On the Mazur-Tate refined conjecture of BSD type

太田 和惟 (Kazuto Ota)*

慶應義塾大学

概　要

本稿は, 第12回数学総合若手研究集会 (2016年2月29日〜3月3日, 北海道大学) における著者の講演のテクニカルレポートである. 楕円曲線の基本事項と弱BSD予想の主張を簡単に復習した後で, BSD予想の群環版と見なせる, Mazur-Tateが定式化したBSD型精密化予想を紹介する. 主結果は, この予想の階数に関する部分を比較的弱い仮定のもとで証明したというものである.

1. BSD予想

1.1. 楕円曲線 (参考文献 [7])

体 K 上の楕円曲線 E とは, 方程式

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (a_i \in K) \tag{1.1}$$

に無限遠点 ∞ を付け加えて定義される射影的な非特異代数曲線である. 特徴的なのは, これが群構造をもつ曲線だということである. つまり, K-有理点全体の集合

$$E(K) := \{(x, y) \in K^2;\ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{\infty\}$$

がアーベル群の構造をもつ（無限遠点 ∞ が単位元となる）. 例えば K が複素数体 $\mathbb{C}$ の場合, $E(\mathbb{C})$ にはコンパクトリーマン面の構造が入り, 複素トーラス $\mathbb{C}/\Lambda$ ($\Lambda \subseteq \mathbb{C}$ は格子) に群構造込みで同型となることが知られている.

さて, 整数論的に興味深いのは, K が有理数体 $\mathbb{Q}$, あるいはその有限次拡大体の場合である. このとき, 次の定理が知られている:

定理 1.1 (cf. [7])**.** *K が $\mathbb{Q}$ の有限次拡大体のとき, $E(K)$ は有限生成アーベル群, つまり,*

$$E(K) \cong \mathbb{Z}^{\oplus r(E)} \oplus E(K)_{\mathrm{tors}}.$$

ここで, $r(E) = \mathrm{rank}(E(K)) \geq 0$ は整数, $E(K)_{\mathrm{tors}}$ は $E(K)$ のトーション元全体がなす有限アーベル群である.

以下では, $K = \mathbb{Q}$ 上の楕円曲線 E を固定する. このとき, 上の定理より, $E(\mathbb{Q}) \cong \mathbb{Z}^{\oplus r(E)} \oplus E(\mathbb{Q})_{\mathrm{tors}}$ と書ける. 有限アーベル群 $E(\mathbb{Q})_{\mathrm{tors}}$ の方はMazurによって完全に分類されている (cf. [7, VIII, Theorem 7.5]). 一方, 階数 $r(E)$ の方はまだまだわからないことが多く, 例えば, $\mathbb{Q}$ 上の楕円曲線を動かしたとき, $r(E)$ がどれくらい大きくなるかもわかっていない. この代数的な量である $r(E)$ が驚くべきことに, 解析的な L 関数 $L(E, s)$ の振る舞いと結びつくと予想しているのが次に述べる (弱)BSD予想である.

* e-mail: kazutoota@math.keio.ac.jp

1.2. BSD 予想

まず, L 関数の定義に必要な Hasse 不変量 $a_\ell(E)\in\mathbb{Z}$ について復習する. E が $\mathbb{Q}$ 上の楕円曲線であるということから, 適当な変数変換により方程式 (1.1) の係数が $a_i\in\mathbb{Z}$ となるようにできる. そのような方程式で, *discriminant* $\Delta\in\mathbb{Z}$ (の絶対値) が最小のものを固定する (cf. [7, VIII.8]). (以下, $\mathbb{Q}$ 上の楕円曲線を考えるときは常にこのような $\mathbb{Z}$ 係数の方程式を固定することとする.) このとき, 方程式 (1.1) を素数 ℓ に対し modulo ℓ することにより $\mathbb{F}_\ell$ 上の代数曲線を得る. さらに $\ell\nmid\Delta$ のとき, この代数曲線は非特異となり $\mathbb{F}_\ell$ 上の楕円曲線 $E\otimes\mathbb{F}_\ell$ を定める. これの $\mathbb{F}_\ell$-有理点全体の集合を $E(\mathbb{F}_\ell)$ とも書く. $\ell\nmid\Delta$ のときの $a_\ell(E)\in\mathbb{Z}$ を $a_\ell(E)=\ell+1-\#E(\mathbb{F}_\ell)$ で定義する. E の Hasse-Weil L 関数 $L(E,s)$ は次の形の無限積で定義される:

$$L(E,s)=\prod_{\ell:\text{素数}}\left(1-a_\ell(E)\ell^{-s}+\epsilon(\ell)\ell^{1-2s}\right)^{-1}=:\sum_{n\geq 1}\frac{a_n}{n^s}. \tag{1.2}$$

ここで, $\ell\nmid\Delta$ なら, $\epsilon(\ell)=1$ である ($\ell|\Delta$ については [7, Appendix C.16] 参照). Hasse の定理 $|a_\ell(E)|\leq 2\sqrt{\ell}$ より, (1.2) は $\mathrm{Re}(s)>3/2$ なる $s\in\mathbb{C}$ に対し収束することがわかる. さらに, Wiles, Taylor-Wiles らによって解決された志村谷山予想により, $L(E,s)$ は $\mathbb{C}$ 全体に解析接続される. 特に, $s=1$ での零点の位数 $\mathrm{ord}_{s=1}(L(E,s))$ が定義される. 弱 BSD 予想とは次の予想である:

予想 1.2 (Birch, Swinnerton-Dyer)**.** 等式

$$r(E)=\mathrm{ord}_{s=1}(L(E,s))$$

が成り立つ.

さらに, $s=1$ での Taylor 展開の主要項 $\lim_{s\to 1}\left(L(E,s)/(s-1)^{r(E)}\right)$ を $\#E(\mathbb{Q})_{\mathrm{tors}}$ や Tate-Shafarevich 群 $\text{Ш}(E/\mathbb{Q})$ の位数といった数論的不変量で記述する公式 (full BSD 予想) も予想されているがここでは詳しく述べない (cf. [7, Appendix C.16]).

2. BSD 型精密化予想

Mazur-Tate [4] によって定式化された BSD 型精密化予想は, $\mathbb{Q}$ 上の楕円曲線 E に対する $L(E,s)$ を Mazur-Tate 元という群環の元で置き換え, E の数論的不変量と結びつける予想である.

2.1. Mazur-Tate 元 (cf. [4])

非負整数 S に対し, $G_S=(\mathbb{Z}/S\mathbb{Z})^\times$ とおく. このとき, Mazur-Tate 元 $(\theta_S)_S\in\prod_S\mathbb{Q}[G_S]$ は次を満たす (記号の説明はすぐ下):

1. 導手 S の Dirichlet 指標 $\chi:G_S\to\mathbb{C}^\times$ に対し, χ を $\mathbb{Q}$ 線形に $\mathbb{Q}[G_S]\to\mathbb{C}$ に延長すると,
$$\chi(\theta_S)=\tau_S(\chi)\frac{L(E,\chi^{-1},1)}{\Omega^\pm},$$
2. 素数 ℓ に対し, $\pi_{S\ell/S}:\mathbb{Q}[G_{S\ell}]\to\mathbb{Q}[G_S]$ を自然な射影とすると, $\pi_{S\ell/S}(\theta_{S\ell})$ と θ_S の間には明示的な関係式がある.
3. ある正の整数 M が存在して, 任意の非負整数 S に対し $M\theta_S\in\mathbb{Z}[G_S]$.

ここで, $\zeta_S := \exp(2\pi i/S)$ で, Dirichlet 指標 $\chi : G_S \to \mathbb{C}^\times$ に対し,

- $\tau_S(\chi) := \sum_{a\in G_S} \chi(a)\zeta_S^a$,
- $L(E,\chi,s) := \prod_{\ell\nmid S:\text{素数}} (1 - a_\ell(E)\chi(\ell)\ell^{-s} + \epsilon(\ell)\chi(\ell)^2\ell^{1-2s})^{-1} = \sum_{(n,S)=1} \frac{a_n\chi(n)}{n^s}$.

また, Ω^+, Ω^- (定義は [4, Chapter 1] 参照のこと) は周期と呼ばれる複素数で次を満たす: 任意の Dirichlet 指標 χ に対し, $\dfrac{L(E,\chi,1)}{\Omega^\pm} \in \mathbb{Q}(\mathrm{Im}(\chi))$. ここで, 符号 $\pm$ は $\chi(-1)$ の符号と同じものをとる.

注意 2.1. Mazur-Tate 元は p 進 L 関数の精密化である. p 進 L 関数は, 導手が p べきの Dirichlet 指標 χ による捻りの特殊値 $L(E,\chi^{-1},1)/\Omega^\pm$ を全て“補間”するような p 進解析的関数として定義されるが (例えば, $p \nmid a_p(E)$ なら $\left(\varprojlim_{\pi_{p^n/p^{n-1}}} \mathbb{Z}_p[G_{p^n}]\right) \otimes \mathbb{Q}_p \cong \mathbb{Z}_p[[T]]^{\oplus p-1} \otimes \mathbb{Q}_p$ の元になる), 構成の一つは $\{\theta_{p^n}\}_n$ を適当に modify して（逆）極限をとるというものである. p 進 L 関数を巡る大きな予想は, BSD 予想の素朴な類似である p 進 BSD 予想と, p 進 L 関数と $\cup_{n\geq 1} E(\mathbb{Q}(\zeta_{p^n}))$ をガロワ作用込みで結びつける岩澤主予想がある. [4] では, これらの予想の部分的な精密化として, (θ_{p^n} だけでなく) 一般の θ_S に対して予想が定式化された. 本稿で扱うのは, このうち p 進 BSD 予想の精密化に当たる BSD 型精密化予想である. 次の小節では, 本講演における主定理に関係深い, 弱 BSD 予想の類似に関して説明する.

2.2. BSD 型精密化予想の（階数に関する部分の）主張

S を非負整数とし, $\mathbb{Q}$ の部分環 R を $\theta_S \in R[G_S]$ となるようにとる. I_S を $R[G_S]$ の augmentation イデアルとする. つまり $I_S = \ker\left(R[G_S] \to R;\ \sum_{\sigma\in G_S} a_\sigma\sigma \mapsto \sum_{\sigma\in G_S} a_\sigma\right)$. このとき, Mazur-Tate [4] は θ_S の自明指標での零点の位数が $r(E)$ 以上であると予想した:

予想 2.2 (Mazur-Tate [4])**.** $\theta_S \in I_S^{r(E)}$.

注意 2.3. 予想 1.2 とは異なり, 零点の位数が $r(E)$ より大きくなることがある, つまり $\theta_S \in I_S^{r(E)+1}$ が起こりうる. 例えば, $\#G_S \in R^\times$ なら, $I_S = I_S^2 = \cdots$.

3. 主結果

E を $\mathbb{Q}$ 上の楕円曲線とし, CM をもたないとする (i.e. $\mathrm{End}(E) = \mathbb{Z}$, cf. [7]). 以下の 3 つの条件全てを満たす素数 p を**許容素数**と呼ぶ:

1. $p \nmid 6(a_p(E)-1)\Delta\prod_{\ell\mid\Delta} c_\ell$ (c_ℓ については [7, Appendix C.16] 参照),
2. Tate 加群 $T_p(E) := \varprojlim_n E[p^n]$ からくるガロワ表現 $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}_{\mathbb{Z}_p}(T_p(E))$ が全射 ($\overline{\mathbb{Q}}$ は $\mathbb{Q}$ の代数閉包),
3. $p \geq r(E)$.

注意 3.1. Serre の結果を用いると, 許容素数の密度が 1 であることがわかる.

以下, 部分環 $R \subseteq \mathbb{Q}$ を, <u>非許容素数が R で全て可逆</u>になるようにとる. 主結果は次である:

定理 3.2 ([5]). S を次の $(*)$ を満たす素数 $\ell \nmid \Delta$ の *square-free* な積とする.

$$(*) \quad \text{任意の許容素数}\, p\, \text{に対し},\ E(\mathbb{F}_\ell)[p] \cong \{0\}, \mathbb{Z}/p\mathbb{Z}.$$

このとき,

$$\theta_S \in I_S^{r(E)}.$$

注意 3.3.

1. $(*)$ を満たす ℓ の密度は 0.997 以上であることが Chebotarev 密度定理を用いることでわかる.
2. 抽象的に部分環 R を取ったが, $E(\mathbb{Q})_{\mathrm{tors}} \neq \{0\}$ のときには, 非許容素数の個数は有限となり, (数値的に) 明示的に R をとることができる (cf. [5, Corollary 1.4]).
3. 定理 3.2 以前に予想 2.2 について既に知られていた結果を簡単に述べる. 簡単のため, p を許容素数とする. $\theta_{p^n} \in I_{p^n}^{r(E)} \otimes \mathbb{Z}_p$ が, $p \nmid a_p(E)$ のときは Kato[1] の結果から, $p | a_p(E)$ の場合は, Kato[1], Kobayashi[2], Pollack[6] の結果から導ける. Kurihara[3] は $p \nmid a_p(E)$ のとき, "$\mu = 0$ 予想" を仮定したうえで, $(S, \Delta) = 1$ なる S に対し, $\theta_S \in I_S^{r(E)} \otimes \mathbb{Z}_p$ を (含む定理を) 証明している. Tan[8] は full BSD 予想を仮定したうえで, 特別な S に対し, $\theta_S \in I_S^{r(E)}$ を示している.

予想 2.2 は弱 BSD 予想（予想 1.2）の類似だったが, full BSD 予想の類似も定式化されている. これに関して得られた結果を紹介する.

Mazur-Tate [4] は, Mazur-Tate 元の主要項 $\tilde{\theta}_S$ を θ_S の $I_S^{r(E)}/I_S^{r(E)+1}$ への像として定義し, これを, full BSD 予想のように $\text{Ш}(E/\mathbb{Q})$ や高さ関数, J_S で記述する予想を定式化した. ここで, J_S は次で定義される有限群である:

$$J_S = \operatorname{coker}\left(E(\mathbb{Q}) \to \left(\oplus_{\ell | S} E(\mathbb{F}_\ell)\right) \oplus \left(\oplus_{\ell | \Delta} E(\mathbb{Q}_\ell)/E_0(\mathbb{Q}_\ell)\right)\right).$$

定理 3.4 ([5]). p を許容素数とし, S を $\ell \equiv 1 \bmod p$ かつ $(*)$ を満たす ℓ の *square-free* な積とする. もし, $\tilde{\theta}_S \not\equiv 0 \bmod p(I_S^{r(E)}/I_S^{r(E)+1})$ なら,

$$\text{Ш}(E/\mathbb{Q})[p] = J_S[p] = 0.$$

参考文献

[1] K. Kato, p-adic Hodge theory and values of zeta functions of modular forms, *Cohomologies p-adiques et applications, arithmétiques. III, Astérisque* **295** (2004), ix, 117–290.

[2] S. Kobayashi, Iwasawa theory for elliptic curves at supersingular primes, *Invent. Math.* **152** (2003), 1–36.

[3] M. Kurihara, The structure of Selmer groups for elliptic curves and modular symbols, *Iwasawa theory 2012, Contrib. Math. Comput. Sci.* **7**, 317–356, Springer, Heidelberg, 2014.

[4] B. Mazur and J. Tate, Refined conjectures of the "Birch and Swinnerton-Dyer type", *Duke Math. J.* **54** (1987), 711–750.

[5] K. Ota, Kato's Euler system and the Mazur-Tate refined conjecture of BSD type, *arXiv*:1509.006821v1, submitted.

[6] R. Pollack, On the p-adic L-function of a modular form at a supersingular prime, *Duke Math. J.* **118** (2003), 523–558.

[7] J. H. Silverman, *The arithmetic of elliptic curves*, Second edition, *Graduate Texts in Mathematics* **106**, Springer, Dordrecht, 2009.

[8] K.-S. Tan, Refined theorems of the Birch and Swinnerton-Dyer type, *Ann. Inst. Fourier* (Grenoble) **45** (1995), 317–374.