Canad. J. Math. Vol. **60** (3), 2008 pp. 481–490

Heegner Points and the Rank of Elliptic Curves over Large Extensions of Global Fields

Florian Breuer and Bo-Hae Im

Abstract. Let k be a global field, $\overline{k}$ a separable closure of k, and G_k the absolute Galois group $\mathrm{Gal}(\overline{k}/k)$ of $\overline{k}$ over k. For every $\sigma \in G_k$, let $\overline{k}^{\sigma}$ be the fixed subfield of $\overline{k}$ under σ. Let E/k be an elliptic curve over k. It is known that the Mordell–Weil group $E(\overline{k}^{\sigma})$ has infinite rank. We present a new proof of this fact in the following two cases. First, when k is a global function field of odd characteristic and E is parametrized by a Drinfeld modular curve, and secondly when k is a totally real number field and E/k is parametrized by a Shimura curve. In both cases our approach uses the non-triviality of a sequence of Heegner points on E defined over ring class fields.

1 Introduction

This paper is motivated by the following result, conjectured by Michael Larsen and recently proved by him and the second-named author [12].

Theorem 1.1 *Let A/k be an abelian variety over a finitely generated infinite field k with characteristic not equal to 2. Then for every $\sigma \in G_k := \mathrm{Gal}(\overline{k}/k)$ where $\overline{k}$ is a separable closure of k, the Mordell–Weil group $A(\overline{k}^{\sigma})$ of A over $\overline{k}^{\sigma} = \{x \in \overline{k} \mid \sigma(x) = x\}$ has infinite rank.*

Prior to this result, substantial progress had been made on the case of elliptic curves of Theorem 1.1 which has covered many cases with hypothesis on rational points of A [9, 10].

In this paper, we present a different proof of this result in the case of elliptic curves with *modular parametrization* (MP), that is, elliptic curves parametrized by Shimura curves (when k is a totally real number field) or by Drinfeld modular curves (when k is a global function field). The result is stated in Theorem 6.2 below, which extends the result in [11].

Our approach is the following. Let E/k be an MP elliptic curve. Then for a given automorphism $\sigma \in G_k$, we produce an infinite sequence of distinct imaginary quadratic extensions $K_1, K_2, \dots, K_m, \dots$, of k in such a way that (E, K_m) satisfies the *Heegner hypothesis* (definitions are given below) and the rank of E over the compositum of these fields K_m's is infinite. If $\sigma|_{K_m} = \mathrm{id}_{K_m}$ for all m, then we are done. Otherwise, we fix a K in this list for which $\sigma|_K \neq \mathrm{id}_K$. Then the Heegner hypothesis allows us to construct a suitable sequence of Heegner points on E defined over

Received by the editors February 8, 2006; revised January 18, 2007.
Bo Hae Im was supported by the Korea Science and Engineering Foundation (KOSEF) grant, funded by the Korean government (MOST) No. R01-2007-000-10660-0.
AMS subject classification: 11G05.

https://doi.org/10.4153/CJM-2008-023-0 Published online by Cambridge University Press

a tower of ring class fields of K over which the rank of E is unbounded. Then we use the dihedral structure of these ring class fields to show that the rank of $E(\overline{k}^{\sigma})$ is infinite.

Note that for number fields we simplify and generalize the results of [11], using an argument from [2], and we also show that the rank of elliptic curves grows over ring class fields of global fields.

2 Elliptic Curves With Modular Parametrization

2.1 Notation

Let k denote either a totally real number field, or a global function field. In this paper, we will label the two cases with the symbols NF and FF, respectively. We first define the notion of an elliptic curve E/k with *modular parametrization* (MP), which is the object of interest in this paper. At the same time, we will fix our notation for the rest of the paper.

NF: When k is a totally real number field, we denote by $\mathcal{O}_k$ its ring of integers, with profinite completion $\hat{\mathcal{O}}_k = \mathcal{O}_k \otimes \prod_p \mathbb{Z}_p$. We denote by $\mathbb{A}_k$ the ring of adèles of k. Let $\mathfrak{n} \subset \mathcal{O}_k$ be a non-zero ideal. If $[k:\mathbb{Q}]$ is even, we further assume that $\operatorname{ord}_{\mathfrak{p}}(\mathfrak{n})$ is odd for some prime $\mathfrak{p}$.

Let f be a newform on $\mathrm{GL}_2(\mathbb{A}_k)$ of parallel weight 2, level

$$K_0(\mathfrak{n}) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix} \right) \in \mathrm{GL}_2(\hat{\mathcal{O}}_k) \mid c \in \hat{\mathfrak{n}} \right\},$$

trivial central character, and rational Hecke eigenvalues. Then by [18, Theorem B], there exists an elliptic curve E'/k of conductor $\mathfrak{n}$ such that

- the L-functions of E' and f coincide up to factors at primes dividing $\mathfrak{n}$,
- there exists a Shimura curve X/k and a surjective k-morphism $\pi'\colon X \to E'$.

If E/k is an elliptic curve which is k-isogenous to an elliptic curve E'/k arising from the above Eichler–Shimura construction, then we say that E/k has a *modular parametrization*. Composing with the isogeny, we get the parametrization $\pi\colon X \to E$. For example, all elliptic curves over $F = \mathbb{Q}$ have MP [3,16,17]. Notice, however, that not all elliptic curves over number fields have MP (even though they are conjectured to be "modular" in the sense of Langlands).

FF: When k is a global function field, suppose E/k is any elliptic curve with split multiplicative reduction at a place ∞ of k. We denote by $\mathcal{O}_k$ the ring of elements of k regular away from ∞. Then the conductor of E can be written $\mathfrak{n} \cdot \infty$, where $\mathfrak{n} \subset \mathcal{O}_k$ is an ideal.

Let $X_0(\mathfrak{n})$ be the Drinfeld modular curve parametrizing pairs of rank-2 Drinfeld $\mathcal{O}_k$-modules linked by cyclic $\mathfrak{n}$-isogenies. Then there is a morphism $\pi\colon X_0(\mathfrak{n}) \to E$ defined over k (see [7]). In this case, too, we say that E/k has MP.

If E/k is any elliptic curve with non-constant j-invariant, then there exists a finite extension L/k such that E/L is parametrized by a Drinfeld modular curve, and hence our results will apply to E/L, but this case is already covered by [14, Theorem 5].

2.2 Heegner Hypothesis

Let K/k be a quadratic imaginary extension (when k is a function field, this means that the place ∞ does not split in K/k). We denote by

$$\varepsilon = \bigotimes_{\nu} \varepsilon_\nu \colon k^\times \backslash \hat{k}^\times \longrightarrow \{\pm 1, 0\}$$

the character associated with K/k, where ν ranges over the finite places of k.

Let E/k be an MP elliptic curve. We say that the pair (E, K) satisfies the *Heegner hypothesis* if the following conditions hold:

NF: The relative discriminant of K/k is prime to $\mathfrak{n}$ and $\varepsilon(\mathfrak{n}) = (-1)^{[k:\mathbb{Q}]-1}$.
FF: All primes $\mathfrak{p}|\mathfrak{n}$ split in K/k (*i.e.*, $\varepsilon(\mathfrak{p}) = 1$ for all $\mathfrak{p}|\mathfrak{n}$).

2.3 Ring Class Fields

Let K/k be a quadratic imaginary extension, and denote by $\mathcal{O}_K$ the integral closure of $\mathcal{O}_k$ in K. Let $\mathfrak{p} \subset \mathcal{O}_k$ be a non-zero prime. For any integer $n \geq 0$, we denote by $K[\mathfrak{p}^n]$ the ring class field of K of conductor $\mathfrak{p}^n$ (*i.e.*, the class field associated with the order $\mathcal{O}_n := \mathcal{O}_k + \mathfrak{p}^n \mathcal{O}_K$). We also denote $K[\mathfrak{p}^\infty] := \cup_{n \geq 0} K[\mathfrak{p}^n]$.

3 Torsion and Rank

In this section, we gather some useful results on the Mordell–Weil groups of elliptic curves.

Lemma 3.1 *Let E/k be an elliptic curve, K/k a quadratic imaginary extension, and $\mathfrak{p} \subset \mathcal{O}_k$ a prime. Then $E(K[\mathfrak{p}^\infty])_{\mathrm{tors}}$ is a finite group.*

Proof When k is a function field, this is shown in [1, Lemma 2.2], and when k is a number field, it is even easier to show. One just considers the reduction of E at two distinct primes which are inert in K/k and at which E has good reduction. ■

Lemma 3.2 *Let E/k be an elliptic curve. Then for any integer $d > 1$, the set*

$$\bigcup_{[L:k] \leq d} E(L)_{\mathrm{tors}} \text{ is finite.}$$

Proof See [8, Proposition 1.1]. ■

Let G be an abelian group. We say that G has infinite rank if $\dim_{\mathbb{Q}}(G \otimes \mathbb{Q}) = \infty$.

Lemma 3.3 *Let E/k be an elliptic curve and L/k a Galois extension over k. Let $\{P_m\}_{m=1}^{\infty}$ be a sequence of points in $E(L)$. Denote by $\mathcal{S}$ the subgroup of $E(L)$ generated by the P_m. Suppose that*

(i) *$E(L)_{\mathrm{tors}}$ is finite,*
(ii) *$\mathcal{S}$ is not finitely generated.*

Then $\mathcal{S}$, and thus also $E(L)$, has infinite rank.

Proof [11, Lemma 2.5] can be generalized to the Mordell–Weil groups over global fields. ■

https://doi.org/10.4153/CJM-2008-023-0 Published online by Cambridge University Press

4 Heegner Points

In this section, we construct a sequence of Heegner points on MP elliptic curves which generate a group of infinite rank. Let E/k be an MP elliptic curve with conductor $\mathfrak{n}$ (or rather $\mathfrak{n}\cdot\infty$ if k is a function field). Let K/k be a quadratic imaginary extension, and suppose that (E, K) satisfies the Heegner hypothesis.

Let $\mathfrak{p} \subset \mathcal{O}_k$ be a non-zero prime satisfying the following.

NF: $\mathfrak{p} \nmid 2\mathfrak{n}$ and $\varepsilon(\mathfrak{p}) = 1$.
FF: $\mathfrak{p} \nmid \mathfrak{n}$.

Since the constructions of Heegner points in the number field case and the function field case are somewhat different, we treat them in separate subsections.

4.1 Number Fields

We first construct a suitable Shimura curve parametrizing E: $\pi\colon X \to E$. Our standard reference is Zhang [18].

Fix a real place τ of k. Then there exists a unique quaternion algebra B over k which is non-split precisely at all archimedean places other than τ and at all the finite places ν with $\varepsilon_\nu(\mathfrak{n}) = -1$ (the number of such places is even, because we are assuming the Heegner hypothesis). We fix an embedding $\rho\colon K \hookrightarrow B$.

Let $R \subset B$ be an order of type $(\mathfrak{n}, K)$, in other words R contains $\rho(\mathcal{O}_K)$ and has conductor $\mathfrak{n}$. Then the Shimura curve X/k corresponds to the Riemann surface

$$X(\mathbb{C}) \cong B_+\backslash\mathbb{H} \times \hat{B}^\times/\hat{k}^\times\hat{R}^\times \cup \{\text{cusps}\},$$

where B_+ denotes the elements of B of totally positive reduced norm, $\mathbb{H}$ denotes the complex upper half-plane, and $\{\text{cusps}\}$ is a finite set, which is non-empty only in the case where $k = \mathbb{Q}$ and $X = X_0(\mathfrak{n})$.

For the construction of Heegner points it is more convenient to work with the Shimura curve Y corresponding to the Riemann surface

$$Y(\mathbb{C}) \cong B^\times\backslash\mathbb{H}^\pm \times \hat{B}^\times/\hat{R}^\times \cup \{\text{cusps}\},$$

of which X is a quotient by the action of $\hat{k}^\times$.

A point $z \in Y(\mathbb{C})$ is called a *CM point* if it is represented by an element of $\mathbb{H}^\pm \times \hat{B}$ of the form $(\sqrt{-1}, g)$. We associate the morphism $\phi_z = g^{-1}\rho g\colon K \to \hat{B}$ with a CM point z. The order $\operatorname{End}(z) := \phi_z^{-1}(\hat{R})$ in K is called the *endomorphism ring* of z, and does not depend on the choice of g. It is of the form $\operatorname{End}(z) = \mathcal{O}_k + \mathfrak{c}\,\mathcal{O}_K$, for an ideal $\mathfrak{c} \subset \mathcal{O}_k$ called the *conductor* of z.

Denote by $k_\mathfrak{p}$ the completion of k at $\mathfrak{p}$ with uniformizer ϖ. Then B splits at $\mathfrak{p}$, and we choose an isomorphism $B \otimes k_\mathfrak{p} \cong M_2(k_\mathfrak{p})$ such that $\rho(\sqrt{-d}) \otimes 1$ in $\rho(K) \otimes k_\mathfrak{p}$ corresponds to the matrix $\left(\begin{smallmatrix} 0 & -1 \\ d & 0 \end{smallmatrix}\right) \in M_2(k_\mathfrak{p})$, where $K = k(\sqrt{-d})$, $d \in \mathcal{O}_k$.

Now let $P \in \hat{B}^\times$ be the element with $\mathfrak{p}$-component $\left(\begin{smallmatrix} \varpi & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and all other components equal to 1. Let z_n be the CM point in $Y(\mathbb{C})$ corresponding to

$$(\sqrt{-1}, P^n) \in \mathbb{H}^\pm \times \hat{B}^\times.$$

As $\mathfrak{p} \nmid 2\mathfrak{n}$ we see that z_n has conductor $\mathfrak{p}^n$, *i.e.*, $\operatorname{End}(z_n) = \mathcal{O}_n = \mathcal{O}_k + \mathfrak{p}^n\mathcal{O}_K$.

Denote by $x_n \in X(\mathbb{C})$ and $y_n \in E(\mathbb{C})$ the respective images of $z_n \in Y(\mathbb{C})$ under the maps $Y \to X \xrightarrow{\pi} E$. We call the points y_n *Heegner points* (in contrast, Zhang only uses the term Heegner points for CM points with trivial conductor). Moreover, the points x_n, and thus also y_n, are defined over $K[\mathfrak{p}^n]$. In fact, by [18, §2.1.1] the set X_n of (positively oriented) CM points on X with conductor $\mathfrak{p}^n$ is in bijection with $K^\times\backslash\hat{K}^\times/\hat{\mathcal{O}}_n^\times \cong \operatorname{Pic}(\mathcal{O}_n)$, with the action by $\operatorname{Gal}(K[\mathfrak{p}^n]/K)$ given by class field theory.

Notice that the Shimura curves X and Y depend on the choice of K, but the elliptic curve E parametrized by them remains the same up to k-isogeny, by Faltings' isogeny theorem [5, §5, Korollar 2], since their L-functions coincide up to finitely many local factors with the L-function of the newform f.

4.2 Function Fields

We now consider the case where k is a global function field and $\pi\colon X_0(\mathfrak{n}) \to E$ is a modular parametrization. Since we are assuming the Heegner hypothesis, there exists an ideal $\mathfrak{N} \subset \mathcal{O}_K$ such that $\mathcal{O}_K/\mathfrak{N} \cong \mathcal{O}_k/\mathfrak{n}$. For every integer $n \geq 0$, we let $\mathfrak{N}_n = \mathfrak{N} \cap \mathcal{O}_n$, where we recall $\mathcal{O}_n = \mathcal{O}_k + \mathfrak{p}^n\mathcal{O}_K$. Then we have $\mathcal{O}_K/\mathfrak{N}_n \cong \mathcal{O}_k/\mathfrak{n}$ for all n.

Denote by $\mathbb{C}_\infty = \hat{\bar{k}}_\infty$ the completion of an algebraic closure of the completion of k at ∞, a field both algebraically closed and complete. Then $\mathcal{O}_K$ and $\mathfrak{N}_n^{-1}$ are rank-2 $\mathcal{O}_k$-lattices in $\mathbb{C}_\infty$, hence define a pair of Drinfeld modules $(\Phi^{\mathcal{O}_K}, \Phi^{\mathcal{N}_n^{-1}})$ linked by a cyclic $\mathfrak{n}$-isogeny. The pair thus defines a point x_n on $X_0(\mathfrak{n})$, which is defined over the ring class field $K[\mathfrak{p}^n]$ by the theory of complex multiplication. Its image $y_n = \phi(x_n) \in E(K[\mathfrak{p}^n])$ is called a *Heegner point* on E.

4.3 Infinite Rank over a Tower of Ring Class Fields

We have constructed our Heegner points over ring class fields. Now we show that they generate a subgroup of infinite rank.

Proposition 4.1 *Let $I \subset \mathbb{N}$ be an infinite set. Then the subgroup of $E(K[\mathfrak{p}^\infty])$ generated by $\{y_n \mid n \in I\}$ has finite torsion and infinite rank,* i.e., *the rank of $E(K[\mathfrak{p}^n])$ is unbounded as n goes to infinity.*

Proof By Lemmas 3.1 and 3.3, we need only to establish that the subgroup $\mathcal{S} \subset E(K[\mathfrak{p}^\infty])$ generated by the y_n's is not finitely generated. For this we adopt the argument of [2].

Suppose that $\mathcal{S}$ is finitely generated. Then $\mathcal{S} \subset E(L)$ for some finite separable extension L/k, which we may extend to include K. Denote by $G_L = \operatorname{Gal}(\bar{L}/L)$ the absolute Galois group of L. Then G_L acts on the fibers $\pi^{-1}(y_n)$, and the G_L-orbit of x_n is bounded: $\#(G_L \cdot x_n) \leq \deg(\pi)$.

On the other hand, $\#(G_L \cdot x_n) \geq \#\operatorname{Pic}(\mathcal{O}_n)/[L{:}K]$. But $\#\operatorname{Pic}(\mathcal{O}_n)$ is unbounded, as can be seen from the exact sequence [15, §I.12]

$$1 \to \mathcal{O}_K^\times/\mathcal{O}_n^\times \longrightarrow (\mathcal{O}_K/\mathfrak{p}^n\mathcal{O}_K)^\times/(\mathcal{O}_n/\mathfrak{p}^n\mathcal{O}_n)^\times \longrightarrow \operatorname{Pic}(\mathcal{O}_n) \longrightarrow \operatorname{Pic}(\mathcal{O}_K) \to 1.$$

■

5 Some Algebraic Lemmas

In this section, we collect some lemmas that we will need in the proof of the main result. We start off with two group-theoretic results.

Proposition 5.1 *Let k be global field and K/k a quadratic imaginary extension. Let $\mathfrak{p} \subset \mathcal{O}_k$ be a non-zero prime. Then for every positive integer n, $\operatorname{Gal}(K[\mathfrak{p}^n]/k)$ is a dihedral group and $\operatorname{Gal}(K[\mathfrak{p}^n]/K[\mathfrak{p}])$ is an abelian p-group, where $\mathfrak{p}|p$ (resp. $p = \operatorname{char} k$) when k is a number field (resp. global function field).*

Proof See [4, (2.3.12); Proposition 2.5.7] for the function field case, and we generalize the result in [11, Lemma 2.3], which is elementary class field theory, in the number field case. ■

Lemma 5.2 *Let G be a generalized dihedral group acting on a vector space M, and suppose that the reflection $\sigma \in G$ acts by $\pm \operatorname{id}$ on M. Let $H < G$ be an abelian subgroup of odd order. Then H acts trivially on M.*

Proof We have $\sigma\tau\sigma = \tau^{-1}$, for all $\tau \in G$. Denote by $\rho\colon G \to \mathrm{GL}(M)$ the representation, so $\rho(\sigma) = \pm \operatorname{id}$, and let $\tau \in H$. Then

$$\rho(\tau^2) = \rho(\tau)\rho(\tau) = (\pm \operatorname{id})\rho(\tau)(\pm \operatorname{id})\rho(\tau) = \rho(\sigma\tau\sigma\tau) = \operatorname{id}.$$

Since H has odd order, we have $\langle\tau\rangle = \langle\tau^2\rangle$, hence τ also acts trivially on M. ■

Lemma 5.3 *Let k be a number field with ring of integers $\mathcal{O}_k$. Let $d \in \mathcal{O}_k$, and suppose d is not a square modulo 4. Let $K = k(\sqrt{d})$. Then we have the following.*

(i) *The ring of integers of K is $\mathcal{O}_K = \mathcal{O}_k[\sqrt{d}]$.*
(ii) *Let $\mathfrak{p} \subset \mathcal{O}_k$ be a non-zero prime not lying above 2. Then $\mathfrak{p}$ is inert (resp. split, resp. ramified) in K/k if and only if d is non-square (resp. a non-zero square, resp. zero) modulo $\mathfrak{p}$.*

Proof To prove (i), note that we have $\mathcal{O}_K = \mathcal{O}_k[\omega]$ for some $\omega \in \mathcal{O}_K$ satisfying an equation of the form $\omega^2 - b\omega - c = 0$, $b, c \in \mathcal{O}_k$. Thus $\omega = \frac{1}{2}(b \pm \sqrt{b^2 + 4c})$. Now if $\mathcal{O}_k[\sqrt{d}] \subsetneq \mathcal{O}_k[\omega]$, then we must have $\frac{1}{2}\sqrt{b^2 + 4c} = \frac{1}{2}\sqrt{d}$, in which case $d = b^2 + 4c$ is a square modulo 4.

Now part (ii) follows since the splitting behavior of $\mathfrak{p}$ in K/k is given by the splitting behavior of the polynomial $x^2 - d$ modulo $\mathfrak{p}$. ■

Lemma 5.4 *Let k be a totally real number field with real embeddings τ_j for $j = 1, \dots, n$. Then if $a \in k$ such that $\tau_j(a) < 0$ for all j, the field $k(\sqrt{a})$ is a totally imaginary quadratic extension over k.*

Proof Elementary. ■

Suppose k is a field, and $g(x, y) \in k[x, y]$. Then we denote by

$$H_k(g) := \{\alpha \in k \mid g(\alpha, y) \in k[y] \text{ is irreducible over } k\}$$

the Hilbert set of g over k. Notice that by [13, Ch. 9, Theorem 4.2] every global field is Hilbertian.

Lemma 5.5 *Let L be a field extension of a global field k and $\mathcal{O}_k$ the ring of integers in k. Let $g \in k[x,y]$ be irreducible over L. Then we have the following.*

(i) *If L is a finite separable extension of k, then $H_L(g) \cap \mathcal{O}_k$ is infinite. Moreover, if $k = \mathbb{Q}$, then $H_L(f) \cap \mathbb{Q}$ is dense in $\mathbb{Q}$.*

(ii) *If L is any non-abelian extension of k, and if g is quadratic in y, then $H_L(g) \cap \mathcal{O}_k$ is infinite.*

Proof For (i), the first assertion follows from [13, Ch. 9, Proposition 3.3] and [6, Proposition 13.4.1], and the second from [13, Ch. 9, Corollary 2.5].

For (ii), let M be the maximal abelian extension of a global field k in L. Then $M \subsetneqq L$, and since k is Hilbertian, M is also a Hilbertian field by [6, Theorem 16.11.3]. So $H_M(g)$ is infinite. By applying [6, Proposition 16.11.1], $H_M(g)$ contains a Hilbert set H over a subfield N which is a finite abelian extension of k. So by (i), $H \cap \mathcal{O}_k$ is infinite, so $H_M(g) \cap \mathcal{O}_k$ is infinite. So we get an infinite sequence of elements $\{m_i\}_{i\geq 1}$ in $H_M(g) \cap \mathcal{O}_k$. For each $i \geq 1$, let α_i be an element in an algebraic closure of k such that $g(m_i, \alpha_i) = 0$. Then by the Hilbertian property, $k(\alpha_i)$ and $M(\alpha_i)$ are quadratic extensions of k and M respectively since g is quadratic in y, and $k(\alpha_i)$ and M are linearly disjoint over k. Then by [6, Lemma 2.5.6],

$$\mathrm{Gal}(M(\alpha_i)/k) \cong \mathrm{Gal}(M/k) \times \mathrm{Gal}(k(\alpha_i)/k) \cong \mathrm{Gal}(M/k) \times \mathbb{Z}/2\mathbb{Z},$$

which is abelian. So $M(\alpha_i)$ is an abelian extension of k. By the maximality of M in L, $M(\alpha_i) \not\subseteq L$. Therefore, $m_i \in H_L(g) \cap \mathcal{O}_k$ for all i. ∎

6 Proof of the Main Results

Proposition 6.1 *Let k be a totally real number field or a global function field of odd characteristic p. Let K/k be a quadratic imaginary extension, and let E/k be an MP elliptic curve such that (E,K) satisfies the Heegner hypothesis (§2.2). Let $\mathfrak{p} \subset \mathcal{O}_k$ be a prime satisfying the conditions in Section 4. Let $\sigma \in G_k$ be uch that $\sigma|K \neq \mathrm{id}_K$.*

Then the rank of $E(K[\mathfrak{p}]^\sigma)$ is unbounded as $n \to \infty$. In particular, $E(K_{\mathrm{ab}}^\sigma)$ has infinite rank, where K_{ab} denotes the maximal abelian extension of K.

Proof For the given $\sigma \in G_k$, let $\sigma_n = \sigma|_{K[\mathfrak{p}^n]}$ denote the restriction to $K[\mathfrak{p}^n]$. Since $\sigma|_K \neq \mathrm{id}_K$, σ_n is a reflection of the dihedral group $\mathrm{Gal}(K[\mathfrak{p}^n]/k)$.

Suppose that the rank of $E(K[\mathfrak{p}^n]^\sigma)$ is bounded. Then there exists an integer n_0 such that σ_n acts by $-\mathrm{id}$ on $M_n := E(K[\mathfrak{p}^n]) \otimes \mathbb{Q}/E(K[\mathfrak{p}^{n_0}]) \otimes \mathbb{Q}$ for every $n > n_0$. Now $\mathrm{Gal}(K[\mathfrak{p}^n]/k)$ acts on M_n, and $H = \mathrm{Gal}(K[\mathfrak{p}^n]/K[\mathfrak{p}^{n_0}])$ is an abelian subgroup of odd order (since p is assumed to be odd), hence acts trivially by Lemma 5.2.

It follows that

$$E(K[\mathfrak{p}^n]) \otimes \mathbb{Q} = \big(E(K[\mathfrak{p}^n]) \otimes \mathbb{Q}\big)^H = E(K[\mathfrak{p}^{n_0}]) \otimes \mathbb{Q},$$

which contradicts the unboundedness of the rank of $E(K[\mathfrak{p}^n])$ (Proposition 4.1). ∎

We are now ready to prove our main result.

Theorem 6.2 *Let k be a totally real number field or a global function field of odd characteristic. Let E/k be an MP elliptic curve of conductor $\mathfrak{n}$ (resp. $\mathfrak{n} \cdot \infty$). If k is a number field of even degree over $\mathbb{Q}$, we further assume that $\operatorname{ord}_{\mathfrak{q}}(\mathfrak{n})$ is odd for some prime $\mathfrak{q} \nmid 2$ of k. Then, for all $\sigma \in G_k$, the rank of $E(\bar{k}^{\sigma})$ is infinite.*

Proof Since the characteristic of k is not 2, we may choose a Weierstrass equation for E/k of the form $y^2 = x^3 + ax^2 + bx + c$. By a change of variables, we may assume that a, b and c are in $\mathcal{O}_k$.

Our aim is to construct a sequence of quadratic imaginary extensions K_i/k which are linearly disjoint over k, and such that (E, K_i) satisfies the Heegner hypothesis for each i.

Consider the polynomial

$$f(x) := (\alpha + Nx)^3 + aN^2(\alpha + Nx)^2 + bN^4(\alpha + Nx) + cN^6 \quad \in \mathcal{O}_k[x],$$

with $\alpha \in \mathcal{O}_k$ and $0 \neq N \in \mathfrak{n}$ chosen as follows:

NF: α is non-square modulo 4. If $[k:\mathbb{Q}]$ is even, we choose a prime $\mathfrak{q} \nmid 2$ with $\operatorname{ord}_{\mathfrak{q}}(\mathfrak{n})$ odd, and require that α be non-square modulo this $\mathfrak{q}$. For all other $\mathfrak{p}|\mathfrak{n}$, $\mathfrak{p} \neq \mathfrak{q}$, we require that α be square modulo $\mathfrak{p}$. Such $\alpha \in \mathcal{O}_k$ exists by the Chinese Remainder Theorem. We choose $N \in 4\mathfrak{n}$ totally negative.

FF: $\alpha = 1$, $N \in \mathfrak{n}$ is any non-zero element.

Let $K_0 = k$ and $K_i = k(\sqrt{f(m_i)})$, for $i \geq 1$, where the m_i's are constructed recursively as follows.

NF: Since N is totally negative, we see that there exists $r > 0$ such that $f(x)$ is totally negative for all $x \in \mathbb{Q}$, $x > r$. Now for $i \geq 0$, we choose

$$m_{i+1} \in H_{K_0 \cdots K_i}(y^2 - f(x)) \cap \mathbb{Z}, \quad m_i > r.$$

This is possible by Lemma 5.5(i). Since $f(m_i)$ is totally negative, it follows that K_i is a quadratic imaginary extension of k. Furthermore, since $f(m_i) \equiv \alpha^3 \bmod 4\mathfrak{n}$, we find that (E, K_i) satisfies the Heegner hypothesis by Lemma 5.3.

FF: Denote by k_∞ the completion of k at ∞. By Lemma 5.5(ii), we may find $m_1 \in H_{k_\infty}(y^2 - f(x)) \cap \mathcal{O}_k$, so $f(m_1)$ is neither a square in k_∞ nor in k. We let $K_1 = k(\sqrt{f(m_1)})$, and recursively construct $K_i = k(\sqrt{f(m_i)})$ with $m_{i+1} \in H_{k_\infty K_1 K_2 \cdots K_i}(y^2 - f(x))$ by applying Lemma 5.5(ii).

For every i, we see that K_i/k is quadratic imaginary. Furthermore $f(m_i) \equiv 1 \bmod \mathfrak{n}$, so that every $\mathfrak{p}|\mathfrak{n}$ splits in K_i/k, so (E, K_i) satisfies the Heegner hypothesis.

Let $\sigma \in G_k$. Then either $\sigma|_{K_i} = \mathrm{id}_{K_i}$ for all i, or $\sigma|_{K_i} \neq \mathrm{id}_{K_i}$ for some i.

First, suppose that for all i, $\sigma|_{K_i} = \mathrm{id}_{K_i}$. Then, for each i, consider the element $\frac{\alpha + Nm_i}{N^2} \in k$. By plugging this into the given Weierstrass equation of E/k, we get

$$y^2 = \Big(\frac{\alpha + Nm_i}{N^2}\Big)^3 + a\Big(\frac{1 + Nm_i}{N^2}\Big)^2 + b\Big(\frac{1 + Nm_i}{N^2}\Big) + c = \frac{f(m_i)}{N^6}.$$

Hence, if we let

$$P_i = \Big(\frac{\alpha + Nm_i}{N^2}, \frac{\sqrt{f(m_i)}}{N^3}\Big),$$

then P_i is a point in $E(K_i)$ but it is not in $E(k)$. And moreover, since $K_i = K_i^\sigma$, P_i is fixed under σ.

So we get an infinite sequence $\{P_i\}_{i=1}^{\infty}$ of points in $E(\overline{k}^\sigma)$ such that each P_i is defined over the imaginary quadratic extension K_i over k. We may assume that these points P_i are not torsion points by Lemma 3.2. Now we show the points P_i are linearly independent. Suppose that they are dependent. Then for some integers a_j,

$$(*) \qquad a_1P_1 + a_2P_2 + \cdots + a_rP_r = O.$$

Since the fields K_i are pairwise linearly disjoint over k, for each i, there is an automorphism of $\overline{k}$ which fixes all but one K_i of $K_1, \dots, K_r$. Note that such an automorphism takes P_i to its inverse, $-P_i$. Applying this automorphism to $(*)$, we get

$$a_1P_1 + \cdots + a_{i-1}P_{i-1} - a_iP_i + \cdots + a_rP_r = O.$$

By subtracting this from $(*)$, we get $2a_iP_i = O$, which implies $a_i = 0$ since the characteristic p of k is not 2 and P_i is not a torsion point. We conclude that the $P_i \in E(\overline{k})$ are linearly independent. Moreover, P_i are defined over the composite field of all quadratic field extensions of k, which is an abelian extension of k. Hence, the rank of E over the maximal abelian extension of k in $\overline{k}^\sigma$ is infinite, so the rank of $E(\overline{k}^\sigma)$ is infinite.

Next, suppose that there is an integer i such that $\sigma|_{K_i} \neq \mathrm{id}_{K_i}$. Then fix such a quadratic imaginary extension K_i. Our construction shows that K_i satisfies the hypothesis of Proposition 6.1, so we complete the proof of this case as a consequence of Proposition 6.1. ■

Acknowledgements We would like to thank Henri Darmon for his encouragement and for suggesting the case of totally real fields. Also we would like to thank Michael Larsen for his interest in our result and his encouragement. Lastly, we are grateful to the referee, whose comments led to a significant improvement in the presentation of this manuscript.

References

[1] F. Breuer, *Higher Heegner points on elliptic curves over function fields.* J. Number Theory **104**(2004), no. 2, 315–326.

[2] ———, *Images of isogeny classes on modular elliptic curves.* Math. Res. Lett. **11**(2004), no. 5-6, 649–651.

[3] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, *On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises.* J. Amer. Math. Soc. **14**(2001), no. 4, 843–939.

[4] M. L. Brown, *Heegner Modules and Elliptic Curves*, Lecture Notes in Mathematics 1849, Springer-Verlag, Berlin, 2000.

[5] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern.* Invent. Math. **73**(1983), no. 3, 349–366.

[6] M. Fried and M. Jarden, *Field Arithmetic.* Second edition. Ergebnisse der Mathematik und ihrer Grenzgebiete 11, Springer-Verlag, Berlin, 2005.

[7] E.-U. Gekeler and M. Reversat, *Jacobians of Drinfeld modular curves.* J. Reine Angew. Math. **476**(1996), 27–93.

[8] W.-D. Geyer and M. Jarden, *The rank of abelian varieties over large algebraic fields.* Arch. Math. (Basel) **86**(2006), no. 3, 211–216.

[9] B. Im, *Mordell–Weil groups and the rank of elliptic curves over large fields.* Canad. J. Math. **58**(2006), no. 4 (2006), 796–819.
[10] ———, *The rank of elliptic curves with 2-torsion points over large fields. Proc. Amer. Math. Soc.* **134**(2006), no. 6, 1623–1630.
[11] ———, *Heegner points and the rank of elliptic curves over large fields.* Trans. Amer. Math. Soc. **359**(2007), no. 12, 6143–6154.
[12] B. Im and M. Larsen, *Abelian varieties over cyclic fields.* To appear in Amer. J. Math.
[13] S. Lang, *Fundamentals of Diophantine Geometry.* Springer-Verlag, New York, 1983.
[14] M. Larsen, *Rank of elliptic curves over almost algebraically closed fields.* Bull. London Math. Soc. **35**(2003), no. 6, 817–820.
[15] J. Neukirch, "Algebraische Zahlentheorie", Springer-Verlag, Berlin, 1992.
[16] R. Taylor and A. Wiles, *Ring-theoretic properties of certain Hecke algebras.* Ann. of Math. **141**(1995), no. 3, 553–572.
[17] A. Wiles, *Modular elliptic curves and Fermat's last theorem.* Ann. of Math. **141**(1995), no. 3, 443–551.
[18] S. Zhang, *Heights of Heegner points on Shimura curves.* Ann. of Math. **153**(2001), no. 1, 27–147.

Department of Mathematical Sciences, University of Stellenbosch, Stellenbosch 7600, South Africa
e-mail: fbreuer@sun.ac.za

Department of Mathematics, Chung-Ang University, 221 Haukseok-dong, Dongjak-gu, Seoul 156-756, South Korea
e-mail: imbh@cau.ac.kr

https://doi.org/10.4153/CJM-2008-023-0 Published online by Cambridge University Press