TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 359, Number 12, December 2007, Pages 6143–6154
S 0002-9947(07)04364-4
Article electronically published on June 4, 2007

HEEGNER POINTS AND MORDELL-WEIL GROUPS OF ELLIPTIC CURVES OVER LARGE FIELDS

BO-HAE IM

ABSTRACT. Let $E/\mathbb{Q}$ be an elliptic curve defined over $\mathbb{Q}$ of conductor N and let $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ be the absolute Galois group of an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$. For an automorphism $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, we let $\overline{\mathbb{Q}}^{\sigma}$ be the fixed subfield of $\overline{\mathbb{Q}}$ under σ. We prove that for every $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, the Mordell-Weil group of E over the maximal Galois extension of $\mathbb{Q}$ contained in $\overline{\mathbb{Q}}^{\sigma}$ has infinite rank, so the rank of $E(\overline{\mathbb{Q}}^{\sigma})$ is infinite. Our approach uses the modularity of $E/\mathbb{Q}$ and a collection of algebraic points on E – the so-called *Heegner points* – arising from the theory of complex multiplication. In particular, we show that for some integer r and for a prime p prime to rN, the rank of E over all the ring class fields of a conductor of the form rp^n is unbounded, as n goes to infinity.

This paper is motivated by the following conjecture of M. Larsen [8]:

Conjecture. *Let K be a number field and E/K an elliptic curve over K. Then, for every $\sigma \in \mathrm{Gal}(\overline{K}/K)$, the Mordell-Weil group $E(\overline{K}^{\sigma})$ of E over $\overline{K}^{\sigma} = \{x \in \overline{K} \mid \sigma(x) = x\}$ has infinite rank.*

In [3] and [4], we have proved this conjecture in certain cases:
For a number field K and an elliptic curve E/K over K,

- if E/K has a K-rational point P such that $2P \neq O$ and $3P \neq O$, or
- if 2-torsion points of E/K are K-rational,

then for every automorphism $\sigma \in \mathrm{Gal}(\overline{K}/K)$, the rank of the Mordell-Weil group $E(\overline{K}^{\sigma})$ is infinite.

Recall that a field L is said to be PAC (*pseudo algebraically closed*) if every absolutely irreducible nonempty variety defined over L has an L-rational point. We note that if K is a countable separably Hilbertian field, then M. Jarden has proven in [6, Theorem 2.7] that for almost all $\sigma \in \mathrm{Gal}(\overline{K}/K)$ in the sense of Haar measure on $\mathrm{Gal}(\overline{K}/K)$, the maximal Galois extension contained in $\overline{K}^{\sigma}$ is a PAC field with the absolute Galois group isomorphic to the free profinite group on countably many generators, so the maximal Galois extension of K in $\overline{K}^{\sigma}$ is smaller than $\overline{K}^{\sigma}$ for almost all σ. In [3], we have shown that under the first assumption above, the Mordell-Weil group of E over the maximal Galois extension of K in $\overline{K}^{\sigma}$ for every $\sigma \in \mathrm{Gal}(\overline{K}/K)$ has infinite rank, and under the second assumption, we have shown a stronger result in [4] that the rank of E over the maximal abelian extension of K in $\overline{K}^{\sigma}$ (hence, over the maximal Galois extension of K in $\overline{K}^{\sigma}$) is infinite.

Received by the editors August 4, 2004 and, in revised form, April 25, 2006.
2000 *Mathematics Subject Classification.* Primary 11G05.

In this paper, we prove that the conjecture is true for elliptic curves over $\mathbb{Q}$ without any hypothesis on rational points of $E/\mathbb{Q}$, *i.e.* if $E/\mathbb{Q}$ is an elliptic curve over $\mathbb{Q}$, then for every automorphism $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, the Mordell-Weil group of E over the maximal Galois extension of $\mathbb{Q}$ contained in the fixed subfield $\overline{\mathbb{Q}}^{\sigma}$ under σ has infinite rank, so the rank of $E(\overline{\mathbb{Q}}^{\sigma})$ is infinite.

To prove the conjecture for a given E/K, ultimately one must find an infinite supply of rational points of E over finite extensions of K contained in $\overline{K}^{\sigma}$. In [3] and [4], we constructed such points using Diophantine geometry, essentially by searching for sufficiently rational subvarieties of the quotients of the n-fold product E^n of E by certain finite groups.

Here we use a completely different approach, coming from arithmetic: taking advantage of the modularity of elliptic curves over $\mathbb{Q}$, we choose our rational points on E to be algebraic points over ring class fields – the so-called *Heegner points*.

The main strategy is as follows: for a given automorphism $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, we produce a specially designed infinite sequence $K_m \neq \mathrm{End}(E) \otimes \mathbb{Q}$ of imaginary quadratic extensions of $\mathbb{Q}$ such that

(1) if $\sigma|_{K_m} = id_{K_m}$ for all m, then we may show using "elementary" arguments that the rank of $E(\overline{\mathbb{Q}}^{\sigma})$ is infinite and
(2) if $\sigma|_{K_m} \neq id_{K_m}$ for some m, then (E, K_m) satisfies *the Heegner hypothesis* (the definition is given in Section 2) and we show that the rank of E over the fixed subfields under σ of the ring class fields over K_m is unbounded as the ring class fields get larger. Hence the rank of $E(\overline{\mathbb{Q}}^{\sigma})$ is infinite. Here we use the norm compatibility properties of Heegner points and a generalized dihedral group structure of the Galois groups of ring class fields over $\mathbb{Q}$.

1. The main theorem

In this section, we introduce the main theorem. First, we will need the following Hilbert irreducibility and the denseness of Hilbert sets in any open intervals of $\mathbb{R}$.

Let $f \in K(t_1, \ldots, t_m)[X_1, \ldots, X_n]$ be a polynomial with coefficients in the quotient field $K(t_1, \ldots, t_m)$ of $K[t_1, \ldots, t_m]$ which is irreducible over $K(t_1, \ldots, t_m)$. We define

$$H_K(f) = \{(a_1, \ldots, a_m) \in K^m : f(a_1, \ldots, a_m, X_1, \ldots, X_n) \text{ is irreducible over } K\}$$

to be the Hilbert set of f over K. If for every $m \geq 1$, any intersections of a finite number of Hilbert sets with a finite number of nonempty Zariski open subsets in K^m are not empty (in fact, they are infinite), a field K is called *a Hilbertian field*.

Lemma 1.1. *Let L be a finite separable extension of a Hilbertian field K and let f be a polynomial in $L(t_1, \ldots, t_m)[X_1, \ldots, X_n]$ which is irreducible over the quotient field $L(t_1, \ldots, t_m)$. Then, there exists a polynomial $p \in K[t_1, \ldots, t_m, X_1, \ldots, X_n]$ such that p is irreducible over $K(t_1, \ldots, t_m)$ and $H_K(p) \subseteq H_L(f)$.*

Proof. For a given irreducible polynomial $f \in L(t_1, \ldots, t_m)[X_1, \ldots, X_n]$, by [5, Ch.11, Lemma 11.6], there is an irreducible polynomial

$$q \in K(t_1, \ldots, t_m)[X_1, \ldots, X_n]$$

such that $H_K(q) \subseteq H_L(f)$. By [5, Ch.11, Lemma 11.1], there is an irreducible polynomial $p \in K[t_1, \ldots, t_m, X_1, \ldots, X_n]$ which is irreducible over $K(t_1, \ldots, t_m)$ such that $H_K(p) \subseteq H_K(q)$. Hence the Hilbert set $H_L(f)$ of f over L contains the Hilbert set $H_K(p)$ of p over K. □

Lemma 1.2. *Let K be a number field and $\tau_1, \ldots, \tau_m$ be a family of real embeddings of K. For $i = 1, 2, \ldots, k$, let $f_i(x, y) \in K[x, y]$ be an irreducible polynomial over $K(x)$. Let $H_K(f_i) = \{\alpha \in K : f_i(\alpha, y) \in K[y]$ is irreducible over $K\}$ be the Hilbert set of f_i over K. Then for any open interval I in $\mathbb{R}$,*

$$\left(\bigcap_{i=1}^{k} H_K(f_i)\right) \cap \left(\bigcap_{j=1}^{m} \tau_j^{-1}(I)\right) \neq \emptyset.$$

Proof. Since K is a finite separable extension of $\mathbb{Q}$, by Lemma 1.1, there exist irreducible polynomials $F_i(x, y) \in \mathbb{Q}[x, y]$ such that for each $i = 1, 2, \ldots, k$, the Hilbert set $H_{\mathbb{Q}}(F_i)$ of F_i over $\mathbb{Q}$ is contained in the Hilbert set $H_K(f_i)$ of f_i over K.

Let I be an open interval in $\mathbb{R}$. Since $\bigcap_{i=1}^{k} H_{\mathbb{Q}}(F_i)$ is dense in $\mathbb{Q}$ by [7, Chapter 9, Corollary 2.5], and $\mathbb{Q}$ is dense in $\mathbb{R}$, $\left(\bigcap_{i=1}^{k} H_{\mathbb{Q}}(F_i)\right) \cap I$ is not empty. Hence there is $\beta \in \left(\bigcap_{i=1}^{k} H_{\mathbb{Q}}(F_i)\right) \cap I$. Since $\bigcap_{i=1}^{k} H_{\mathbb{Q}}(F_i) \subseteq \bigcap_{i=1}^{k} H_K(f_i)$, we have $\beta \in \bigcap_{i=1}^{k} H_K(f_i)$. On the other hand, for each real embedding τ_j of K, we have $\tau_j|_{\mathbb{Q}} = id_{\mathbb{Q}}$. Hence for all $j = 1, 2, \ldots, m$, $\tau_j(\beta) = \beta \in I$. Hence $\beta \in \bigcap_{j=1}^{m} \tau_j^{-1}(I)$. Therefore, $\beta \in \left(\bigcap_{i=1}^{k} H_K(f_i)\right) \cap \left(\bigcap_{j=1}^{m} \tau_j^{-1}(I)\right)$.

□

Here is our main theorem.

Theorem 1.3. *Let $E/\mathbb{Q}$ be an elliptic curve over $\mathbb{Q}$. Then, for every automorphism $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, the rank of E over the maximal Galois extension contained in $\overline{\mathbb{Q}}^{\sigma}$ is infinite, hence the rank of $E(\overline{\mathbb{Q}}^{\sigma})$ is infinite.*

Proof. Let N be the conductor of E and let $y^2 = x^3 + ax + b$ be a Weierstrass equation of $E/\mathbb{Q}$. By the change of variables, we may assume that a and b are integers. Let $M = 4p_1p_2 \cdots p_k$, where p_k are all distinct prime factors of N. Consider the polynomial

$$f(x) = (1 + Mx)^3 + aM^4(1 + Mx) + bM^6 \in \mathbb{Z}[x].$$

Then, there exists a real number r such that for all $x < r$, the expression $f(x)$ is strictly negative. Let $I = (-\infty, r)$ be the open interval in $\mathbb{R}$ of all real numbers less than r. Choose an integer $m_1 \in I$. Then, $y^2 - f(m_1)$ is irreducible over $\mathbb{Q}$, since $f(m_1) < 0$. If we let $K_{m_1} := \mathbb{Q}(\sqrt{f(m_1)})$, then K_{m_1} is an imaginary quadratic extension of $\mathbb{Q}$.

By Lemma 1.1, there is a polynomial $p(x, y)$ over $\mathbb{Q}$ such that $H_{\mathbb{Q}}(p(x, y)) \subseteq H_{K_{m_1}}(y^2 - f(x))$. Then, since $\mathbb{Q}$ is Hilbertian, by Lemma 1.2, there exists a rational number in $I \cap H_{\mathbb{Q}}(p(x, y))$. In particular, since the Hilbert set $H_{\mathbb{Q}}(p(-x, y))$ contains infinitely many rational primes by [7, Chapter 9, Corollary 2.4], $H_{\mathbb{Q}}(p(x, y))$ contains infinitely many negative (prime) integers. So we can choose an integer $m_2 \in I \cap H_{\mathbb{Q}}(p(x, y))$. Then, since $m_2 \in H_{K_{m_1}}(y^2 - f(x))$, $K_{m_2} := \mathbb{Q}(\sqrt{f(m_2)})$ is a quadratic imaginary extension of $\mathbb{Q}$, and K_{m_1} and K_{m_2} are distinct, hence they

are linearly disjoint over $\mathbb{Q}$. By repeating this procedure over the composite field $K_{m_1}K_{m_2}\cdots K_{m_r}$ of imaginary quadratic extensions obtained from the previous steps inductively, we obtain an infinite set S of integers such that for all $m \in S$,

(1) $f(m) < 0$, so that $K_m := \mathbb{Q}(\sqrt{f(m)})$ is an imaginary quadratic extension of $\mathbb{Q}$,
(2) the fields in the infinite sequence $\{K_m\}_{m\in S}$ are linearly disjoint over $\mathbb{Q}$,

($i.e.$ $[K_{m_1}K_{m_2}\cdots K_{m_r} : \mathbb{Q}] = 2^r,$ for any $m_i \in S$ and for every $r \geq 1$)

and
(3) if $E/\mathbb{Q}$ has CM, then K_m is different from $F = \mathrm{End}(E) \otimes \mathbb{Q}$.

Note that for each $m \in S$ and for every prime p_i dividing N,

$$f(m) \equiv \begin{cases} 1 \pmod{p_i}, & \text{if } p_i \neq 2, \\ 1 \pmod{8}, & \text{if } p_i = 2. \end{cases}$$

Hence, this implies that all primes dividing N are split in K_m. On the other hand, the discriminant of K_m is $f(m)$ or $4f(m)$ depending on whether $f(m) \equiv 1 \pmod 4$ or not, respectively. In any case, the discriminant of K_m is prime to N.

Let $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. We consider two cases. For the first case, suppose that for all $m \in S$, $\sigma|_{K_m} = id_{K_m}$. Then, for each $m \in S$, consider the number $\dfrac{1+Mm}{M^2} \in \mathbb{Q}$. By plugging this number into the given Weierstrass equation of $E/\mathbb{Q}$, we get

$$y^2 = \left(\frac{1+Mm}{M^2}\right)^3 + a\left(\frac{1+Mm}{M^2}\right) + b = \frac{f(m)}{M^6}.$$

Hence the point

$$P_m = \left(\frac{1+Mm}{M^2}, \frac{\sqrt{f(m)}}{M^3}\right)$$

is in $E(K_m)$ but it is not in $E(\mathbb{Q})$. Moreover, since $K_m = K_m^\sigma$, P_m is fixed under σ.

So we get an infinite sequence $\{P_m\}_{m\in S}$ of points in $E(\overline{\mathbb{Q}}^\sigma)$ such that each P_m is defined over the imaginary quadratic extension K_m. As shown in [9, Lemma], we know that the set of all torsion points of E defined over finite extensions of $\mathbb{Q}$ of bounded degree is finite. So we may assume that these points P_m are not torsion points. Now we show that the points P_m for $m \in S$ are linearly independent. Suppose that for some integers a_i and $m_i \in S$,

$$a_1P_{m_1} + a_2P_{m_2} + \cdots + a_kP_{m_k} = O.$$

Since the fields in $\{K_m\}_{m\in S}$ are linearly disjoint over $\mathbb{Q}$, for each i, we can find an automorphism of $\overline{\mathbb{Q}}$ which fixes all but exactly one K_{m_i} of $K_{m_1}, \ldots, K_{m_k}$. Note that such an automorphism takes P_{m_i} to its inverse, $-P_{m_i}$. Applying this automorphism, we get

$$a_1P_{m_1} + \cdots + a_{i-1}P_{m_{i-1}} - a_iP_{m_i} + \cdots + a_kP_{m_k} = O.$$

By subtracting, we get $2a_iP_{m_i} = O$, which implies $a_i = 0$. We conclude that the P_m for $m \in S$ are linearly independent in $E(\overline{\mathbb{Q}}^\sigma) \otimes \mathbb{Q}$. Since P_m are defined over the composite field of all quadratic extensions which is Galois as an abelian extension over $\mathbb{Q}$, this implies that the rank of E over the maximal abelian (Galois) extension $\mathbb{Q}_{ab}$ in $\overline{\mathbb{Q}}^\sigma$ is infinite. Hence the rank of $E(\overline{\mathbb{Q}}^\sigma)$ is infinite.

For the second case, suppose that there exists an integer $m \in S$ such that $\sigma|_{K_m} \neq id_{K_m}$. Then, fix such an imaginary quadratic extension K_m, and call it K, and let K_{ab} be the maximal abelian extension of K. Then, we complete the proof of this case as a consequence of the following statement:

Theorem 1.4. *Under the assumption in the second case above (i.e. if K is different from $\mathrm{End}(E) \otimes \mathbb{Q}$, all primes dividing N are split in K, and $\sigma|_K \neq id_K$), the rank of the Mordell-Weil group of E over the fixed subfield $(K_{ab})^\sigma$ of K_{ab} under σ is infinite, hence the rank of E over the maximal Galois extension contained in $\overline{\mathbb{Q}}^\sigma$ is inifinte.*

The proof of Theorem 1.4, which lies deeper than the methods used in the first case will be treated in the following section and will be given explicitly in Proposition 2.9, as it requires modularity of $E/\mathbb{Q}$ and the theory of complex multiplication which give nontorsion algebraic points of E under the given assumption in the second case. □

2. The rank of E over ring class fields of imaginary quadratic fields

The goal of this section is to prove Theorem 1.4 — stated at the end of the previous section. By a theorem of Wiles [12] and Taylor-Wiles [11] (completed by a later work of Breuil, Conrad, Diamond and Taylor [1]), the elliptic curve $E/\mathbb{Q}$ is known to be *modular*. Our strategy is to construct algebraic points on E using *Heegner points* over the ring class fields arising from the theory of complex multiplication.

Through out this section, we let $E/\mathbb{Q}$ be an elliptic curve over $\mathbb{Q}$ of conductor N. Let K be an imaginary quadratic extension of $\mathbb{Q}$ with discriminant D such that all prime divisors of N split in K. For each integer n relatively prime to ND, set $\mathcal{N}_n = \mathcal{N} \cap \mathcal{O}_n$, where $\mathcal{O}_n$ is the order of index n in the ring of integers $\mathcal{O}_K$ of K and $\mathcal{N}$ is an ideal of $\mathcal{O}_K$ with $\mathcal{O}_K/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$. Then, $\mathcal{O}_n/\mathcal{N}_n \cong \mathbb{Z}/N\mathbb{Z}$ and the elliptic curve $\mathbb{C}/\mathcal{O}_n$ defines the Heegner point Q_n on the modular curve $X_0(N)$ corresponding to the cyclic N-isogeny $(\mathbb{C}/\mathcal{O}_n \to \mathbb{C}/\mathcal{N}_n^{-1})$. Let H_n denote the ring class field of K of conductor n. By [2, Chapter 3, Theorem 3.6], there is an algebraic point $P_n \in E(H_n)$ which is in the image of Q_n under the modular parametrization and is also called a *Heegner point of conductor n*. Let $HP(n) \subset E(H_n)$ denote the set of all Heegner points of conductor n in $E(H_n)$. Let H_∞ be the compositum of all ring class fields of conductor prime to ND. Then, the sets $HP(n)$ and $E(H_\infty)$ satisfy the following properties.

First, we recall some of the norm-compatibility properties of Heegner points P_n.

Proposition 2.1. *Let n be an integer and ℓ a prime number such that both n and ℓ are prime to ND. Let $P_{n\ell}$ be any point in $HP(n\ell)$ and a_ℓ the coefficient of the Hecke operator T_ℓ of the modular form of E. Then, there are points $P_n \in HP(n)$ and $P_{n/\ell} \in HP(n/\ell)$ (when $\ell|n$) such that*

$$\mathrm{Trace}_{H_{n\ell}/H_n}(P_{n\ell}) = \begin{cases} a_\ell P_n & \text{if } \ell \nmid n \text{ is inert in } K, \\ a_\ell P_n - P_{n/\ell} & \text{if } \ell | n. \end{cases}$$

Proof. See [2, Chapter 3, Proposition 3.10]. □

Lemma 2.2. *The set $E(H_\infty)_{\mathrm{tors}}$ is finite.*

Proof. See [2, Chapter 3, Lemma 3.14]. □

The following lemma describes the structure of the Galois groups of ring class fields over a given imaginary quadratic extension K of $\mathbb{Q}$. It is essentially well-known, but we include a proof here for lack of an adequate reference.

Lemma 2.3. *In our setting for H_m over K,*

(1) *If p is a prime not dividing $c\cdot N\cdot D\cdot[H_c:K]\cdot disc(H_c)$, then for all integers $n\geq 1$,*

$$\mathrm{Gal}(H_{cp^n}/H_{cp})\cong\mathbb{Z}/p^{n-1}\mathbb{Z},\ \textit{and}\ \mathrm{Gal}(H_{cp^{n+1}}/H_{cp^n})\cong\mathbb{Z}/p\mathbb{Z}.$$

(2) *If $k=\prod_{j=1}^{m}p_j$ for distinct primes p_j which are relatively prime to N and inert in K, then for each j,*

$$\mathrm{Gal}(H_k/H_{\frac{k}{p_j}})\cong\mathbb{Z}/(p_j+1)\mathbb{Z}.$$

Proof. First, we note that if H is the Hilbert class field of K, then for $n\geq 1$,

$$\mathrm{Gal}(H_{cp^n}/H)\cong(\mathcal{O}_K/cp^n\mathcal{O}_K)^*/(\mathbb{Z}/cp^n\mathbb{Z})^*$$

and $\mathrm{Gal}(H_{cp^n}/K)$ is an extension of the ideal class group $C\ell_K$ of K by $\mathrm{Gal}(H_{cp^n}/H)$.

To prove the first part of (1), for $n\geq 1$,

$$\begin{aligned}
\mathrm{Gal}(H_{cp^n}/H_{cp}) &\cong ker(\mathrm{Gal}(H_{cp^n}/K)\to\mathrm{Gal}(H_{cp}/K))\\
&\cong ker((\mathcal{O}_K/cp^n\mathcal{O}_K)^*/(\mathbb{Z}/cp^n\mathbb{Z})^*\to(\mathcal{O}_K/cp\mathcal{O}_K)^*/(\mathbb{Z}/cp\mathbb{Z})^*)\\
&=\frac{[(1+cp\mathcal{O}_K)/cp^n\mathcal{O}_K]^*\cdot(\mathbb{Z}/cp^n\mathbb{Z})^*}{(\mathbb{Z}/cp^n\mathbb{Z})^*}\\
&=\frac{[(1+cp\mathcal{O}_K)/cp^n\mathcal{O}_K]^*}{[(1+cp\mathbb{Z})/cp^n\mathbb{Z}]^*}\\
&=\frac{[(1+p\mathcal{O}_K)/p^n\mathcal{O}_K]^*}{[(1+p\mathbb{Z})/p^n\mathbb{Z}]^*}\quad(\text{since } p\nmid c\cdot D\cdot[H_c:K]\cdot disc(H_c))\\
&\cong\frac{[(1+p\mathcal{O}_K)/p^n\mathcal{O}_K]^*}{(\mathbb{Z}/p^{n-1}\mathbb{Z})}\\
&\qquad(\text{since } [(1+p\mathbb{Z})/p^n\mathbb{Z}]^*\cong ker((\mathbb{Z}/p^n\mathbb{Z})^*\to(\mathbb{Z}/p\mathbb{Z})^*))\cong\mathbb{Z}/p^{n-1}\mathbb{Z}).
\end{aligned}$$

By the logarithmic function from $1+p\widehat{\mathcal{O}}_{K,p}\to p\widehat{\mathcal{O}}_{K,p}$ which maps $1+p^n\widehat{\mathcal{O}}_{K,p}\mapsto p^n\widehat{\mathcal{O}}_{K,p}$, where $\widehat{\mathcal{O}}_{K,p}$ is the completion of $\mathcal{O}_K$ at p,

$$[(1+p\widehat{\mathcal{O}}_{K,p})/p^n\widehat{\mathcal{O}}_{K,p}]^*\cong\widehat{\mathcal{O}}_{K,p}/p^{n-1}\widehat{\mathcal{O}}_{K,p}\cong\mathcal{O}_K/p^{n-1}\mathcal{O}_K.$$

Hence, we have

$$\mathrm{Gal}(H_{cp^n}/H_{cp})\cong(\mathcal{O}_K/p^{n-1}\mathcal{O}_K)/(\mathbb{Z}/p^{n-1}\mathbb{Z})\cong\mathbb{Z}/p^{n-1}\mathbb{Z}.$$

For the second part of (1),

$$\begin{aligned}
\mathrm{Gal}(H_{cp^{n+1}}/H_{cp^n}) &\cong ker(\mathrm{Gal}(H_{cp^{n+1}}/H_{cp})\to\mathrm{Gal}(H_{cp^n}/H_{cp}))\\
&\cong ker((\mathbb{Z}/p^n\mathbb{Z})^*\to(\mathbb{Z}/p^{n-1}\mathbb{Z})^*)\\
&\cong\mathbb{Z}/p\mathbb{Z}.
\end{aligned}$$

To prove (2), for $k = \prod_{j=1}^{m} p_j > 1$ and for each $i = 1, ..., m$,

$$\begin{aligned}
\mathrm{Gal}(H_k/H_{\frac{k}{p_i}}) &\cong ker(\mathrm{Gal}(H_k/K) \to \mathrm{Gal}(H_{\frac{k}{p_i}}/K)) \\
&\cong ker((\mathcal{O}_K/k\mathcal{O}_K)^*/(\mathbb{Z}/k\mathbb{Z})^* \to (\mathcal{O}_K/\frac{k}{p_i}\mathcal{O}_K)^*/(\mathbb{Z}/\frac{k}{p_i}\mathbb{Z})^*) \\
&\cong ker\left(\prod_{j=1}^{m} \mathrm{Gal}(H_k/H_{\frac{k}{p_j}}) \to \prod_{j=1}^{i-1} \mathrm{Gal}(H_k/H_{\frac{k}{p_j}})\right. \\
&\qquad \left. \times\{1\} \times \prod_{j=i+1}^{m} \mathrm{Gal}(H_k/H_{\frac{k}{p_j}})\right) \\
&\cong (\mathbb{Z}/\lambda\mathbb{Z})^*/(\mathbb{Z}/p_i\mathbb{Z})^* \text{ where } \lambda \text{ is a prime factor of } p_i \\
&\cong \mathbb{Z}/(p_i+1)\mathbb{Z}.
\end{aligned}$$

□

A Heegner system attached to (E, K) is a collection of points $P_n \in E(H_n)$ indexed by integers n prime to the conductor N of $E/\mathbb{Q}$ and the discriminant D of K, and satisfying the norm compatibility properties given in Proposition 2.1 and the behavior under the action of reflections described in [2, Chapter 3, Proposition 3.11].

In our setting, since all primes dividing N are split in K (recall the construction of K in the proof of Theorem 1.3), there is a Heegner system in which at least one of the Heegner points P_n of conductor n for some n is a nontorsion point as a consequence of Lemma 2.2, together with the fact that the modular parametrization $X_0(N) \to E$ has finite degree (see [2, Chapter 3, Theorem 3.13]). We call such a Heegner system a *nontrivial Heegner system.*

Now we will need the following lemmas to prove Proposition 2.7 later.

Lemma 2.4. *For a given elliptic curve E/F over a number field F, suppose there exists a point $Q \in E(\overline{F}) - E(F)$ and suppose that $m > 1$ is the smallest positive integer such that $mQ \in E(F)$. If there exists a prime p such that p^r divides m for some integer $r \geq 1$, then there exists an automorphism $\tau \in \mathrm{Gal}(\overline{F}/F)$ such that $\tau\left(\frac{m}{p}Q\right) - \frac{m}{p}Q$ is a nontrivial point, and for such τ, the point $\tau\left(\frac{m}{p^r}Q\right) - \frac{m}{p^r}Q$ is a nontrivial torsion point of exact order p^r.*

Proof. First, by the minimality of m, $\frac{m}{p}Q \notin E(F)$, so there exists an automorphism $\tau \in \mathrm{Gal}(\overline{F}/F)$ such that $\tau\left(\frac{m}{p}Q\right) \neq \frac{m}{p}Q$.

Then, since τ fixes F and $mQ \in E(F)$, we see that

$$p^r\left(\tau\left(\frac{m}{p^r}Q\right) - \frac{m}{p^r}Q\right) = \tau(mQ) - mQ = mQ - mQ = O.$$

So $\tau\left(\frac{m}{p^r}Q\right) - \frac{m}{p^r}Q$ is a torsion point and its order is of the form p^i for some $0 \leq i \leq r$.

If $i < r$, then $r - i - 1 \geq 0$ and

$$\tau\left(\frac{m}{p}Q\right) - \frac{m}{p}Q = p^{r-i-1} \cdot p^i\left(\tau\left(\frac{m}{p^r}Q\right) - \frac{m}{p^r}Q\right) = p^{r-i-1}O = O,$$

which contradicts its nontriviality. Hence, $i = r$ and the order of $\tau\left(\frac{m}{p^r}Q\right) - \frac{m}{p^r}Q$ is p^r. □

Lemma 2.5. *For a given elliptic curve E/L over a number field L, let H be an (infinite) Galois extension of L and let $\{P_m\}_{m=1}^{\infty}$ be an infinite sequence of points in $E(H)$. Denote by $\mathcal{S}$ the subgroup of $E(H)$ generated by the P_m. Suppose that*

(1) *$E(H)_{\mathrm{tors}}$ is finite, and*
(2) *$\mathcal{S}$ is not finitely generated.*

Then, $\dim \mathcal{S} \otimes \mathbb{Q} = \dim E(H) \otimes \mathbb{Q} = \infty$.

Proof. Suppose not. Then there exists an integer $N > 0$ such that for each $m > N$, the set $\{P_1, \ldots, P_N\} \cup \{P_m\}$ is linearly dependent. Then there exists a number field F such that $L \subseteq F \subset H$ and the points $P_1, \ldots, P_N$ are defined over F. Since $\mathcal{S}$ is not finitely generated but $P_1, \ldots, P_N$ and P_m are dependent for all $m > N$, there are infinitely many $m > N$ such that $P_m \notin E(F)$ and for such m, there exists $k > 1$ such $kP_m \in E(F)$. Let

$$M := \{m > N : P_m \notin E(F)\}.$$

Also, for each $m \in M$, let

$$k_m = \min\{k : k > 1 \text{ and } kP_m \in E(F)\}.$$

Let

$$U = \{k_m : m \in M\}.$$

First, suppose U is finite. If $k = \prod_{k_m \in U} k_m$, then $\{P_m : m \in M\} \subset [k]^{-1}E(F)$. Since $[k]^{-1}E(F)$ is finitely generated, this implies that $\mathcal{S}$ is finitely generated, which is a contradiction to condition (2).

So U must be infinite. Let

$$V = \{\ell : \ell \text{ is a prime and } \ell \mid k \text{ for some } k \in U\}.$$

We consider two subcases. First, suppose that V is finite. Then as U is infinite, there exists a prime $\ell \in V$, an infinite sequence $m_1 < m_2 < \cdots$ in M, and an infinite sequence of exponents $1 \le r_1 < r_2 < \cdots$ such that $\mathrm{ord}_\ell k_{m_i} = r_i$ for each i. By the minimality of k_{m_i}, for each i, there exists an automorphism $\tau_i \in \mathrm{Gal}(H/F)$ such that $(\tau_i - 1)\left(\frac{k_{m_i}}{\ell^{r_i}}\right) P_{m_i} \neq O$. Then by Lemma 2.4, the point $Q_i = (\tau_i - 1)\left(\frac{k_{m_i}}{\ell^{r_i}}\right) P_{m_i}$ is a torsion point in $E(H)$ of exact order ℓ^{r_i}. Since the r_i form a strictly increasing sequence, this contradicts condition (1) of the finiteness of $E(H)_{\mathrm{tors}}$.

Now suppose that V is infinite. Then we can find infinitely many distinct integers $m_1, m_2, \ldots$ in M and distinct prime integers $\ell_1, \ell_2, \ldots$ in V such that for each i, $\ell_i \mid k_{m_i}$ and $\ell_i \nmid k_{m_j}$ for all $j \neq i$. As above, we find automorphisms $\tau_i \in \mathrm{Gal}(H/F)$ such that $Q_i := (\tau_i - 1)\left(\frac{k_{m_i}}{\ell^{r_i}}\right) P_{m_i} \neq O$. Then by Lemma 2.4, the point Q_i is a torsion point in $E(H)$ of exact order ℓ_i. Since ℓ_i are distinct, this again contradicts the finiteness of $E(H)_{\mathrm{tors}}$. □

Now we prove the unboundedness of the rank of Mordell-Weil groups over all the ring class fields of conductor cp^n as n goes to infinity for a prime p prime to ND and to some integer c. This will play an important role in the proof of the main theorem. To prove this, we need the following simple lemma.

Lemma 2.6. *For an elliptic curve $E/\mathbb{Q}$ and for a prime p not dividing the conductor of E, let $a_p = p + 1 - \#E(\mathbb{F}_p)$. Then there is no infinite sequence $\{c_n\}_{n=0}^{\infty}$*

of integers with $c_0 \neq 0$ and satisfying the following linear recurrence:

$$pc_{n+1} = a_p c_n - c_{n-1}, \text{ for all } n \geq 1,$$

and for every N, there exists $n > N$ such that $c_n \neq 0$.

Proof. Suppose there is such an infinite sequence $\{c_n\}_{n=0}^{\infty}$ of integers satisfying the above conditions. Then, the linear recurrence implies that

$$(*) \qquad c_n = \alpha^n b_0 + \beta^n b_1, \text{ for all } n \geq 1,$$

where α and β are two solutions of the quadratic equation $x^2 - \frac{a_p}{p}x + \frac{1}{p} = 0$ and

$$b_0 = \left(\frac{-\beta}{\alpha - \beta}c_0 + \frac{1}{\alpha - \beta}c_1\right) \text{ and } b_1 = \left(\frac{\alpha}{\alpha - \beta}c_0 - \frac{1}{\alpha - \beta}c_1\right).$$

Note that this quadratic equation has no rational solutions, because if there were, the only possible pairs of rational solutions would be 1 and $\frac{1}{p}$ or -1 and $-\frac{1}{p}$ and in either case, we would get $a_p = \pm(p+1)$ which is impossible since $|a_p| < 2\sqrt{p}$ by Hasse's inequality [10, Chapter V, Theorem 1.1]. Also, $b_0 \neq 0$ and $b_1 \neq 0$ since c_0 is a nonzero integer and α and β are not rational numbers.

Let F be a quadratic extension of $\mathbb{Q}$ containing α and β and choose an embedding of F into $\overline{\mathbb{Q}}_p$ with the valuation v_p such that $v_p(\alpha) < 0$ and $v_p(\beta) = 0$, where $\overline{\mathbb{Q}}_p$ is an algebraic closure of the p-adic field $\mathbb{Q}_p$. This is possible because $\alpha\beta = \frac{1}{p}$.

Since $b_0 \neq 0$ and $v_p(\beta) = 0$, the recurrence relation $(*)$ implies that for all large positive integers n, $v_p(c_n)$ is dominated by $v_p(\alpha^n)$ which is negative. But for each N, there exists $n > N$ such that $c_n \neq 0$. Since a nonzero integer c_n has a nonnegative valuation, we get a contradiction. Hence, there is no such sequence. □

Proposition 2.7. *For a given elliptic curve $E/\mathbb{Q}$ of conductor N, if there is a nontrivial Heegner system attached to (E, K), where K is an imaginary quadratic extension of $\mathbb{Q}$ with discriminant D such that $K \neq \mathrm{End}(E) \otimes \mathbb{Q}$, then there exists an integer $r > 0$ prime to ND such that for any prime p such that $p \nmid r \cdot N \cdot D \cdot [H_r : K] \cdot disc(H_r)$, the rank of $E(H_{rp^n})$ is unbounded, as n goes to infinity.*

Proof. First, we show that there exists a positive integer r such that for a prime p such that $p \nmid r \cdot N \cdot D \cdot [H_r : K] \cdot disc(H_r)$, the subgroup $\mathcal{S}$ of $E(H_\infty)$ generated by all Heegner points of conductor rp^n for all integer $n \geq 1$ in the given nontrivial Heegner system is not finitely generated.

Suppose for any integer r, this group $\mathcal{S}$ is finitely generated. Then, by Lemma 2.2, since $E(H_\infty)_{\mathrm{tors}}$ is finite, for some integer k there is a fixed ring class field H_{rp^k} over which all Heegner points of conductor rp^n for all $n \geq 1$ are defined.

Let $m_0 = rp^k$ and $m_n = rp^{k+n}$ for $n \geq 1$. Since the given Heegner system is nontrivial, we may assume that a Heegner point P_0 of conductor $m_0 = rp^k$ is of infinite order.

By the second norm-compatibility property given in Proposition 2.1, we have that for all $n \geq 1$,

$$\mathrm{Trace}_{H_{m_{n+1}}/H_{m_n}}(P_{n+1}) = a_p P_n - P_{n-1},$$

where P_i are Heegner points of conductor $m_i = m_0 p^i$.

Since P_{n+1} is defined over H_{m_0}, hence over H_{m_n} by assumption, the trace of P_{n+1} from $H_{m_{n+1}}$ to H_{m_n} is the degree of $H_{m_{n+1}}$ over H_{m_n} which is p by (1) of

Lemma 2.3. Therefore, the infinite sequence of Heegner points of conductor of the form $m_n = m_0 p^n$ satisfies the linear recurrence relation,

$$(**) \qquad pP_{n+1} = a_p P_n - P_{n-1}, \text{ for all } n \geq 1.$$

By the Mordell-Weil Theorem, $E(H_{m_0})$ is finitely generated, so by dividing by its torsion subgroup $E(H_{m_0})_{\text{tors}}$, all points $P_n \mod E(H_{m_0})_{\text{tors}}$ lie in $\mathbb{Z}^k$ for some k. Suppose that $E(H_{m_0}) \cong \mathbb{Z}Q_1 + \cdots + \mathbb{Z}Q_k + E(H_{m_0})_{\text{tors}}$ where Q_i are linearly independent points of $E(H_{m_0})$. Now we consider all points $P_n \mod E(H_{m_0})_{\text{tors}}$ and denote it by P_n again by abuse of notation. Let $P_n = \sum_{i=1}^{k} c_{n,i} Q_i$ for some integers $c_{n,i}$. Since P_0 is not a torsion point by the assumption, without loss of generality we may assume that $c_{0,1} \neq 0$. Then, at least one of $c_{1,1}$ and $c_{2,1}$ is nonzero, since otherwise, the relation $(**)$ implies that $c_{0,1}Q_1$ is a linear combination of points $Q_2, Q_3, \ldots, Q_k$ over $\mathbb{Z}$ which contradicts the linear independence of the points Q_i. Inductively, by using $(**)$ and linear dependence of the points Q_i, we can show that $pc_{n+1,i} = a_p c_{n,i} - c_{n-1,i}$ for all $n \geq 1$, and if $c_{n-1,1} \neq 0$, then $c_{n,1} \neq 0$ or $c_{n+1,1} \neq 0$. Hence, by setting $c_n = c_{n,1}$, we get an infinite sequence $\{c_n\}_{n=0}^{\infty}$ of integers satisfying the $pc_{n+1} = a_p c_n - c_{n-1}$ for all $n \geq 1$ with $c_0 \neq 0$ and for each N, there exists $n > N$ such that $c_n \neq 0$. This is a contradiction to Lemma 2.6. Therefore, we conclude that the group $\mathcal{S}$ is not finitely generated as a subgroup of $E(H_\infty)$.

Then, since the torsion subgroup $E(H_\infty)_{\text{tors}}$ is finite by Lemma 2.2, the dimension of $\mathcal{S} \otimes \mathbb{Q}$ is infinite by Lemma 2.5. Therefore, the dimension of $E(H_{rp^n}) \otimes \mathbb{Q}$ (*i.e.* the rank of $E(H_{rp^n})$) cannot be bounded, as n goes to infinity. □

Remark 2.8. By using the Čevotarev Density Theorem and the first norm-compatibility property given in Proposition 2.1, for the given nontrivial Heegner system, we can prove that the subgroup generated by all Heegner points of conductor of the form rm for some r, where m is a square-free integer relatively prime to rND. Then, Lemma 2.5 implies the unboundedness of the rank of Mordell-Weil groups over all of those ring class fields of conductor rm as a square-free m goes to infinity.

Finally, the following proposition proves Theorem 1.4, hence completing the proof of Theorem 1.3.

Proposition 2.9. *Let $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and K an imaginary quadratic extension of $\mathbb{Q}$ with discriminant D such that $\sigma|_K \neq id_K$ and $K \neq \text{End}(E) \otimes \mathbb{Q}$. Suppose that all primes dividing the conductor N of $E/\mathbb{Q}$ split in K. Then, the rank of the Mordell-Weil group $E(H_n^\sigma)$ is unbounded, as n goes to ∞. Hence, the rank of $E((K_{ab})^\sigma)$ and the rank of E over the maximal Galois extension of $\mathbb{Q}$ contained in $\overline{\mathbb{Q}}^\sigma$ are infinite, where K_{ab} is the maximal abelian extension of K.*

Proof. Since all primes dividing the conductor N of E split in K, there is a nontrivial Heegner system attached to (E, K) by [2, Chapter 3, Theorem 3.13]. For a given $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, since $\sigma|_K \neq id_K$, the restriction of σ to each ring class field H_n in the given Heegner system can be lifted as an involution of H_n. Let $\sigma_n = \sigma|_{H_n}$ be the restriction of σ to H_n. Then, each ring class field H_n has a generalized dihedral group structure as its Galois group over $\mathbb{Q}$ with an involution σ_n such that for any $\tau \in \text{Gal}(H_n/K)$, $\sigma_n \tau \sigma_n = \tau^{-1}$.

By Proposition 2.7, we may fix a positive integer r and an odd prime p such that $p \nmid r \cdot N \cdot D \cdot [H_r : K] \cdot disc(H_r)$ and the rank of $E(H_{rp^n})$ is unbounded, as n goes to infinity. We prove that the rank of $E(H^{\sigma}_{rp^n})$ is unbounded as n goes to infinity.

Suppose not. Then since the restriction σ_n of σ to H_{rp^n} is an involution of the ring class field H_{rp^n}, there exists an integer $k \geq 1$ such that σ acts by -1 on any nontrivial quotient $(E(H_{rp^{k+n}}) \otimes \mathbb{Q})/(E(H_{rp^k}) \otimes \mathbb{Q})$, for all $n \geq 1$.

By (1) of Lemma 2.3, $\mathrm{Gal}(H_{rp^{k+n}}/H_{rp})$ is a cyclic group of order p^{k+n-1}. Also, $\mathrm{Gal}(H_{rp^{k+n}}/H_{rp^k})$ is a subgroup of $\mathrm{Gal}(H_{rp^{k+n}}/H_{rp})$. Hence, it is a cyclic subgroup of order p^m for some $m < k + n - 1$.

Let $m_0 = rp^k$ and $m_n = rp^{k+n}$ for each $n \geq 1$. Let τ_n be a generator of $\mathrm{Gal}(H_{m_n}/H_{m_0})$. Consider $E(H_{m_n}) \otimes \mathbb{Q}$ as a representation of $\mathrm{Gal}(H_{m_n}/\mathbb{Q})$. Also, for each $n \geq 1$, let

$$M_n = (E(H_{m_n}) \otimes \mathbb{Q})/(E(H_{m_0}) \otimes \mathbb{Q}).$$

For every element $\alpha \in \mathrm{Gal}(H_{m_n}/\mathbb{Q})$, let $\alpha|_{H_{m_0}}$ be the restriction of α to H_{m_0}. Then, $\alpha|_{H_{m_0}}$ is an element of $\mathrm{Gal}(H_{m_0}/K)$, since H_{m_0} is Galois over $\mathbb{Q}$. Therefore, $\mathrm{Gal}(H_{m_n}/\mathbb{Q})$ acts on $E(H_{m_0}) \otimes \mathbb{Q}$ as well. So we can consider the quotient M_n as a representation of $\mathrm{Gal}(H_{m_n}/\mathbb{Q})$.

Let

$$\rho : \mathrm{Gal}(H_{m_n}/\mathbb{Q}) \to \mathrm{Aut}(M_n)$$

be the representation of $\mathrm{Gal}(H_{m_n}/\mathbb{Q})$. Then, by the hypothesis, σ_n acts by -1 on M_n. Hence, $\rho(\sigma_n) = -id$ on M_n. On the other hand, by the dihedral group structure of $\mathrm{Gal}(H_{m_n}/\mathbb{Q})$, $\sigma_n \tau_n \sigma_n = \tau_n^{-1}$. Therefore,

$$\rho(\tau_n^2) = \rho(\tau_n)\rho(\tau_n) = (-id)\rho(\tau_n)(-id)\rho(\tau_n) = \rho(\sigma_n\tau_n\sigma_n\tau_n) = \rho(1) = id.$$

Hence, the restriction of ρ to the cyclic subgroup $\mathrm{Gal}(H_{m_n}/H_{m_0})$ of $\mathrm{Gal}(H_{m_n}/\mathbb{Q})$ generated by τ_n^2 is a trivial representation of M_n. Since the order of τ_n is an odd integer p^m,

$$\langle \tau_n^2 \rangle = \langle \tau_n \rangle = \mathrm{Gal}(H_{m_n}/H_{m_0}).$$

Therefore, we have

$$M_n^{\mathrm{Gal}(H_{m_n}/H_{m_0})} = M_n^{\langle \tau_n^2 \rangle} = M_n.$$

This implies that

$$E(H_{m_n}^{\mathrm{Gal}(H_{m_n}/H_{m_0})}) \otimes \mathbb{Q} + E(H_{m_0}) \otimes \mathbb{Q} = E(H_{m_n}) \otimes \mathbb{Q}.$$

Since $H_{m_n}^{\mathrm{Gal}(H_{m_n}/H_{m_0})} = H_{m_0}$,

$$E(H_{m_0}) \otimes \mathbb{Q} = E(H_{m_n}) \otimes \mathbb{Q}, \quad \text{for all } n \geq 1,$$

which is a contradiction to Proposition 2.7.

Hence, the rank of $E(H^{\sigma}_{rp^{k+n}})$ is unbounded, as $n \to \infty$. Since all ring class fields H_{m_n} are abelian over K and are Galois over $\mathbb{Q}$, this implies that the rank of $E((K_{ab})^{\sigma})$ and the rank E over the maximal Galois extension of $\mathbb{Q}$ contained in $\overline{\mathbb{Q}}^{\sigma}$ are infinite. □

Acknowledgements

I would like to thank my thesis advisor, Michael Larsen, for suggesting this problem and for valuable discussions and helpful comments on this paper. I wish to thank Henri Darmon for inviting me to speak at the Québec-Vermont Number Theory Seminar at McGill University in 2003, for having very useful discussions and suggesting this approach during my visit, and for his guidance, valuable advice and comments on an earlier draft of this paper. Also, I would like to thank Joseph H. Silverman for correcting misprints and giving helpful comments on the earlier draft. At last, I express my gratitude to the referee for the careful reading of the original manuscript and a lot of helpful comments and suggestions that helped improve the presentation and shorten the previous version of the manuscript.

References

[1] 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. MR1839918 (2002d:11058)

[2] H. Darmon, *Rational points on modular elliptic curves*, CBMS Regional Conference Series in Mathematics, 101. Published for the Conference Board of the Mathematical Sciences, Washington, DC; by the AMS, Providence, RI, 2004. MR2020572 (2004k:11103)

[3] B. Im, *Mordell-Weil groups and the rank of elliptic curves over large fields*, *Canad. J. Math.*, Vol. **58** (4) (2006), 796-819. MR2245274 (2006e:11064)

[4] B. Im, *The rank of elliptic curves with 2-torsion points over large fields*, *Proc. Amer. Math. Soc.*, Vol.**134** (2006), no.6, 1623-1630. MR2204272 (2006j:11078)

[5] M. Jarden and M. Fried, *Field Arithmetic*, A series of Modern Surveys in Math. **11**, Springer-Verlag, 1980. MR868860 (89b:12010)

[6] M. Jarden, *Large normal extensions of Hilbertian fields*, *Math. Z.*, **224**, (1997), 555-565. MR1452049 (98e:12003)

[7] S. Lang, *Fundamentals of Diophantine Geometry*, Springer-Verlag, New York, 1983. MR715605 (85j:11005)

[8] M. Larsen, *Rank of elliptic curves over almost algebraically closed fields*, *Bull. London Math. Soc.* **35** (2003), 817–820. MR2000029 (2004i:11054)

[9] J. H. Silverman, *Integer points on curves of genus* 1, *J. London Math. Soc.* **(2), 28** *(1983)*, 1-7. MR703458 (84g:10033)

[10] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, GTM **106**, 1986. MR817210 (87g:11070)

[11] R. Taylor and A. Wiles, *Ring-Theoretic properties of certain Hecke algebras*, *Ann. of Math.* (2) **141** (1995), no. 3, 553-572. MR1333036 (96d:11072)

[12] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, *Ann. of Math.* (2) **141** (1995), no. 3, 443-551. MR1333035 (96d:11071)

Department of Mathematics, Chung-Ang University, 221 Heukseok-dong, Dongjak-gu, Seoul 156-756, South Korea

E-mail address: imbh@cau.ac.kr