Mathematical Research Letters **3**, 103–107 (1996)

GALOIS REPRESENTATIONS IN THE TATE-SHAFAREVICH GROUP OF AN ELLIPTIC CURVE

David E. Rohrlich

This letter is intended as a footnote to a paper of Kramer [2]. The main result of [2] is that there exist semistable elliptic curves E over $\mathbb{Q}$ with arbitrarily large $Ш(E/\mathbb{Q})_2$, where $Ш(E/\mathbb{Q})$ is the Tate-Shafarevich group of E over $\mathbb{Q}$ and $Ш(E/\mathbb{Q})_2$ the subgroup of elements of order dividing 2. The footnote to be added here is that Kramer's construction also gives Tate-Shafarevich groups which are arbitrarily large as Galois-modules:

Theorem. *Let K be a finite Galois extension of $\mathbb{Q}$ and n a positive integer. There exists a semistable elliptic curve E over $\mathbb{Q}$ such that the natural representation of $\mathrm{Gal}(K/\mathbb{Q})$ on $Ш(E/K)_2$ contains a subrepresentation isomorphic to the direct sum of n copies of the regular representation of $\mathrm{Gal}(K/\mathbb{Q})$ over $\mathbb{F}_2$.*

Let m be an integer. As in [2], we consider the elliptic curves

$$A : y^2 + xy = x^3 + 8mx^2 + m(16m+1)x$$

and

$$B : y^2 + xy = x^3 - 16mx^2 - 8mx - m$$

over $\mathbb{Q}$. They are related by an isogeny $f : A \to B$ with kernel the group of order 2 generated by the point (0,0) on A. Let $\mathrm{Sel}_2(A/K)$ and $\mathrm{Sel}_g(B/K)$ denote respectively the 2-Selmer group of A over K and the g-Selmer group of B over K, where $g : B \to A$ is the isogeny dual to f. Since $f \circ g$ is multiplication by 2, the kernel of the map $Ш(B/K) \to Ш(A/K)$ induced by g is a subgroup $Ш(B/K)_g$ of $Ш(B/K)_2$. A key role in Kramer's argument is played by the commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A(K)/2A(K) & \longrightarrow & \mathrm{Sel}_2(A/K) & \longrightarrow & Ш(A/K)_2 & \longrightarrow & 0 \\
 & & \alpha\downarrow & & \pi\downarrow & & & & \\
0 & \longrightarrow & A(K)/gB(K) & \longrightarrow & \mathrm{Sel}_g(B/K) & \xrightarrow{\beta} & Ш(B/K)_g & \longrightarrow & 0,
\end{array}$$

Received November 1, 1995.

Research partially supported by NSF grant DMS-9396090 and the Mathematical Sciences Research Institute.

where α is surjective and the rows are exact. If V is a subspace of $\mathrm{Sel}_g(B/K)$ which intersects the image of π trivially then β maps V injectively into $Ш(B/K)_g$, because α is surjective. We shall see that for an appropriate choice of m there exists such a subspace V which is stable under $\mathrm{Gal}(K/\mathbb{Q})$ and isomorphic as a representation to the direct sum of n copies of the regular representation.

Our choice of m differs slightly from Kramer's in that we take m even rather than odd. The reason for this change is that we want A to have split multiplicative reduction at 2 rather than ordinary reduction so that we will be able to apply the local results of Brumer-Kramer [1] even when K is ramified at 2. The 2-Selmer group of an elliptic curve with ordinary reduction over a ramified extension of $\mathbb{Q}_2$ does not seem to have been determined as yet.

We denote the completion of K at a place v by K_v. If v is the finite place corresponding to a prime ideal $\mathfrak{m}$ then we write $v = v(\mathfrak{m})$. If $v = v(\mathfrak{m})$ and $\mathfrak{m}$ divides m then we also write $v|m$.

Lemma. *Given a positive integer n, there exists a positive even integer m with the following properties:*

(i) *There are at least n distinct primes $m_1, m_2, \dots, m_n$ which divide m and split completely in K.*

(ii) *The integer $\ell = 16m + 1$ has the form*

$$\ell = \ell_1 \ell_2 \dots \ell_n r,$$

where r is a prime congruent to $1 \pmod 4$ and $\ell_1, \ell_2, \dots, \ell_n$ are distinct primes congruent to $1 \pmod 4$ which split completely into principal prime ideals of K.

(iii) *Suppose that the principal fractional ideal generated by an element $b \in K^\times$ is the square of an ideal of K. Then $b \in K_v^{\times 2}$ for $v|m_i$ $(1 \leqslant i \leqslant n)$. Furthermore, there exist*

- *prime ideals $\mathfrak{m}_1, \mathfrak{m}_2, \dots, \mathfrak{m}_n$ of K lying over $m_1, m_2, \dots, m_n$ respectively,*
- *prime ideals $\mathfrak{l}_1, \mathfrak{l}_2, \dots, \mathfrak{l}_n$ of K lying over $\ell_1, \ell_2, \dots, \ell_n$ respectively, and*
- *generators $\lambda_1, \lambda_2, \dots, \lambda_n$ of $\mathfrak{l}_1, \mathfrak{l}_2, \dots, \mathfrak{l}_n$ respectively*

such that for $1 \leqslant i, j \leqslant n$ and $\sigma, \tau \in \mathrm{Gal}(K/\mathbb{Q})$,

$$\lambda_i^\sigma \notin K_v^{\times 2} \text{ with } v = v(\mathfrak{m}_j^\tau) \Longleftrightarrow i = j \text{ and } \sigma = \tau.$$

Proof. The proof is much the same as in [2], but with the additional input of the Chebotarev density theorem.

Let H be the Hilbert class field of K and let $\ell_1, \ell_2, \ldots, \ell_n$ be distinct primes which split completely in $H(\sqrt{-1})$. Then the ℓ_i split completely in K and are congruent to 1 (mod 4) because they split in $\mathbb{Q}(\sqrt{-1})$. Let $\mathfrak{l}_i$ be any prime ideal of K lying over ℓ_i. Since $\mathfrak{l}_i$ splits completely in H it is a principal ideal, and we let λ_i be any generator.

Next choose a set of fractional ideals of K which represent the distinct ideal classes of order 2, and for each representative $\mathfrak{b}$ choose a generator $b(\mathfrak{b})$ of the principal ideal $\mathfrak{b}^2$. Let B be the set of elements $b(\mathfrak{b})$ so obtained, and let U be a set of generators of the group of integral units of K. Then the extension F of K defined by

$$F = K(\{\sqrt{z} : z \in B \cup U\})$$

is independent of any choices and hence Galois over $\mathbb{Q}$. Put

$$\Lambda = \{\lambda_i^\sigma : 1 \leqslant i \leqslant n,\ \sigma \in \mathrm{Gal}(K/\mathbb{Q})\}.$$

Since the ℓ_i are odd primes while the extension F/K is unramified outside 2 and infinity, the extension

$$L = F(\{\sqrt{\lambda} : \lambda \in \Lambda\})$$

has the same degree over F as $K(\{\sqrt{\lambda} : \lambda \in \Lambda\})$ has over K, namely $2^{n[K:\mathbb{Q}]}$. In particular, putting

$$\Lambda_j = \Lambda - \{\lambda_j\}$$

and

$$L_j = F(\{\sqrt{\lambda} : \lambda \in \Lambda_j\}),$$

we have $[L : L_j] = 2$ for $1 \leqslant j \leqslant n$. Let $\mathfrak{M}_1, \mathfrak{M}_2, \ldots, \mathfrak{M}_n$ be primes ideals of L, unramified over $\mathbb{Q}$, such that the Artin symbol $(\mathfrak{M}_j, L/\mathbb{Q})$ coincides with the nontrivial element of $\mathrm{Gal}(L/L_j)$. Put $\mathfrak{m}_j = K \cap \mathfrak{M}_j$ and let m_j be the rational prime lying below $\mathfrak{m}_j$. If $\mathfrak{m}$ is a prime ideal of K lying over some m_j, then $\mathfrak{m}$ splits completely in F and consequently $b \in K_v^{\times 2}$ when $v = v(\mathfrak{m})$ and b is as in (iii). Furthermore, for $v = v(\mathfrak{m}_j)$ we have $\lambda_i^\sigma \notin K_v^{\times 2}$ if and only if $i = j$ and $\sigma = 1$, whence the second assertion in (iii) follows on replacing σ by $\sigma\tau^{-1}$.

To complete the proof of the lemma, choose a prime r such that

$$\ell_1\ell_2 \ldots \ell_n r \equiv 1 \pmod{32 m_1 m_2 \ldots m_n},$$

and put $m = (\ell_1\ell_2 \ldots \ell_n r - 1)/16$. Then m is a positive even integer with the required properties, and $\ell = 1 + 16m$ has the required form.

Let $\mathcal{L}$ and $\mathcal{M}$ be the sets of prime divisors of ℓ and m respectively, where ℓ and m are as in the lemma. Then A has good reduction outside $\mathcal{L} \cup \mathcal{M}$ and split multiplicative reduction at each prime in $\mathcal{L} \cup \mathcal{M}$ (cf. Lemma 1 of [2] – the key point is that the number $b_2 = 1 + 32m = 2\ell - 1$ belongs to $\mathbb{Q}_p^{\times 2}$ for every $p \in \mathcal{L} \cup \mathcal{M}$, because if $p \in \mathcal{L}$ then $p \equiv 1 \pmod 4$). We may therefore use the results of Brumer-Kramer [1] to calculate the relevant Selmer groups. As in [2], we view $\mathrm{Sel}_2(A/K)$ and $\mathrm{Sel}_g(B/K)$ as subgroups

$$\mathrm{Sel}_2(A/K) \subset \prod_{\nu=1}^{3} (K^\times/K^{\times 2})$$

and

$$\mathrm{Sel}_g(B/K) \subset K^\times/K^{\times 2}.$$

The map $\pi : \mathrm{Sel}_2(A/K) \to \mathrm{Sel}_g(B/K)$ is then identified with the restriction to $\mathrm{Sel}_2(A/K)$ of the projection map

$$\begin{aligned} \prod_{\nu=1}^{3} (K^\times/K^{\times 2}) &\to K^\times/K^{\times 2} \\ [a,b,c] &\mapsto [a], \end{aligned}$$

where the square brackets denote the class modulo squares of the triple (a,b,c) or the element a. Given a finite place v of K, let $\mathcal{O}_v$ denote the ring of integers of K_v. Arguing as in Lemma 2 of [2], but omitting part (ii) of the lemma and observing that the restriction "p odd" in part (iii) is unnecessary, we find that $\mathrm{Sel}_2(A/K)$ consists of all classes $[a,b,ab]$ satisfying the following conditions:

(1) If v is finite but $v \nmid \ell m$ then $a, b \in K_v^{\times 2}\mathcal{O}_v^\times$
(2) If $v|m$ then $b \in aK_v^{\times 2}$.
(3) If $v|\ell$ then $b \in K_v^{\times 2}$.
(4) If $K_v = \mathbb{R}$ then $b \in aK_v^{\times 2}$.

In addition, the remark following the proof of Lemma 2 on p. 382 of [2] shows that $\mathrm{Sel}_g(B/K)$ consists of all classes $[a]$ such that $a \in K_v^{\times 2}\mathcal{O}_v^\times$ for finite $v \nmid \ell m$.

Now let V be the subgroup of $K^\times/K^{\times 2}$ generated by the classes $[\lambda_i^\sigma]$ for $1 \leqslant i \leqslant n$ and $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, where the λ_i are as in the lemma. Then V is contained in $\mathrm{Sel}_g(B/K)$ and the representation of $\mathrm{Gal}(K/\mathbb{Q})$ on V is isomorphic to the direct sum of n copies of the regular representation. We claim that V intersects the image of π trivially. Indeed, suppose that

$[a, b, ab] \in \mathrm{Sel}_2(A/K)$ and $[a] \in V$. After replacing a by another element of $aK^{\times 2}$, we may assume that a has the form

$$a = \prod_{\substack{1 \leqslant i \leqslant n \\ \sigma \in \mathrm{Gal}(K/\mathbb{Q})}} (\lambda_i^\sigma)^{\epsilon(i,\sigma)}$$

with $\epsilon(i, \sigma) = 0$ or 1 for all i and σ. In particular, $a \in \mathcal{O}_v^\times$ for $v|m$. Condition (2) above then implies that $b \in K_v^{\times 2}\mathcal{O}_v^\times$ for $v|m$. But by conditions (1) and (3) we also have $b \in K_v^{\times 2}\mathcal{O}_v^\times$ for finite $v \nmid m$. Hence the principal ideal generated by b is the square of an ideal of K. Therefore $b \in K_v^{\times 2}$ whenever v has the form $v = v(\mathfrak{m}_j^\tau)$ for some j and τ. For all such v condition (2) then gives $a \in K_v^{\times 2}$. It follows that $\epsilon(i, \sigma) = 0$ for all i and σ, whence $[a]$ is trivial.

Acknowledgement

The original version of this note (submitted before I was aware of Kramer's beautiful paper) pertained only to $\mathrm{Sel}_2(E/K)$, not to $Ш(E/K)_2$. My attention was drawn to [2] by the referee, for whose knowledgeable comments I am deeply grateful.

References

1. A. Brumer and K. Kramer, *The rank of elliptic curves*, Duke Math. J. **44** (1977), 715–743.
2. K. Kramer, *A family of semistable elliptic curves with large Tate-Shafarevitch groups*, Proc. AMS **89** (1983), 379–386.

Department of Mathematics, Boston University, Boston, MA 02215
E-mail address: rohrlich@math.bu.edu