SPANS OF HECKE POINTS ON MODULAR CURVES

BJORN POONEN

ABSTRACT. We correct a theorem in the literature describing the rank of the span of the images of a point on a modular curve under Hecke correspondences.

Let $X$ be a modular curve over $\mathbb{Q}$ associated to one of the congruence subgroups $\Gamma_0(N)$, $\Gamma_1(N)$, or $\Gamma(N)$. Assume that $X$ has genus at least 2. Identify $X$ with its image in the jacobian $J$ under the map taking $x$ to the class of $x - \infty$, where $\infty \in X(\mathbb{Q})$ denotes the usual cusp. Let $J_{\text{tors}}$ denote the torsion subgroup of $J(\mathbb{Q})$. For any prime $p$ not dividing $N$, the Hecke correspondence $T_p$ on $X$ induces an endomorphism $\tau_p$ of $J$. Finally, let $\mathbb{Z}T_p(x)$ denote the $\mathbb{Z}$-span in $J(\mathbb{Q})$ of the $p + 1$ points of $X(\mathbb{Q})$ obtained by applying $T_p$ to $x$.

The main result of this note is Theorem 2, which contradicts the following.

**Statement 1** (Theorem 0.4 in [Si2]). Let $x \in X(\overline{\mathbb{Q}})$ be a noncuspidal, non-CM point. Then for $p$ sufficiently large,

$$\text{rank } \mathbb{Z}T_p(x) = \begin{cases} p, & \text{if } x \in J_{\text{tors}}, \\ p + 1, & \text{otherwise.} \end{cases}$$

It is only the last sentence of the proof in [Si2] that is flawed: the “$i(x) \in J_{\text{tors}}$ or $\tau_p = 0$” on the left hand side of the last chain of equivalences should be replaced by “$\tau_p(i(x)) \in J_{\text{tors}}$”. Therefore Statement 1 becomes true if “$x \in J_{\text{tors}}$” is replaced by “$\tau_p x \in J_{\text{tors}}$”.

Theorem 0.4 in [Si2] plays the role only of a remark: the main results of that paper, which are concerned with the heights of the images of a point under a Hecke correspondence, are unaffected by the correction. Silverman explained to me that he attributed Theorem 0.4 in [Si2] to “Mazur, unpublished” because Mazur sketched a statement and proof to him verbally; therefore he feels that Mazur should get credit for the idea, while he accepts responsibility for the minor error in its write-up.

**Theorem 2.** Suppose that $J$ is isogenous over $\mathbb{Q}$ to a product of elliptic curves $E \times F$. Then there exist infinitely many nontorsion, noncuspidal, non-CM points $x \in X(\overline{\mathbb{Q}})$ such that there exist infinitely many primes $p$ not dividing $N$ for which $\text{rank } \mathbb{Z}T_p(x) = p$.

Received October 23, 2001.

2000 Mathematics Subject Classification. Primary 14G35.

Key words and phrases. Modular curve, Hecke operator, height, CM point.

This research was supported by NSF grant DMS-9801104, and a Packard Fellowship.
Proof. The composition $X \hookrightarrow J \to E \times F \to F$ is a finite morphism $\pi$. The set $F_{\text{tors}}$ is infinite and of bounded height, so the same is true of $\pi^{-1}(F_{\text{tors}})$. Any set of CM points of bounded height on $X$ is finite (see our appendix), the set of cusps on $X$ is finite, and $X \cap J_{\text{tors}}$ is finite [Ra], so $\pi^{-1}(F_{\text{tors}})$ contains infinitely many nontorsion, noncuspidal, non-CM points.

Let $x$ be any such point. Eichler-Shimura theory implies that for any prime $p$ not dividing $N$, the diagram

$$
\begin{array}{ccc}
J & \xrightarrow{\tau_p} & J \\
\downarrow & & \downarrow \\
E \times F & \xrightarrow{(a_p,b_p)} & E \times F
\end{array}
$$

(1)

commutes, where $a_p : E \to E$ denotes multiplication by the integer that is the trace of the action of a $p$-power Frobenius automorphism on the $\ell$-adic Tate module of $E$ for some prime $\ell \neq p$, and $b_p$ is defined similarly for $F$. By [El], there exist infinitely many primes $p$ for which $a_p = 0$. For any such $p$, (1) shows that $\tau_p x$ maps to zero in $E$, and to a torsion point in $F$, since $x$ maps to a torsion point in $F$. Hence $\tau_p x \in J_{\text{tors}}$. If moreover $p$ is sufficiently large, then $\text{rank } \mathbb{Z}T_p(x) = p$ by the corrected version of Statement 1.

Remarks.

1. Checking the list of $X_0(N)$, $X_1(N)$, and $X(N)$ of genus 2, we find that the hypothesis of Theorem 2 is satisfied if and only if $X$ is one of $X_0(22)$, $X_0(26)$, $X_0(28)$, $X_0(37)$, and $X_0(50)$.

2. Checking these cases shows that $F$ in Theorem 2 is never CM. If $\ell$ is a sufficiently large prime, if $y \in F_{\text{tors}}$ has exact order $\ell$, and if $x \in X(\overline{\mathbb{Q}})$ is CM, then $\pi(x) \neq y$, because the fields of definition of CM points on $X$ are contained in bounded degree extensions of abelian extensions of imaginary quadratic number fields, whereas [Se] shows that for $\ell$ large, the Galois group of the Galois closure of the field of definition of $y$ is $\text{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$, which has a large nonabelian Jordan-Hölder constituent. This remark lets one prove Theorem 2 without the result in our appendix.

3. We give one explicit counterexample to Statement 1. Let $X = X_0(37)$. Let $\iota$ be the hyperelliptic involution, and let $x = \iota(\infty)$. Then $J$ is isogenous to a product of elliptic curves $E \times F$ such that $x$ maps to a nontorsion point in $E$ but to a torsion point in $F$, and $x$ is not a cusp [MS, §5.2]. Also $x$ is not CM: this can be proved by comparing the value of $j(x)$ given in [MS, §5.2] against the 13 $j$-invariants of elliptic curves over $\mathbb{Q}$, or by ruling out the existence of a CM elliptic curve over $\mathbb{Q}$ with a rational subgroup of order 37. The proof of Theorem 2 shows that Statement 1 fails for $x$.

4. The example of $X = X_0(37)$ and $x = \iota(\infty)$ also gives a counterexample to Corollary 4.2 of [Ba], whose proof relied on Theorem 0.4 of [Si2].
Appendix: heights of CM $j$-invariants

Define the naive Weil height $h : \mathbb{Q} \to \mathbb{R}$ by identifying $\mathbb{Q} = A^1(\mathbb{Q})$ with a subset of $\mathbb{P}^1(\mathbb{Q})$. Let $j_E$ denote the $j$-invariant of an elliptic curve $E$ over $\mathbb{Q}$. For the sake of the nonexperts, we indicate how the following can be deduced from results in the literature.

**Lemma 3.** Let $S$ be the set of elliptic curves over $\mathbb{Q}$ having CM. For any $B > 0$, \( \{ E \in S \mid h(j_E) < B \} \) is finite.

**Proof.** By the one-dimensional case of a result of Faltings (the last sentence of Proposition 2.1 of [Si1]), the stable Faltings height $h_{\text{Fal}}^\text{st}(E)$ is bounded above and below by increasing affine linear functions of $h(j_E)$. Therefore it suffices to prove Lemma 3 with $h(j_E)$ replaced by $h_{\text{Fal}}^\text{st}(E)$. Suppose $E \in S$ has CM by the order of conductor $f$ in the ring of integers $\mathcal{O}_K$ of the quadratic number field $K$ of discriminant $-D$. Then there exists an isogeny $E \to E_1$ of degree $f$, for some $E_1$ with CM by $\mathcal{O}_K$. Let $\chi : \mathbb{Z}/D \mathbb{Z} \to \{0, \pm 1\}$ denote the Kronecker symbol associated to $K$. By (1.5) and Lemma 2 of [NT],

\[
h_{\text{Fal}}^\text{st}(E) = h_{\text{Fal}}^\text{st}(E_1) + \sum_{\text{prime } p | f} \left( \frac{n_p - e_p}{2} \right) \log p,
\]

where $n_p = \text{ord}_p(f)$ and $e_p = \frac{(1 - \chi(p))(1 - p^{-n_p})}{(p - \chi(p))(1 - p^{-1})}$. A short argument shows $e_p \leq \frac{2}{3} n_p$, so $h_{\text{Fal}}^\text{st}(E) \geq h_{\text{Fal}}^\text{st}(E_1) + (\log f)/6$. Théorème 1 of [Co] shows that $h_{\text{Fal}}^\text{st}(E_1) \geq c_1 \log D + c_2$ for some universal constants $c_1 > 0$ and $c_2 \in \mathbb{R}$, so

\[
h_{\text{Fal}}^\text{st}(E) \geq c_3 \log(f^2 D) + c_4
\]

for some universal $c_3 > 0$ and $c_4 \in \mathbb{R}$. The result follows, since there are finitely many imaginary quadratic orders whose discriminant $-f^2 D$ is bounded in absolute value by a given constant, and finitely many $E$ over $\mathbb{Q}$ with CM by a given order. \qed

By the functoriality of Weil heights, Lemma 3 implies that a set of CM points of bounded height on any modular curve is finite.

**Acknowledgements**

It was Matt Baker who first noticed that the proof of Theorem 0.4 in [Si2] seemed to be incomplete. I thank Ken Ribet for a conversation, and I thank Pierre Colmez for pointing out how Lemma 3 is a consequence of known results.
References


Department of Mathematics, University of California, Berkeley, CA 94720-3840, USA.

E-mail address: poonen@math.berkeley.edu