maximal ideal $\mathcal{M}$ of $\mathbb{T}$ (acting on $J_1(N)$) is irreducible as a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module. This provides an alternate proof for the case $d = 2$, since an irreducible Galois representation will not admit a trivial subspace over an extension of degree 2 when $p > 3$.

References

[1] S. Kamienny, *Rational points on modular curves*, J. Reine Angew. Math. 359 (1985), 174–187.

[2] N. Katz, *p-adic properties of modular schemes and modular forms*, in: Lecture Notes in Math. 350, Springer, 1973, 69–190.

[3] D. Kubert and S. Lang, *Modular Units*, Springer, 1981.

[4] S. Lang, *Introduction to Modular Forms*, Springer, 1976.

[5] B. Mazur, *Modular curves and the Eisenstein ideal*, Publ. Math. I.H.E.S. 47 (1978), 33–186.
[6] F. Oort and J. Tate, *Group schemes of prime order*, Ann. Sci. École Norm. Sup. (4) 3 (1970), 1–21.
[7] M. Raynand, *Schémas en groupes de type* $(p, \ldots, p)$, Bull. Soc. Math. France 102 (1974), 241–280.
[8] K. Ribet, *Images of semistable Galois representations*, Pacific J. Math. 81 (1997), 277–297.
[9] J.-P. Serre, *Formes modulaires et fonctions zêta p-adiques*, in: Lecture Notes in Math. 350, Springer, 1973, 191–268.
[10] A. Wiles, *Modular curves and the class group of* $\mathbb{Q}(\zeta_p)$, Invent. Math. 58 (1980), 1–35.

Department of Mathematics
University of Southern California
3620 S. Vermont Avenue
Los Angeles, CA 90089-2532, U.S.A.
E-mail: kamienny@usc.edu

Received on 4.1.2005 (4920)