

modular 楕円曲線の Heegner 点

東京工業高等専門学校 中 里 肇 (Hajime Nakazato)

E-mail address: nakaz@tokyo-ct.ac.jp

1.

E を $\mathbb{Q}$ 上の modular 楕円曲線とし、 N をその導手とする。非自明な $\mathbb{Q}$ 有理写像 $\varphi: X_0(N) \rightarrow E$ が存在し $\text{cusp } \infty$ を E の 0 に移すとする。

(i) E が虚数乗法を持たないとき、有理素数の集合 S_E を次の様に定義する。

$$S_E := \{p; \text{Gal}(\mathbb{Q}(E_p)/\mathbb{Q}) \not\simeq \text{Aut}(E_p)\} \cup \{p; p|N\} \cup \{2, 3\}.$$

Serre の定理 [8] Théorème 3 により、 $\text{Gal}(\mathbb{Q}(E_p)/\mathbb{Q}) \simeq \text{Aut}(E_p)$ が有限個の素数 p を除き成立するので、 S_E は有限集合である。

(ii) E が虚数乗法を持つとき、 $\mathcal{O} := \text{End}_{\mathbb{Q}}(E)$ と置くと、 $k := \mathcal{O} \otimes \mathbb{Q}$ は虚 2 次体となる。(このような虚 2 次体は 9 個、order は 13 個ある [7] Example p295。) k の判別式を $-d$ とすると、 d は N の約数となる。 E に対して、有理素数の有限集合 S_E を次の様に定義する。

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

虚 2 次体 $K := \mathbb{Q}(\sqrt{-D})$ を判別式が $-D$ であり、次の 3 条件を満たすとする。

- (1) $\ell|D \Rightarrow \ell \notin S_E$.
- (2) $h_K > \deg(\varphi)$ (h_K は K の類数).
- (3) $\ell|N \Rightarrow \ell$ は K において分解する.

楕円曲線 E に対して、この 3 条件を満たす虚 2 次体 K は無限個存在する。

以後、modular 楕円曲線 E に対して K は上の 3 条件を満たすと仮定する。条件 (3) から、 K の整数環 $\mathcal{O}_K$ の整イデアル $\mathfrak{n}$ で、 $\mathcal{O}_K/\mathfrak{n} \simeq \mathbb{Z}/N\mathbb{Z}$ を満たすものが存在する。 K のイデアル $\mathfrak{a}$ に対して、modular 曲線 $X_0(N)$ の moduli 性質で定まる $\mathbb{C}$ 有理点を $x_1 = (\mathbb{C}/\mathfrak{a}, \mathbb{C}/\mathfrak{a}\mathfrak{n}^{-1})$ と定義する [2]。体 K_1 を K の Hilbert 類体とすると、虚数乗法論により、点 x_1 は K_1 有理点となり、 $X_0(N)$ の Heegner 点と呼ばれる。 $E(K_1)$ の点を $y_1 := \varphi(x_1)$ と定義する。点 y_1 を、modular 楕円曲線 E の Heegner 点と呼ぶことにする。

Theorem 1.1. Heegner 点 y_1 の位数は無限大である。

$E(K)$ の点を $y_K := \text{Tr}_{K_1/K}(y_1)$ と定義する。Kolyagin [4, 5, 6, 3] は、点 y_K の位数が無
限大ならば、Mordell-Weil 群 $E(K)$ の階数は 1 であり、Tate-Shafarevich 群 $\text{III}(E/K)$ は
有限であることを示した。 ρ は複素共役を表す。

Theorem 1.2. もし y_K の位数が有限ならば、 $y_K \in E(\mathbb{Q})$.

Corollary 1.3. もし $y_K^\rho \neq y_K$ ならば、点 y_K の位数は無限大である。

2.

次の Lemma は、既に知られていることである。

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

Proof. K のイデアル $\mathfrak{a}$ に対して、 $\mathbb{C}$ 上の楕円曲線 $\mathbb{C}/\mathfrak{a}$ は $K(j(\mathfrak{a}))$ 上で定義されたモデル
 E' を持ち、 $\mathcal{O}_K \simeq \text{End}(E')$ である。志村 [9] の Theorem 5.7 (iv) によって、 $K(j(\mathfrak{a})) = K_1$.

modular 曲線 $X_0(N)$ の $\mathbb{Q}$ 上の関数体が $\mathbb{Q}(j(z), j(Nz))$ であることは、よく知られてい
る [9] p157。Gross [2] の I.2. で述べられている様に、 $\mathfrak{a} = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, $\text{Im}(\omega_1/\omega_2) > 0$ 、 $\mathfrak{a}n^{-1} =$
 $\mathbb{Z}\omega_1 + \mathbb{Z}(\omega_2/N) \simeq \mathbb{Z}N\omega_1 + \mathbb{Z}\omega_2$. 従って、 x_1 の座標 $j(\mathfrak{a}) = j(\omega_1/\omega_2)$, $j(\mathfrak{a}n^{-1}) = j(N\omega_1/\omega_2)$
が、 K 上 K_1 を生成する。□

Lemma 2.2. $y_1 \notin E(K)$.

Proof. もし、 $y_1 \in E(K)$ ならば、 $y_1^\sigma = y_1$, $\forall \sigma \in \text{Gal}(K_1/K)$. 写像 φ は $\mathbb{Q}$ 上定義されて
いて、 $y_1 = \varphi(x_1)$ であるから、 $\varphi(x_1^\sigma) = (\varphi(x_1))^\sigma = y_1^\sigma = y_1$. 従って、 $x_1^\sigma \in \varphi^{-1}(y_1)$,

$$T := \{x_1^\sigma; \sigma \in \text{Gal}(K_1/K)\} \subseteq \varphi^{-1}(y_1).$$

Lemma 2.1 により、 $x_1^\sigma (\sigma \in \text{Gal}(K_1/K))$ は相異なるので、

$$h_K = |T| \leq |\varphi^{-1}(y_1)| \leq \deg(\varphi).$$

これは K の条件 (2) に矛盾する。□

Proof of Theorem 1.1.

Heegner 点 y_1 の位数が有限で、 $\text{ord}(y_1) = m$ であると仮定する。

(i) $\exists \ell | m$ s.t. $\ell \notin S_E$ の時:

ℓ を $\ell | m$, $\ell \notin S_E$ である素数とする。位数 ℓ の点 $z := (m/\ell)y_1 \in E(K_1)$ とおく。

$\sigma \in \text{Gal}(\mathbb{Q}(E_\ell)/\mathbb{Q})$ の $\text{Aut}(\bar{\mathbb{Q}})$ への拡張を $\tilde{\sigma}$ で表すことにする。

(a) E が虚数乗法を持たない時;

S_E の定義により、 $\ell \notin S_E$ から、 $\text{Gal}(\mathbb{Q}(E_\ell)/\mathbb{Q}) \simeq \text{Aut}(E_\ell)$. 従って、 $z^{\bar{\sigma}} (\forall \sigma \in \text{Gal}(\mathbb{Q}(E_\ell)/\mathbb{Q}))$ は E_ℓ を生成する。

拡大 $K_1/\mathbb{Q}$ は正規であるから、 $K_1^{\bar{\sigma}} = K_1$, $\forall \sigma \in \text{Gal}(\mathbb{Q}(E_\ell)/\mathbb{Q})$. 従って、 $z^{\bar{\sigma}} \in E(K_1)^{\bar{\sigma}} = E(K_1)$, $\forall \sigma \in \text{Gal}(\mathbb{Q}(E_\ell)/\mathbb{Q})$. 故に、 $E_\ell \subseteq E(K_1)$.

Weil-pairing を使うと、 $\zeta = \exp(2\pi i/\ell) \in K_1$. ところが、 ℓ の分岐指数を考えると、 $\mathbb{Q}(\zeta)$ においては $\ell - 1 \geq 4$ であるが、 K_1 においては $\ell \notin S_E$ より、1 または 2 である。これは、矛盾である。

(b) E が虚数乗法を持つ時;

Tate 加群 $T_\ell(E)$ は、 $\mathcal{O}_\ell := \mathcal{O} \otimes \mathbb{Z}_\ell$ 上自由で階数が1であり、 $E_\ell = T_\ell(E)/\ell T_\ell(E)$ であるから、 $E_\ell = \mathcal{O}t_1 = (\mathcal{O}/\ell\mathcal{O})t_1$ ($\exists t_1 \in E_\ell$). 従って、 $z = \alpha t_1 \exists \alpha \in \mathcal{O} - \ell\mathcal{O}$.

[b-1] ℓ が k で分解しないとき:

ℓ が素元であるから、 $\alpha \notin \ell\mathcal{O}$ より、 $\alpha + \ell\mathcal{O} \in (\mathcal{O}/\ell\mathcal{O})^*$. 従って、 $\mathcal{O}z = (\mathcal{O}/\ell\mathcal{O})z = (\mathcal{O}/\ell\mathcal{O})\alpha t_1 = (\mathcal{O}/\ell\mathcal{O})t_1 = E_\ell$. $\mathcal{O} = \text{End}_{\bar{\mathbb{Q}}}(E)$ の元は k 上有理的である[9] (5.1.3)p114 から、 $z \in E(K_1)$ より、 $E_\ell = \mathcal{O}z \subseteq E(kK_1)$.

[b-2] ℓ が k で分解するとき:

$\rho \in \text{Aut}(\bar{\mathbb{Q}})$ を複素共役とする。 $\mathcal{O}$ の類数が1であるから、素元 $\pi, \pi^\rho \in \mathcal{O}$ が存在して $\ell = \pi\pi^\rho$. また、 $\rho^2 = \text{id}$, $E_\ell^\rho = E_\ell$ より、 $t_1^\rho = \beta t_1 \exists \beta \in \mathcal{O}$ s.t. $\beta + \ell\mathcal{O} \in (\mathcal{O}/\ell\mathcal{O})^*$ であり、 $\beta^\rho t_1^\rho = t_1$.

もし、 $\alpha \notin \pi\mathcal{O} \cup \pi^\rho\mathcal{O}$ ならば、 $\alpha + \ell\mathcal{O} \in (\mathcal{O}/\ell\mathcal{O})^*$ となり、 $\mathcal{O}z = (\mathcal{O}/\ell\mathcal{O})z = (\mathcal{O}/\ell\mathcal{O})\alpha t_1 = (\mathcal{O}/\ell\mathcal{O})t_1 = E_\ell$.

もし、 $\alpha \in \pi\mathcal{O}$ ならば、 $\alpha t_1 = z \neq 0$ より、 $\alpha \notin \pi^\rho\mathcal{O}$ であるから、 $\alpha^\rho \in \pi^\rho\mathcal{O} - \pi\mathcal{O}$. 従って、 $\alpha\mathcal{O} + \alpha^\rho\mathcal{O} = \gamma\mathcal{O}$, $\exists \gamma \in \mathcal{O} - \pi\mathcal{O} \cup \pi^\rho\mathcal{O}$ であるから、 $\delta\alpha + \varepsilon\alpha^\rho = \gamma$, $\exists \delta, \varepsilon \in \mathcal{O}$. ところが、 $\mathcal{O}z + \mathcal{O}z^\rho \ni \delta z + \varepsilon\beta^\rho z^\rho = \delta\alpha t_1 + \varepsilon\beta^\rho\alpha^\rho t_1^\rho = \delta\alpha t_1 + \varepsilon\alpha^\rho t_1 = \gamma t_1$ であるから、 $E_\ell = \mathcal{O}t_1 = \mathcal{O}\gamma t_1 \subseteq \mathcal{O}z + \mathcal{O}z^\rho \subseteq E_\ell$ となり、 $\mathcal{O}z + \mathcal{O}z^\rho = E_\ell$.

もし、 $\alpha \in \pi^\rho\mathcal{O}$ ならば、 z の代わりに z^ρ を使うと同様な議論で同じ結果となる。

$\mathcal{O} = \text{End}_{\bar{\mathbb{Q}}}(E)$ の元は k 上有理的であり、 $z \in E(K_1)$ であるから、 $\mathcal{O}z \subseteq E(kK_1)$. $\mathcal{O}^\rho = \mathcal{O}$, $(kK_1)^\rho = kK_1$ から、 $E_\ell = \mathcal{O}z + \mathcal{O}z^\rho \subseteq E(kK_1)$.

総ての場合に、 $E_\ell \subseteq E(kK_1)$.

Weil-pairing を使うと、 $\zeta = \exp(2\pi i/\ell) \in kK_1$. ところが、 ℓ の分岐指数を考えると、 $\mathbb{Q}(\zeta)$ においては $\ell-1 \geq 4$ であるが、 $d|N$ であるから kK_1 においては $\ell \notin S_E$ より、1 または 2 である。これは、矛盾である。

(ii) $\forall \ell|m \Rightarrow \ell \in S_E$ の時 ($m=1$ を含む):

$\text{ord}(y_1) = m$ であるから、 $y_1 \in E_m$. $L = \mathbb{Q}(E_m)$ とすると、 $y_1 \in E(L)$.

$L/\mathbb{Q}$ において分岐する素数 ℓ は、 $\ell \in S_E$. $K_1/\mathbb{Q}$ において分岐する素数 ℓ は、 $\ell|D_K$. しかし、 K の条件 (1) により、 $\ell \notin S_E$.

従って、 $L \cap K_1$ は $\mathbb{Q}$ 上不分岐であるから、 $L \cap K_1 = \mathbb{Q}$. (もし、 $m=1$ ならば $L = \mathbb{Q}$.)

$y_1 \in E(K_1)$ かつ $y_1 \in E(L)$ であるから、 $y_1 \in E(\mathbb{Q})$. これは、Lemma 2.2 に矛盾する。

Proof of Theorem 1.2.

Heegner 点 y_K の位数が有限で、 $\text{ord}(y_K) = m$ であると仮定する。

(i) $\exists \ell|m$ s.t. $\ell \notin S_E$ の時:

Theorem 1.2 の証明と同じ議論で、矛盾がでる。

(ii) $\forall \ell|m \Rightarrow \ell \in S_E$ の時 ($m=1$ を含む):

Theorem 1.2 の証明と同じ議論で、 $y_K \in E(\mathbb{Q})$.

REFERENCES

1. Gross, B. H., and Zagier, D., *Heegner points and derivatives of L-series*, Invent. math. **84**(1986), pp. 225–320.
2. Gross, B. H., *Heegner points on $X_0(N)$* , in Modular Forms (Rankin, R. A, ed.) Chichester, Ellis Horwood, 1984, pp. 87–106.
3. ———, *Kolyagin's work on modular elliptic curves*, in L-functions and Arithmetic (Coates, J. and Taylor, M. J. eds.) Proc. Durham 1989, London Math. Soc. Lecture Note Ser., vol. 153, Cambridge Univ. Press, London and New York, 1991.
4. Kolyagin, V. A., *Finiteness of $E(\mathbb{Q})$ and $\text{III}(E, \mathbb{Q})$ for a subclass of Weil curves*, Izv. Akad. Nauk SSSR Ser. Mat. **52**(1988), pp. 522–540; English transl., Math USSR-Izv. **32**(1989), pp. 523–542.
5. ———, *On the Mordell-Weil group and the Shafarevich-Tate group of Weil curves*, Izv. Akad. Nauk SSSR Ser. Mat. **52**(1988), pp. 1154–1180; English transl., Math USSR-Izv. **33**(1989), pp. 473–499.
6. ———, *Euler systems*, in The Grothendieck Festschrift, vol. II (A collection of articles written in honor of the 60th Birthday of Alexander Grothendieck), Birkhäuser, Basel, 1991, pp. 435–483.
7. Serre, J.-P., *Complex multiplication* In Algebraic Number Theory, J. W. S. Cassels and A. Fröhlich, eds, Academic Press, 1968, pp. 292–296.

8. ———, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques* Inventiones math. **15**(1972), pp. 259-331.
9. Shimura, G., *Introduction to the Arithmetic Theory of Automorphic Functions*, Princeton Univ. Press, Princeton, 1971.