数理解析研究所講究録
1154巻 2000年 33-43

supersingular reduction を持つ楕円曲線の岩澤理論

東京都立大学　　栗原 将人（Masato Kurihara）

1 序

次の有名な定理から始めよう。

Theorem 1.1 (Iwasawa 1959 [1]) K を代数体、p を素数とし、K_∞/K を $\mathbf{Z}_p$-拡大とする。K_∞/K の p^n 次中間体を K_n で表し、そのイデアル類群の p-成分（p-Sylow 部分群）を A_{K_n} で表すことにするとき、

$$\#A_{K_n} = p^{e_n}$$

と書くことにすると、ある $\lambda, \mu \in \mathbf{Z}_{\geq 0}$ と $\nu \in \mathbf{Z}$ が存在し、十分大きな n に対して

$$e_n = \lambda n + \mu p^n + \nu$$

が成立する。

この定理から岩澤理論は始まったと言ってよく、つまりこの定理は岩澤理論の最初の定理である。不変量 λ, μ に関して、K_∞/K が cyclotomic $\mathbf{Z}_p$-拡大のときは、$\mu = 0$ であることが岩澤先生により予想されており、

この予想は K が abel 体のときは Ferrero と Washington により証明されている。cyclotomic でない $\mathbf{Z}_p$-拡大については、$\mu > 0$ となることもある。

70 年代に入って、Mazur はイデアル類群に対して使われていた岩澤理論の手法を楕円曲線の Selmer 群に適用することにより、楕円曲線の整数論に大きな進歩をもたらした。特に次が成立することを示した。

Theorem 1. 2 (Mazur 1972 [2]) K を代数体、p を素数とし、cyclotomic $\mathbf{Z}_p$-拡大 K_∞/K の p^n 次中間体を K_n で表すことにする。E を K 上に定義された楕円曲線とし、p の上のすべての素点で ordinary reduction を持つとする。さらに次の二つを仮定する。

(a) Selmer 群の Pontrjagin daul $\mathrm{Sel}(E/K_\infty)^\vee$ は torsion $\Lambda = \mathbf{Z}_p[[\mathrm{Gal}(K_\infty/K)]]$-加群。

(b) すべての $n \geq 0$ に対して、Tate Shafarevich 群 $Ш(E/K_n)$ の p 成分 (p のべきで消える元全体) $Ш(E/K_n)\{p\}$ は有限。

このとき

$$\#Ш(E/K_n)\{p\} = p^{e_n}$$

と書くことにすると、ある $\lambda, \mu \in \mathbf{Z}_{\geq 0}$ と $\nu \in \mathbf{Z}$ が存在し、十分大きな n に対して

$$e_n = \lambda n + \mu p^n + \nu$$

が成立する。

上で現れた Selmer 群や Tate Shafarevich 群の定義は第 3 節で述べる。

この定理は Mazur の control theorem と呼ばれているものの帰結である。仮定に関しては、Tate Shafarevich 群は有限になるものと一般に予想さ

れていることを考えると、(b) はもっともな仮定だが、(a) が成立するためには上に仮定したように E が p の上のすべての素点で ordinary reduction を持つことが必要である。(そうでないと $\mathrm{Sel}(E/K_\infty)^\vee$ は torsion にならない。) また、十分であることが予想されている。このことに関して、現在では次が知られている。

Theorem 1.3 (Rubin, Kato) E を $\mathbf{Q}$ 上に定義された modular な楕円曲線とし、p で ordinary reduction を持つとする。$K/\mathbf{Q}$ を有限次 abel 拡大とし、K_∞/K を cyclotomic $\mathbf{Z}_p$-拡大とすると、Selmer 群の Pontrjagin daul $\mathrm{Sel}(E/K_\infty)^\vee$ は torsion $\Lambda = \mathbf{Z}_p[[\mathrm{Gal}(K_\infty/K)]]$-加群となる。

Theorem 1.1 , Theorem 1.2 の証明には本質的に torsion Λ-加群の理論が使われるので、Theorem 1.2 のような Tate Shafarevich 群の位数に関する公式を得るためには、ordinary の仮定をおくことは絶対に必要であった。そこで素朴な疑問として、

Theorem 1.2 の状況で ordinary の仮定をはずすと、Tate Shafarevich 群の位数はどう増えるのか？

ということが考えられる。この疑問に関しては、今までほとんど何も知られていなかった。ordinary の仮定をはずすと、K_∞ 上の Selmer 群の daul $\mathrm{Sel}(E/K_\infty)^\vee$ や Tate Shafarevich 群の dual $Ш(E/K_\infty)^\vee$ は巨大で、もはや torsion Λ-加群にならない。そこで、その $\mathrm{Gal}(K_\infty/K_n)$-coinvariant ももはや有限にはならず、岩澤理論の普通の方法が使えない。そのため、ordinary の仮定をはずしたときに、Tate Shafarevich 群の位数がどのように増えていくのか、ということに関しては、今まで一つの例すら知られていなかった。また、どのようになるべきか、という予想もたてられていなかった。

この稿の目的は、条件がついた特別の場合にではあるが、この疑問に答えることである。

2 主結果

Theorem 2.1 E を $\mathbf{Q}$ 上に定義された modular な楕円曲線、素数 p で supersingular reduction を持つとする。$L(E,s)$ を E の L 関数、Ω_E を Néron period とし、

$$p \nmid L(E,1)/\Omega_E$$

と仮定する（これが主な仮定である）。また、$\mathrm{Tam}(E) = \Pi_\ell(E(\mathbf{Q}_\ell) : E_0(\mathbf{Q}_\ell))$ を Tamagawa factor とし、p は $\mathrm{Tam}(E)$ を割らないと仮定する（Birch Swinnerton-Dyer 予想が正しければこれは最初の仮定から導かれる）。また、$p \geq 5$ とし、p 等分点へのガロア群の作用

$$\rho_{E[p]} : G_{\mathbf{Q}} = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathrm{Aut}(E[p]) \simeq GL_2(\mathbf{F}_p)$$

は全射であると仮定する。$K_\infty/\mathbf{Q}$ を有理数体の cyclotomic $\mathbf{Z}_p$-拡大とし、K_n を次数 p^n の中間体とする。$\Lambda = \mathbf{Z}_p[[\mathrm{Gal}(K_\infty/\mathbf{Q})]]$ とおく。このとき、

(1) K_∞ 上の Tate Shafarevich 群の p-成分の Pontrjagin dual $(Ш(E/K_\infty)\{p\})^\vee$ は Λ-加群として、Λ と同型である。

(2) すべての $n \geq 0$ に対して、$\mathrm{rank}\, E(K_n) = 0$。（Ribet の定理により $E(K_\infty)$ の torsion part は一般に有限だから、このことから $E(K_\infty)$ が有限であることがわかる。）

(3) すべての $n \geq 0$ に対して、Tate Shafarevich 群の p-成分 $Ш(E/K_n)\{p\}$ は有限である。その位数を p^{e_n} と書くことにすると、**すべての** $n \geq 0$ に対して、

$$e_n = [\lambda n + \mu p^n]$$

が成立する。ここに、

$$\lambda = -\frac{1}{2}, \qquad \mu = \frac{p}{p^2-1}$$

であり、$[*]$ はガウス記号である。

Remark 2.2 (1) Theorem 2.1 (3) の等式を具体的に書き下すと

$$\begin{aligned} &e_0 = 0, \qquad e_1 = 0 \\ &e_n = p^{n-1} + p^{n-3} + \ldots + p - \tfrac{n}{2} \qquad n\text{: 偶数} \geq 2 \\ &e_n = p^{n-1} + p^{n-3} + \ldots + p^2 - \tfrac{n-1}{2} \qquad n\text{: 奇数} \geq 3 \end{aligned}$$

となる。1月のシンポジウムで講演した際には、この具体的な形で結果を述べた。その際、伊原康隆先生に分数の不変量を使って結果を述べることを示唆して頂き、上の Theorem 2.1 (3) で述べたような形の定式化をすることができました。有益な示唆をして下さったことに関し、伊原先生にここに心から感謝致します。

(2) 上のように、E が p で supersingular reduction を持つときは、$Ш(E/K_\infty)\{p\}$ が巨大になる。岩澤理論では普通、K_∞ 上のものから K_n 上のものの情報を得るには、$\mathrm{Gal}(K_\infty/K_n)$ 不変部分（もしくは coinvariant）を考える。しかしたとえば上の定理の状況では、Theorem 2.1 (1) により、$(Ш(E/K_\infty)\{p\})^{\mathrm{Gal}(K_\infty/K_n)}$ は $\mathbf{Z}_p[\mathrm{Gal}(K_n/\mathbf{Q})]$ の双対と同型になり、従ってまだ大きな無限群である。$Ш(E/K_n)\{p\}$ は有限であるはずだから、$(Ш(E/K_\infty)\{p\})^{\mathrm{Gal}(K_\infty/K_n)}$ と $Ш(E/K_n)\{p\}$ には大きな差があることになる。(E が p で ordinary reduction を持つ場合は、$(Ш(E/K_\infty)\{p\})^{\mathrm{Gal}(K_\infty/K_n)}$ は $Ш(E/K_n)\{p\}$ に一般には一致しないが、かなり近い。) このように、

$Ш(E/K_\infty)\{p\}$ と、この群への $\mathrm{Gal}(K_\infty/K)$ 作用がわかったとしても、このことは $Ш(E/K_n)\{p\}$ の位数についての何の情報も与えず、ここに、supersingular の場合の難しさがあるのである。

(3) Theorem 2. 1 の仮定は、E が虚数乗法を持たなければ、ほとんどすべての supersingular prime について成り立つ。たとえば、$E = X_0(11)$ に対しては、supersingular なすべての奇素数 $p = 19, 29, \ldots$ に対して仮定はみたされる。

(4) E が p で ordinary reduction を持つ場合に、上に対応すると思われるのは、次の Mazur の定理である。

定理 (Mazur) E は p で good ordinary reduction を持つとし、$a_p = p + 1 - E(\mathbf{F}_p)$ とおくとき、$a_p \not\equiv 1 \pmod{p}$ であるとする (not anomalous)。また、p は $\mathrm{Tam}(E)$ を割らず、さらに $E(\mathbf{Q}) \otimes \mathbf{Z}_p = 0$、$Ш(E/\mathbf{Q})\{p\} = 0$ であると仮定する。このとき、すべての $n \geq 0$ に対して、$\mathrm{rank}\, E(K_n) = 0$、$Ш(E/K_n)\{p\} = 0$ となる。

イデアル類群に関しては、対応するのは次の岩澤先生の定理である。

定理 (Iwasawa) K を有限次代数体とし、$\mathbf{Z}_p$-拡大 K_∞/K で分岐する素点はただひとつ、しかもそれは完全分岐すると仮定する。K_n を K_∞/K の p^n 次中間体とし、A_{K_n} を K_n のイデアル類群の p Sylow 部分群とする。このとき、$A_K = 0$ であると仮定すると、すべての $n \geq 0$ に対して $A_{K_n} = 0$ となる。

それでは、上の定理のような仮定がみたされないもっと一般にはどうなっているのだろうか。このことに関しては、現在のところ（私は）次のように考えている。

Conjecture 2. 3 (1) E を $\mathbf{Q}$ 上に定義された楕円曲線、素数 $p \geq 5$ で supersingular reduction を持つとする。$K_\infty/\mathbf{Q}$ を有理数体の cyclotomic $\mathbf{Z}_p$-拡大とし、K_n を次数 p^n の中間体とする。Tate Shafarevich 群 $Ш(E/K_n)\{p\}$ の位数を p^{e_n} と書くことにする。このとき、ある有理数 $\lambda, \mu, \mu', \nu, \nu' \in \mathbf{Q}$ が存在して、十分大きな n に対して、

$$e_n = [\lambda n + \mu p^n + \nu] \qquad n \text{ が偶数のとき}$$
$$e_n = [\lambda n + \mu' p^n + \nu'] \qquad n \text{ が奇数のとき}$$

が成立する。

(2) 上でいつでも

$$\mu = \mu' = \frac{p}{p^2 - 1}$$

である。

上で予想を2つに分けたのは、(1) の方が確からしいからである。E が p で supersingular reduction を持つとき、p 等分点 $E[p]$ への $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ の作用が既約であることを考えて、(2) は ordinary のときの次の Greenberg の予想からの類推である。

Conjecture 2. 4 (Greenberg)　Mazur の定理（Theorem 1. 2）の状況で、E の p 等分点へのガロア作用 $\rho_{E[p]} : \mathrm{Gal}(\overline{K}/K) \longrightarrow \mathrm{Aut}(E[p])$ が既約なら、Theorem 1. 2 に現れる不変量 μ は $\mu = 0$ である。

3 証明について

Theorem 2. 1 (1) の証明は難しくないので、ここでは、Theorem 2. 1 (2), (3) の証明の概略について述べる。まず、第1節と第2節で使ってきた Selmer 群の定義をきちんと与えておこう。この稿で使う Selmer 群は E の p べき等分点全体 $E[p^\infty]$ に関する Selmer 群のことで、代数拡大 $F/\mathbf{Q}$ に対して、

$$\mathrm{Sel}(E/F) = \mathrm{Ker}(H^1(F, E[p^\infty]) \longrightarrow \prod_{v:\mathrm{all}} H^1(F_v, E(\overline{F_v})))$$

で定義される。ここに、v は F の素点をすべて走る。Tate Shafarevich 群の定義は

$$Ш(E/F) = \mathrm{Ker}(H^1(F, E(\overline{F})) \longrightarrow \prod_{v:\mathrm{all}} H^1(F_v, E(\overline{F_v})))$$

だから、よく知られているように

$$0 \longrightarrow E(F) \otimes \mathbf{Q}_p/\mathbf{Z}_p \longrightarrow \mathrm{Sel}(E/F) \longrightarrow Ш(E/F)\{p\} \longrightarrow 0$$

なる完全系列が存在する。そこで、Theorem 2. 1 (2), (3) を示すためには、

$$(*) \qquad \mathrm{ord}_p(\#\,\mathrm{Sel}(E/K_n)) = [-\frac{1}{2}n + \frac{p}{p^2-1}p^n]$$

を示せばよいことがわかる。

$k = \mathbf{Q}_p$、k_∞/k を cyclotomic $\mathbf{Z}_p$-拡大、k_n を p^n 次の中間体とする。k_n は K_n の p の上にある素点での完備化である。$T = T_p(E)$ を E の Tate 加群とし、$z_n \in H^1(K_n, T)$ を加藤和也先生により構成された（最良の）zeta element とする。z_n は L-関数の特殊値と関係し、また Euler system をなすことが加藤先生によって証明されている。特に、

$$(z_n) \in \varprojlim H^1(K_n, T)$$

である。z_n の $H^1(k_n, T)$ への像も z_n と書くことにする。最初に次の命題を証明する。

Proposition 3. 1 Theorem 2. 1 の状況で、自然な同型

$$\mathrm{Sel}(E/K_n)^\vee \simeq H^1(k_n, T)/(E(k_n) \otimes \mathbf{Z}_p + < z_n >)$$

が存在する。ここに、$< z_n >$ は z_n で生成される $\mathbf{Z}_p[\mathrm{Gal}(k_n/\mathbf{Q}_p)]$-部分加群である。

Proposition 3. 1 の証明はここでは述べない。上の命題により、$\mathrm{Sel}(E/K_n)$ と $\mathrm{Sel}(E/K_\infty)$ とを比較できるので、ordinary の場合との違いをはっきりさせるために、説明しておこう。p が supersingular のときには局所体 k_n 上の有理点で universal norm になるものが存在しない（どんな $m \geq n$ に対しても $E(k_m)$ からのノルムで書けるような $E(k_n)$ の点はない）。そこで、

$$\begin{aligned} \mathrm{Sel}(E/K_\infty)^\vee &= \varprojlim \mathrm{Sel}(E/K_n)^\vee \\ &\simeq \varprojlim H^1(k_n, T)/ < (z_n) > \end{aligned}$$

となる。$\varprojlim H^1(k_n, T) \simeq \Lambda \oplus \Lambda$ であり、z_n と L 関数との関係を使うと、我々の仮定の下では (z_n) が base の一部をなすことがわかる。そこで、$\mathrm{Sel}(E/K_\infty)^\vee$ が Λ と同型になる。一方、ordinary のときは、$\varprojlim E(k_n) \otimes \mathbf{Z}_p$ は消えず、$\mathrm{Sel}(E/K_\infty)^\vee$ が Λ-torsion となるのである。

Proposition 3. 1 の同型を使って、(*) を示す。$\geq$ と $\leq$ を両方示すことによって等号を得るという方針で示す。$\geq$ は formal group の理論等を使って示す。$\leq$ のポイントとなる部分を書いて終わりにしよう。

$D = D_{cris}(V_p(E))$ を E に対応する Dieudonne 加群とする。D は 2 次元 $\mathbf{Q}_p$ ベクトル空間で、Frobenius $\varphi : D \longrightarrow D$ を持つ。$\zeta_{p^{n+1}}$ を 1 の原始 p^{n+1} 乗根として、

$$\gamma_n : D \longrightarrow D \otimes \mathbf{Q}_p(\zeta_{p^{n+1}})$$

を

$$x \mapsto \frac{1}{p^{n+1}} \sum_{i=0}^{n} \zeta_{p^{n+1}}^{p^i} \varphi^{i-n-1}(x) + (1-\varphi)^{-1}(x)$$

で定義する。この写像は p-進 L-関数の構成と関係のある写像である。$\mathcal{G}_n = \mathrm{Gal}(\mathbf{Q}_p(\zeta_{p^{n+1}})/\mathbf{Q}_p)$ とおき、D の cup 積 $[,]$ を自然に

$$D \otimes \mathbf{Q}_p(\zeta_{p^{n+1}})[\mathcal{G}_n] \times D \otimes \mathbf{Q}_p(\zeta_{p^{n+1}})[\mathcal{G}_n] \longrightarrow \mathbf{Q}_p(\zeta_{p^{n+1}})[\mathcal{G}_n]$$

に延長しておく。$\exp^* : H^1(k_n, V_p(E)) \longrightarrow D \otimes k_n$ を dual exponential map（exponential map $D \otimes k_n \longrightarrow E(k_n) \otimes \mathbf{Q}_p \subset H^1(k_n, V_p(E))$ の双対として定義される写像）とし、$x \in D$ と $z \in H^1(k_n, V_p(E))$ に対して、

$$P(x,z) = [(\sum_{\sigma \in \mathcal{G}_n} \gamma_n(x)^\sigma \sigma), (\sum_{\sigma \in \mathcal{G}_n} \exp^*(\sigma(z))\sigma^{-1})]$$

と定義する。$P(x,z) \in \mathbf{Q}_p[\mathcal{G}_n]$ であることがわかる。

証明のポイントはこの $P(x,z)$ を使うことである。非常に大ざっぱに方針を述べる。x を固定し、$\mathcal{G}_n$ の第二種指標 $\psi : \mathcal{G}_n \longrightarrow \mathbf{Q}_p(\zeta_{p^n})$ に対して $\psi(P(x,z)) \in \mathbf{Q}_p(\zeta_{p^n})$ を考えることにより、$H^1(k_n, T)/(E(k_n) \otimes \mathbf{Z}_p + < z_n >)$ の ψ 成分 $(H^1(k_n, T)/(E(k_n) \otimes \mathbf{Z}_p + < z_n >))^\psi$ の位数についての情報を得る。ここで、z_n は L 関数の値 $L(E, \psi, 1)$ と結びついていることから、問題を $L(E, \psi, 1)/\Omega_E$ の p-進付置を計算することに最終的には帰着する。我々の仮定の下では、modular symbol の理論（Mazur, Tate, Stevens などの）によりこれが計算でき、$\mathrm{Sel}(E/K_n)$ の上からの評価ができるのである。

参考文献

[1] Iwasawa, K., On Γ-extensions of algebraic number fields, Bull Amer Math Soc 65 (1959), 183-226.

[2] Mazur, B., Rational points of abelian varieties with values in towers of number fields, Invent math 18 (1972), 183-266.