数理解析研究所講究録
925巻 1995年 105-109

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φ: $X_0(N) \to E$が存在しcusp ∞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。

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

Serreの定理[8]Théorème 3により、$\mathrm{Gal}(\mathbb{Q}(E_p)/\mathbb{Q}) \simeq \mathrm{Aut}(E_p)$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、$\mathcal{O} := \mathrm{End}_{\bar{\mathbb{Q}}}(E)$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 $y_K := \mathrm{Tr}_{K_1/K}(y_1)$ と定義する。Kolyvagin [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 $Ш(E/K)$ 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、$\mathcal{O}_K \simeq \mathrm{End}(E')$ 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、$\mathfrak{a} = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, $\mathrm{Im}(\omega_1/\omega_2) > 0$、$\mathfrak{a}\mathfrak{n}^{-1} = \mathbb{Z}\omega_1 + \mathbb{Z}(\omega_2/N) \simeq \mathbb{Z}N\omega_1 + \mathbb{Z}\omega_2$. 従って、$x_1$の座標 $j(\mathfrak{a}) = j(\omega_1/\omega_2)$, $j(\mathfrak{a}\mathfrak{n}^{-1}) = j(N\omega_1/\omega_2)$ 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、$y_1^\sigma = y_1, \quad \forall\sigma \in \mathrm{Gal}(K_1/K)$. 写像$\varphi$ 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、$x_1^\sigma \in \varphi^{-1}(y_1)$,

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

Lemma 2.1により、$x_1^\sigma(\sigma \in \mathrm{Gal}(K_1/K))$ 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、$\mathrm{ord}(y_1) = m$ 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。

$\sigma \in \mathrm{Gal}(\mathbb{Q}(E_\ell)/\mathbb{Q})$ の$\mathrm{Aut}(\bar{\mathbb{Q}})$ 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、$\mathrm{Gal}(\mathbb{Q}(E_\ell)/\mathbb{Q}) \simeq \mathrm{Aut}(E_\ell)$. 従って、$z^\sigma (\forall \sigma \in \mathrm{Gal}(\mathbb{Q}(E_\ell)/\mathbb{Q}))$は$E_\ell$を生成する。

拡大$K_1/\mathbb{Q}$は正規であるから、$K_1^\sigma = K_1, \quad \forall \sigma \in \mathrm{Gal}(\mathbb{Q}(E_\ell)/\mathbb{Q})$. 従って、$z^\sigma \in E(K_1)^\sigma = E(K_1), \quad \forall \sigma \in \mathrm{Gal}(\mathbb{Q}(E_\ell)/\mathbb{Q})$. 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、$\ell$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、$\mathcal{O}z = (\mathcal{O}/\ell\mathcal{O})z = (\mathcal{O}/\ell\mathcal{O})\alpha t_1 = (\mathcal{O}/\ell\mathcal{O})t_1 = E_\ell$. $\mathcal{O} = \mathrm{End}_{\bar{\mathbb{Q}}}(E)$ 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:

$\rho \in \mathrm{Aut}(\bar{\mathbb{Q}})$ 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、$\rho^2 = id$, $E_\ell^\rho = E_\ell$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$z^\rho$を使うと同様な議論で同じ結果となる。

$\mathcal{O} = \mathrm{End}_{\bar{\mathbb{Q}}}(E)$ 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、$\ell$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):

$\mathrm{ord}(y_1) = m$ 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、$\mathrm{ord}(y_K) = m$ 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. ———, *Kolybagin'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. Kolyvagin, V. A., *Finiteness of* $E(\mathbb{Q})$ *and* Ш$(E,\mathbb{Q})$ *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.