Heegner Points on Modular Elliptic Curves

By Hajime NAKAZATO

Department of Mathematics, Tokyo National College of Technology

(Communicated by Shokichi IYANAGA, M. J. A., Dec. 12, 1996)

Abstract: We consider an elliptic curve E with a modular parametrization $\varphi : X_0(N) \to E$. Under some conditions the images of Heegner points on $X_0(N)$ by φ are of infinite order.

1. Introduction. Let E be a modular elliptic curve of conductor N defined over $\boldsymbol{Q}$ with a parametrization $\varphi : X_0(N) \to E$ mapping the cusp ∞ of $X_0(N)$ to the origin of E which we consider as given in the following. Let E_n be the group of n-division points of E for an integer n.

If E has no complex multiplication over $\boldsymbol{C}$, then Serre [11] has shown that

$$\mathrm{Gal}(\boldsymbol{Q}(E_\ell)/\boldsymbol{Q}) \simeq \mathrm{Aut}_{\boldsymbol{F}_\ell}(E_\ell) \simeq \mathrm{GL}(2, \boldsymbol{F}_\ell)$$

for almost all primes ℓ (i.e., for all but a finite number of primes).

Definition. (a) If E has no complex multiplication, we define a finite set S_E of rational primes by

$$S_E := \{\ell ; \mathrm{Gal}(\boldsymbol{Q}(E_\ell)/\boldsymbol{Q}) \not\simeq \mathrm{Aut}_{\boldsymbol{F}_\ell}(E_\ell)\} \cup \{\ell ; \ell | N\} \cup \{2,3\}.$$

(b) If E has complex multiplication, we define a finite set S_E of rational primes by

$$S_E := \{\ell ; \ell | N\} \cup \{2,3\}.$$

Remark. For a semi-stable (modular) elliptic curve E without complex multiplication, we can use [11, Corollaire 1,p.308] to determine the set S_E.

Definition. Let K be an imaginary quadratic field of discriminant $-D$ which satisfies the following two conditions:

(1) Each prime factor ℓ of D is not contained in S_E.

(2) Each prime factor ℓ of N splits in K.

There are infinitely many imaginary quadratic fields K which satisfy these two conditions and whose class number h_K is greater than the degree $\deg(\varphi)$. From the second condition, there is an ideal $\mathfrak{n}$ of the integer ring $\mathcal{O}_K$ of K satisfying $\mathcal{O}_K/\mathfrak{n} \simeq \boldsymbol{Z}/N\boldsymbol{Z}$.

From now on we fix an imaginary quadratic field K with discriminant $-D$ which satisfies these two conditions.

Let $[\mathfrak{a}]$ be the ideal class of K which contains an ideal $\mathfrak{a}$. Let $x_1 = (\mathcal{O}_K, \mathfrak{n}, [\mathfrak{a}])$ be the complex point $(\boldsymbol{C}/\mathfrak{a}, \boldsymbol{C}/\mathfrak{a}\mathfrak{n}^{-1})$ of $X_0(N)$ [2], [4]. Let K_1 be the Hilbert class field of K. Then the theory of complex multiplication implies that the point x_1 is rational over K_1. Following [4], x_1 is called a Heegner point on $X_0(N)$ and its image $y_1 = \varphi(x_1)$ in $E(K_1)$ is called a Heegner point on E.

The following is our result with respect to y_1.

Theorem 1.1. *If $h_K > \deg(\varphi)$, then the Heegner point y_1 has infinite order.*

Kurčanov [9, Proposition, p.323] has proved that Heegner points have infinite orders in the case that D is a prime. Our theorem generalizes Kurčanov's Proposition.

Let y_K be $\mathrm{Tr}_{K_1/K}(y_1)$ contained in $E(K)$, where the sum is taken with respect to the group law on E. Gross and Zagier [3] have proved that if y_K has infinite order, then $L'(E/K, 1) \neq 0$. Kolyvagin [5], [6], [7], [8] has proved that if y_K has infinite order, then the Mordell-Weil group $E(K)$ has rank one and the Tate-Shafarevich group $Ш(E/K)$ is finite.

The following is our result with respect to y_K.

Theorem 1.2. *If y_K is a torsion point, then $y_K \in E(\boldsymbol{Q})$.*

We denote by z^ρ the complex conjugate of a point z in $E(\boldsymbol{C})$.

Corollary 1.3. *If $y_K^\rho \neq y_K$, then y_K has infinite order.*

2. Proof of theorems. The following lemma is known to specialists.

Lemma 2.1. $K(x_1) = K_1$.

Proof. For an ideal $\mathfrak{a}$ of $\mathcal{O}_K$ [12, Theorem 5.7 (iv)] asserts $K(j(\mathfrak{a})) = K_1$. Since the function field of $X_0(N)$ over $\boldsymbol{Q}$ is $\boldsymbol{Q}(j(z), j(Nz))$ [12, p.157]. From [4,I.2], if $\mathfrak{a} \simeq \boldsymbol{Z}\tau + \boldsymbol{Z}1$, $\mathrm{Im}(\tau) > 0$, then we have

$$\mathfrak{a}\mathfrak{n}^{-1} \simeq \boldsymbol{Z}\tau + \boldsymbol{Z}(1/N) \simeq \boldsymbol{Z}N\tau + \boldsymbol{Z}1.$$

Hence the coordinates $j(\mathfrak{a}) = j(\tau)$ and $j(\mathfrak{a}\mathfrak{n}^{-1}) = j(N\tau)$ of x_1 generate K_1 over K. □

Lemma 2.2. *If* $h_K > \deg(\varphi)$, *then* $y_1 \notin E(K)$.

Proof. If $y_1 \in E(K)$, then $y_1^{\sigma} = y_1$ for all $\sigma \in \mathrm{Gal}(K_1/K)$. Since φ is defined over $\boldsymbol{Q}$ and $y_1 = \varphi(x_1)$, we have for each $\sigma \in \mathrm{Gal}(K_1/K)$

$$\varphi(x_1^{\sigma}) = (\varphi(x_1))^{\sigma} = y_1^{\sigma} = y_1.$$

Thus $x_1^{\sigma} \in \varphi^{-1}(y_1)$ for each $\sigma \in \mathrm{Gal}(K_1/K)$, hence

$$\{x_1^{\sigma}\,;\, \sigma \in \mathrm{Gal}(K_1/K)\} \subseteq \varphi^{-1}(y_1).$$

Because of Lemma 2.1 $x_1^{\sigma} (\sigma \in \mathrm{Gal}(K_1/K))$ are mutually distinct. Hence we have

$$h_K = |\,\{x_1^{\sigma}\,;\, \sigma \in \mathrm{Gal}(K_1/K)\}\,| \leq |\,\varphi^{-1}(y_1)\,| \leq \deg(\varphi).$$

This contradicts with the assumption. □

Note. Assume that E has complex multiplication. Let $\mathcal{O}$ be $\mathrm{End}_{\bar{\boldsymbol{Q}}}(E)$, then $\mathcal{O} \otimes_{\boldsymbol{Z}} \boldsymbol{Q}$ is an imaginary quadratic field k with discriminant d_k and $\mathcal{O}$ is an order of k. Shimura [13] has shown that d_k divides the level N and $\mathrm{End}_{\bar{\boldsymbol{Q}}}(E) = \mathrm{End}_k(E)$. As E is defined over $\boldsymbol{Q}$, the class number of $\mathcal{O}$ is one. There are thirteen orders with class number one whose conductors are one, two or three [11, Example, p.295]. Let $\mathcal{O}_k$ be the maximal order of k, then $\mathcal{O} \otimes_{\boldsymbol{Z}} \boldsymbol{Z}_{\ell} = \mathcal{O}_k \otimes_{\boldsymbol{Z}} \boldsymbol{Z}_{\ell}$ for each prime $\ell > 3$.

Lemma 2.3. *Assume that each prime factor of* D *is not contained in* S_E, *then*

$$E_{tors}(K_1) = E_{tors}(\boldsymbol{Q}).$$

Proof. Let $y \in E_{tors}(K_1)$. Suppose that y has a finite order m.

Let us consider the case;

(i) where there is a prime factor ℓ of m such that $\ell \notin S_E$.

Let z be $(m/\ell)y$ in $E(K_1)$, then z is a point of order ℓ.

(a) Assume that E has no complex multiplication.

Since $\ell \notin S_E$, we have $\mathrm{Gal}(\boldsymbol{Q}(E_{\ell})/\boldsymbol{Q}) \simeq \mathrm{Aut}_{\boldsymbol{F}_{\ell}}(E_{\ell})$, which is transitive on all points of order ℓ. Thus $\{z^{\sigma}\,;\, \sigma \in \mathrm{Gal}(\boldsymbol{Q}(E_{\ell})/\boldsymbol{Q})\}$ generates E_{ℓ} as module.

For $\sigma \in \mathrm{Gal}(\boldsymbol{Q}(E_{\ell})/\boldsymbol{Q})$, we extend σ to an automorphism of the algebraic closure of $\boldsymbol{Q}$ in $\boldsymbol{C}$ denoted by the same σ. Since the extension $K_1/\boldsymbol{Q}$ is normal, we have $K_1^{\sigma} = K_1$. Hence $z^{\sigma} \in (E(K_1))^{\sigma} = E(K_1^{\sigma}) = E(K_1)$. Thus we have $E_{\ell} \subseteq E(K_1)$.

(b) Assume that E has complex multiplication by $\mathcal{O}$ as in Note.

We use the notations in Note. It is known that $E_{\ell} = \mathcal{O}z + \mathcal{O}z^{\rho}$. Since $\mathcal{O}z \subseteq E(kK_1)$ and $E_{\ell}^{\rho} = E_{\ell}$, we have

$$\mathcal{O}z^{\rho} = (\mathcal{O}z)^{\rho} \subseteq (E(kK_1))^{\rho} = E((kK_1)^{\rho}) = E(kK_1).$$

Therefore we have $E_{\ell} = \mathcal{O}z + \mathcal{O}z^{\rho} \subseteq E(kK_1)$.

Summing up all cases, we have $E_{\ell} \subseteq E(K_1)$ or $E_{\ell} \subseteq E(kK_1)$. Using the nondegeneracy of the Weil-pairing on E_{ℓ}, we have $\zeta_{\ell} = \exp(2\pi i/\ell) \in K_1$ or kK_1. Hence $\boldsymbol{Q}(\zeta_{\ell}) \subseteq K_1$ or kK_1. Since d_k devides N and $\ell \notin S_E$, the ramification index of ℓ in K_1 or in kK_1 is one or two. However the ramification index of ℓ in $\boldsymbol{Q}(\zeta_{\ell})$ is $\ell - 1 \geq 4$. This is a contradiction.

The other is the case;

(ii) where each prime factor ℓ of m is contained in S_E.

We include the case of $m = 1$. Let L be $\boldsymbol{Q}(E_m)$. Since $\mathrm{ord}(y) = m$, $y \in E_m$ thus $y \in E(L)$.

We claim that $L \cap K_1 = \boldsymbol{Q}$. In fact any ramified prime ℓ in $K_1/\boldsymbol{Q}$ divides D, which is not contained in S_E. Any ramified prime ℓ in $L/\boldsymbol{Q}$ divides N or m, which is contained in S_E. Hence $L \cap K_1$ is unramified over $\boldsymbol{Q}$.

As $y \in E(K_1) \cap E(L)$, we have $y \in E(\boldsymbol{Q})$. □

Proof of Theorem 1.1. Lemma 2.2 and Lemma 2.3 imply Theorem 1.1. □

Proof of Theorem 1.2. Since $y_K \in E(K)$, Lemma 2.3 implies Theorem 1.2. □

Remark 2.4. Let K_f be the ring class field with a conductor f. If each prime factor of f is not contained in S_E, then we have theorems for K_f instead of K_1 by a suitable reformulation.

3. Applications and remark. Let $-\varepsilon = \pm 1$ denote the sign in the functional equation for L-function $L(E/\boldsymbol{Q}, s)$. Let [0] be the 0-cusp of $X_0(N)$. In [1] Birch has proved the following:

Lemma 3.1.

$$y_K^{\rho} = \varepsilon y_K + h_K \varphi([0]).$$

Corollary 3.2. *If* $\varepsilon = -1$, *then*

$$y_K^{\rho} \neq y_K \Leftrightarrow y_K \textit{ has infinite order.}$$

Proof. $\Rightarrow$ follows from Corollary 1.3.

Drinfeld-Manin's theorem asserts that the image of [0], in the jacobian variety, is a torsin point. If $y_K^{\rho} = y_K$, then we have

$$2y_K = h_K \varphi([0]).$$

Hence y_K is a torsin point. $\square$

Corollary 3.3. *If* $\varepsilon = 1$, *then* $h_K\varphi([0]) = 0$ *and* $y_K^\rho = y_K$.

Proof. Assume that $y_K^\rho \neq y_K$. Let $E(K)^- = \{z \in E(K)\,;\, z^\rho = -z\}$. Corollary 1.3 implies that y_K has infinte order. In the case of $\varepsilon = 1$, Kolyvagin [5], [6], [7], [8] has proved that $\mathrm{rank}(E(K)^-) = 0$ and $\mathrm{rank}(E(\boldsymbol{Q})) = 1$.

However the point $y_K - y_K^\rho$ is contained in $E(K)^-$ and it has infinite order. Thus we have $y_K^\rho = y_K$. $\square$

Remark 3.4. In the case where E has no complex multiplication we can use the galois group structure in the proof of Lemma 2.3.

References

[1] B. J. Birch: Heegner points of elliptic curves. Symposia Math., no.15, pp.441–445 (1975).

[2] B. J. Birch and N. M. Stephens: Computation of heegner points. Modular Forms (ed. R. A. Rankin). Chichester, Ellis Horwood, pp.13–41 (1984).

[3] B. H. Gross and D. Zagier: Heegner points and derivatives of L-series. Invent. Math., **84**, 225–320 (1986).

[4] B. H. Gross: Heegner points on $X_0(N)$. Modular Forms (ed. R. A. Rankin). Chichester, Ellis Horwood, pp.87–106 (1984).

[5] B. H. Gross: Kolyvagin's work on modular elliptic curves. L-functions and Arithmetic (eds. J. Coates and M. J. Taylor). Proc. Duoham 1989, London Math. Soc. Lecture Note Ser., vol. 153, Cambridge Univ. Press, London and New York (1991).

[6] V. A. Kolyvagin: Finiteness of $E(\mathbf{Q})$ and Ш$(E, \mathbf{Q})$ for a subclass of Weil curves. Izv. Akad. Nauk SSSR Ser, Mat., **52**, 522–540 (1988): English transl., Math. USSR-Izv., **32**, 523–542 (1989).

[7] V. A. Kolyvagin: On the Mordell-Weil group and the Shafarevich-Tate group of Weil curves. Izv. Akad. Nauk SSSR Ser. Mat., **52**, 1154–1180 (1988); English transl., Math. USSR-Izv. **33**, 473–499 (1989).

[8] V. A. Kolyragin: Euler systems. The Grothendieck Festschrift. vol. II (A collection of articles written in honor of the 60th Birthday of Alexander Grothendieck), Birkhäuser, Basel, pp. 435–483 (1991).

[9] P. F. Kurčanov: Elliptic curves of infinite rank over Γ-extensions. Mat. Sbornik, **90**, (132), no.2 (1973): English transl., Math. USSR Sbornik, vol.19, no.2, pp.320–324 (1973).

[10] J. P. Serre: Complex multiplication. Algebraic Number Theory (eds. J.W.S. Cassels and A. Fröhlich). Academic Press (1967).

[11] J. P. Serre: Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. Invent, Math., **15**, 259–331 (1972).

[12] G. Shimura: Introduction to the Arithmetic Theory of Automorphic Functions. Princeton Univ. Press, Princeton (1971).

[13] G. Shimura: On elliptic curves with complex multiplication as factors of the jacobians of modular function fields. Nagoya Math., J., **43**, 199–208 (1971).