

# Kolyvagin による楕円曲線の Tate-Safarevič 群

についての仕事の紹介

東京都立大理 栗原 将人 (Masato Kurihara)

この稿は Kolyvagin の最近の論文 (preprint) "Euler systems" [1] の解説である。円分体 (あるいは楕円曲線の等分点  $E$  つけ加えて得られた体) の ideal 類群, あるいは岩澤の Main Conjecture について Kolyvagin の仕事については市村氏の解説に譲り, ここでは楕円曲線の Tate-Safarevič 群の有限性, あるいはその order を押さえるという仕事についての紹介をしたいと思う。Kolyvagin の言う Euler system という概念がいかによりよく働くかということをわかりやすく解説するために ここでは [1] を Rubin [3] 風に解釈し直して話を進める。このとき Gross [5] を参考にする。ただし [1] は内容がかなり豊富であり, ここに述べるのはその主要部分だけであり, [1] のすべてを紹介するわけではないことを最初に断っておく。

## Convention

Abel 群  $A$  に対して,  $n$  倍写像  $n$  核, 余核をそれぞれ  $nA$   $A/n$  と書く。

## §1. Birch Swinnerton-Dyer conjecture

ここでは有名な楕円曲線に関する Birch Swinnerton-Dyer 予想について復習する。  $K$  を代数体,  $E$  を  $K$  上定義された楕円曲線とするとき,  $E/K$  の  $L$ -関数  $L(E/K, s)$  が定義される (たとえば cf [6], [7]).  $L(E/K, s)$  は  $\operatorname{Re}(s) > \frac{3}{2}$  で正則である。

Conjecture . (Birch, Swinnerton-Dyer)  $L(E/K, s)$  は全平面に解析接続する。

1)  $L(E/K, s)$  の  $s=1$  での零点の order は  $\operatorname{rank} E(K)$  に等しい。

(Mordell Weil の定理により  $K$  有理点の群  $E(K)$  は有限生成 abel 群,  $\operatorname{rank} E(K)$  は  $r$  の rank である。)

2)  $L(E/K, s)$  の  $s=1$  での零点の order は  $r$  とすると

$$\lim_{s \rightarrow 1} \frac{L(E/K, s)}{(s-1)^r} = \frac{\# \text{III}(E/K) \cdot \det \langle \cdot, \cdot \rangle}{(\# E(K)_{\text{tors}})^2 \sqrt{|d_K|}} \cdot V_{\infty} V_{\text{bad}}$$

ここに  $\text{III}(E/K) := \operatorname{Ker}(H^1(K, E) \rightarrow \prod_{v: \text{all primes}} H^1(K_v, E))$  がこの話の主要 Tate-Safarevic 群,  $\det \langle \cdot, \cdot \rangle$  は height pairing による regulator,  $V_{\infty}$  は  $E$  の無限素点の様子に由来する数 (period),  $V_{\text{bad}}$  は  $E$  の bad reduction のところの様子に由来する数 (=  $\prod_{v: \text{finite}} (E(K_v) : E^0(K_v))$  ことに  $E^0(K_v)$  は reduction が smooth な点全体),  $d_K$  は  $K$  の判別式である。

1) について多くの部分的結果があるが, ここでは焦点を 2) に絞ることにする。

Remark 1.  $K$  の Dedekind zeta  $\zeta_K(s)$  の  $s=1$  での leading term

$$\lim_{s \rightarrow 1} \frac{\zeta_K(s)}{(s-1)} = \frac{h_K \cdot R_K}{\#M(K)^2 \sqrt{|d_K|}} \cdot 2^{r_1} (2\pi)^{r_2}$$

( $h_K$ : 類数,  $R_K$ : regulator) と比べると  $\#III(E/K)$  の類数にあたり、このことがわかる。

Remark 2. つい最近まで この予想が成立する楕円曲線の例は一本知られていなかった。これは  $III(E/K)$  が有限群となる例が一つ知られていなかったからである。ただし自然数  $n$  に対し  $\#_n III(E/K)$  が有限であることは昔から知られており (cf. [11 ページ]), 多くの例について計算されていた。

最初に  $\#III(E/K) < \infty$  なる例を与えたのは Rubin である。彼は虚二次体  $K$  上で定義された complex multiplication を持つ楕円曲線  $E$  ( $\text{End}(E) \otimes \mathbb{Q} = K$ ) に対し  $L(E/K, 1) \neq 0$  であれば  $III(E/K)$  は有限であることを示した ([4])。このとき key となったのは elliptic units の arithmetic と ideal 類群の annihilator を与える元を作る Kummer Thaine の idea (cf. [8], [3]) である。Euler system はこの Kummer Thaine の idea の一般化である。Euler system の与えを供、このおかげで  $E/K$  に対し  $L(E/K, 1) \neq 0$  ならば Birch Swinnerton-Dyer 予想をほぼ証明することになる。(Rubin の論文を準備中なのだそうです。)

## §2. Statement of the main results

$E \in \mathbb{Q}$  上で定義された楕円曲線, modular curve を parametrize

と仮定する。(Taniyama Weil 予想によれば  $\mathbb{Q}$  上の楕円曲線はすべて  $n$  倍値を持つ。) すなわち  $E$  の conductor  $\in N_0$  とし

$$\varphi: X_0(N_0) \rightarrow E$$

なる surjective morphism が存在するとする。

$E$  は  $\mathbb{Q}$  上定義と仮定しているが、Gross Zagier の公式 (cf. 6ページ) が虚二次体上にあるために、 $E$  を虚二次体  $K$  上の楕円曲線と見て Birch Swinnerton-Dyer 予想を考へる方が都合がよい。そこで  $-D \equiv \text{square} \pmod{4N_0}$ ,  $(D, 2N_0) = 1$  なる  $D > 0$  をとり判別式  $-D$  の虚二次体  $K = \mathbb{Q}(\sqrt{-D})$  を考へる。このとき Kolyvagin はこれを示した。

Theorem 1.  $L'(E/K, 1) \neq 0$  であるならば  $\text{III}(E/K)$  は有限群。

さらに  $\text{rank } E(K) = 1$ 。

Remark 1. 仮定が  $L(E/K, 1) = 0$  であり上の仮定は  $\text{order}_{s=1} L(E/K, s) = 1$  と同じである。

Remark 2. 「 $\text{III}(E/K)$  が有限」は「 $\text{III}(E/\mathbb{Q})$  が有限」を導く。これは  $n \cdot \text{III}(E/K) = 0$  或  $2n \cdot \text{III}(E/\mathbb{Q}) = 0$  を導くことによる。

Remark 3 Gross Zagier の公式 (6ページ) により、 $\text{rank } E(K) \geq 1$  はすでにわかっていた。よにより Birch Swinnerton-Dyer 予想 a 1) が  $L'(E/K, 1) \neq 0$  の仮定の下で確かめられたことになる。

Remark 4. Kolyvagin の前論文 [2] では  $L'(E/K, 1) \neq 0$  の仮定の下  $L(E/\mathbb{Q}, s)$  の関数等式 の符号が  $+1$  のとき  $\text{III}(E/\mathbb{Q})$  の有限性を示していた。Euler system を考えることにより、関数等式 の符号 についての仮定は不必要になる。たのである。

$\mathbb{Q}$  上の予想を  $E$  上から導くには

$$L(E/K, s) = L(E/\mathbb{Q}, s) \cdot L(E/\mathbb{Q}, \chi, s)$$

を用いる。ここに  $\chi$  は  $K/\mathbb{Q}$  に対応する Dirichlet 指標。

Corollary 1.  $\text{order}_{s=1} L(E/\mathbb{Q}, s) = 1$  であれば  $\text{III}(E/\mathbb{Q})$  は有限、さらに  $\text{rank } E(\mathbb{Q}) = 1$ 。

$\therefore$  Waldspurger の定理により  $L(E/\mathbb{Q}, \chi, 1) \neq 0$  なる  $K$  がとれ Th. 1 を適用できる。

Corollary 2.  $L(E/\mathbb{Q}, 1) \neq 0$  であれば  $\text{III}(E/\mathbb{Q})$  は有限、さらに  $\text{rank } E(\mathbb{Q}) = 0$  (つまり  $E(\mathbb{Q})$  は有限群)。

$\therefore$  最近証明された analytic conjecture を用いる  $\text{order}_{s=1} (L(E/\mathbb{Q}, \chi, s)) = 1$  なる  $K$  がとれ Th. 1 を適用できる。

次に  $\#\text{III}(E/K)$  の評価に進もう。簡単のため  $E$  は complex multiplication を持たないとし、次のような素数  $p$  の  $p$ -part を考えることにする。

Definition 素数  $p$  が  $E$  に対して admissible であるとは、

$p \neq 2$  かつ  $E$  を Tate module  $T_p(E)$  への作用  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{Aut}(T_p(E))$  が全射であるということ。  
 $\text{GL}_2(\mathbb{Z}_p)$

Serre の定理によりほとんどの素数 (有限個を除く) は admissible である。また Mazur の定理により  $N_0$  square-free であるならば  $p \geq 11$  ならば  $p$  は admissible である。

まず Gross Zagier の公式を思い出そう。

Th. (Gross Zagier)  $E, K \in \mathbb{C}$  とする

$$L'(E/K, 1) = V_\infty \cdot \hat{h}(y_K) / c^2 \cdot (\# \mathcal{O}_K^\times)^2 \sqrt{D}$$

ここに  $\hat{h}$  は canonical height,  $y_K \in E(K)$  は Heegner point (§3 に後述),  $c$  は  $\omega \in$  Néron differential とし,  $\varphi: X_0(N_0) \rightarrow E$  により  $c$  は  $c = \int \varphi^*(\omega) = c \sum a_n g^n \frac{dg}{g}$ ,  $\sum a_n g^n$  は normalized new-form, とする。自然数。

この式から  $L'(E/K, 1) \neq 0$  ならば Birch Swinnerton-Dyer 予想は次の型になる。

$$\# \text{III}(E/K) = (E(K) : \langle y_K \rangle)^2 / c^2 (\# \mathcal{O}_K^\times)^2 V_{\text{bad}}$$

ここに  $\langle y_K \rangle$  は  $y_K$  が生成する  $E(K)$  の部分群である。分母は一般に小さい数である。この式はほぼ  $\# \text{III}(E/K) \approx (E(K) : \langle y_K \rangle)^2$  と言え、と思う。

Theorem 2.  $L'(E/K, 1) \neq 0$  と仮定する。  $p \in$  admissible な素数とし  $y_K \in p^a E(K) \setminus p^{a+1} E(K)$  とする。  $\text{III}(E/K)[p] \in \text{III}(E/K)$  の  $p$ -part (  $p$  の中で消える元全体のなす部分群 ) とすると  $p^a \cdot \text{III}(E/K)[p] = 0$ ,  $\# \text{III}(E/K)[p] \leq p^{2a}$  が成立する。

Remark 1.  $L'(E/K) \neq 0$  とすると Gross Zagier の公式から  $y_k$  の位数は無限である。従って  $y_k \in p^a E(K) \setminus p^{a+1} E(K)$  をみたすような自然数  $a$  は必ず存在する。

Remark 2.  $(E(K):\langle y_k \rangle)$  が有限かどうかは最初にはわかっていない。そこで  $a$  を定義する  $a$  に上のような書き方をした  $a$  であるが、これは  $\text{ord}_p(\#(E(K):\langle y_k \rangle)) = a$  かつ  $a > 0$  である。特に Th. 2 の order について  $a$  の主張は  $\#(\coprod (E/K) \text{ p.p.}) \mid (E(K):\langle y_k \rangle)^2$  を導く。

Remark 3. admissible である  $p$  について  $\# \coprod (E/K) \text{ p.p.}$  について  $a$  のもう少し悪い評価を出すことはできる。(cf. [13])

§3. Heegner points の存在性:

§2 の記号をそのまま使う。  $K$  の ideal  $i \subset \mathcal{O}_K$  に対して  $\mathcal{O}_K/i \simeq \mathbb{Z}/N_0\mathbb{Z}$  なる  $N_0 \in 1$  とする。  $(n, N_0) = 1$  なる  $n$  に対して  $\mathcal{O}_n = \mathbb{Z} + n\mathcal{O}_K$ ,  $i_n = i \cap \mathcal{O}_n$  とおく。  $(\mathbb{C}/\mathcal{O}_n, \mathbb{C}/\mathcal{O}_n \rightarrow \mathbb{C}/i_n^{-1})$  は modular curve  $X_0(N_0)$  の  $\mathbb{C}$  有理点を定めるが complex multiplication の理論により  $\mathbb{C}$  の点は conductor  $n$  の ring class field  $K_n$  上に定義される。この点を  $x_n$  とおく。  $x_n \in X_0(N_0)(K_n)$ 。  $\varphi: X_0(N_0) \rightarrow E$  は parametrization とし  $y_n = \varphi(x_n)$  とおく。 §2 の  $y_k$  は  $N_{K_1/K}(y_1) = y_k$  により定義される。ここには  $N_{K_1/K}: E(K_1) \rightarrow E(K)$  は norm map。

Kolyvagin はすべて  $n$  について  $y_n$  を考えているが、定理の証明には特別な  $n$  だけを考える方が十分である。ここでは次のような  $n$  を考える。また簡単のため以下 admissible な  $p$  の  $p$  part を考えていくことにする。以下 admissible な  $p$  と自然数  $N$  (十分大きくとも) を fix する。

$$S = \{ \ell: \text{素数} \mid \ell \nmid NpDP, \text{Gal}(K(E[p^N])/\mathbb{Q}) \text{ において } \ell \text{ の} \\ \text{Frobenius 置換 Frobe の複素共役の conjugacy} \\ \text{class に属する} \}$$

と置く。ここには  $K(E[p^N])$  は  $K$  に  $E$  の  $p^N$  等分点をすべてつけ加えて得られる拡大である。以下  $n$  としては  $S$  の元の square-free な積のみを考えることにする。(ただし 1 も含む。)

$(y_n)$  は Kolyvagin の用語によれば Euler system である。[1] では Euler system という概念がいくつかの公理を満たすものとして定義されているが、それはまだあまり整理されたものではなく、ただ cyclotomic units, elliptic units, Gauss sum, Heegner points という4つの例をとりあげて扱うことができ、程度に抽象化したもののように見える。ただ Kolyvagin はこの idea をもっと、とっと一般化しようという考えは持っているようである。Euler system の公理のうち最も重要なものは Norm に関する性質である。 $(y_n)$  の場合、 $N_{K_{n\ell}/K_n}(y_{n\ell}) = a_\ell \cdot y_n$ ,  $a_\ell = \ell + 1 - \# E(\mathbb{F}_\ell)$  なる性質を満たす。(  $n\ell$  は  $S$  の元の squarefree な積と仮定している )

$n \in S$  である squarefree な積とすると  $\text{Gal}(K_n/K_1) \cong \prod_{l|n} \text{Gal}(K_l/K_1)$ ,  $\text{Gal}(K_l/K_1)$  は位数  $l+1$  の巡回群である。

$\text{Gal}(K_l/K_1)$  の生成元  $\sigma_l \in 1$  とし

$$D_l = \sum_{i=1}^l i \sigma_l^i, \quad D_n = \prod_{l|n} D_l$$

と置く。  $S$  を定義した  $D_n y_n \in (E(K_n)/p^N)^{\text{Gal}(K_n/K_1)}$  を示すことが出来る。次の字像による  $D_n y_n$  の像  $\in K(n)$  と書く。

$$\begin{array}{ccccc} (E(K_n)/p^N)^{\text{Gal}(K_n/K_1)} & \xhookrightarrow{\quad} & H^1(K_n, E[p^N])^{\text{Gal}(K_n/K_1)} & \xrightarrow{\quad} & H^1(K_1, E[p^N]) \\ \downarrow D_n y_n & & & & \downarrow \text{Cor } K_1/K \\ & & & & K(n) \in H^1(K, E[p^N]) \end{array}$$

$\mathbb{Z} = E[p^N]$  は  $E$  の  $p^N$  等分点の作る Galois module,  $\partial$  は Kummer sequence  $0 \rightarrow E[p^N] \rightarrow E \xrightarrow{p^N} E \rightarrow 0$  の boundary map, 自然な字像  $(*)$  は  $p$  に  $1, 2$  を仮定した同型。この元  $K(n)$  が市村氏の紹介の中の  $K_n$  と同じ役割を果たすのである。

$v \in K$  の素点とし、自然な字像による  $K(n)$  の  $H^1(K_v, E[p^N])$ ,  ${}_p H^1(K_v, E)$  への像  $\in$  られられ  $K(n)_v, \widetilde{K(n)}_v$  と書くことにする。

$$H^1(K, E[p^N]) \rightarrow H^1(K_v, E[p^N]) \rightarrow {}_p H^1(K, E)$$

$$K(n) \mapsto K(n)_v \mapsto \widetilde{K(n)}_v$$

Key Proposition 1)  $v \nmid n$  に対し  $\widetilde{K(n)}_v = 0$

2)  $v \in K$  の素点,  $l \mid v$  ( $l$ :素数),  $nl \in S$  である squarefree な積とすると。このとき任意の自然数  $m$  に対し

$$\widetilde{K(nl)}_v \in {}_p^m H^1(K_v, E) \iff K(n)_v \in {}_p^m H^1(K_v, E[p^N])$$

そう 1 つ重要な命題を述べる。

Proposition.  $E \in L(E/\mathbb{Q}, S)$  の関数等式の符号,  $n = l_1 \cdots l_g$  とする。  $k(n) \in H^1(K, E[p^N])^{(-1)^{g-1}E}$ 。ここに  $H^1(K, E[p^N])^\mu$  は  $(\mu = \pm 1)$   $H^1(K, E[p^N])$  の複素共役が  $\mu$  倍の  $\text{act}$  する部分。

このことから  $n = l_1 \cdots l_g$  とすると

$$\widetilde{k(nl)}_v \in {}_{p^N}H^1(K_v, E)^{(-1)^{g-1}E}, \quad k(n)_v \in H^1(K_v, E[p^N])^{(-1)^{g-1}E}$$

—  $\tilde{n}$   $l \in S$  かつ  $\tilde{n}$  は  $2$  の群は  $\tilde{n}$  に位数  $p^N$  の巡回群であることがわかる。位数  $p^N$  の巡回群に対し  $2$   $\text{ord}_p \in p$  の何回割れかにより  $0$  かつ  $N$  での整数を対応させる写像とする。この  $\tilde{n}$   $\text{Key Prop. 2)$  を述べることは  $\text{ord}_p(\widetilde{k(nl)}_v) = \text{ord}_p(k(n)_v)$  である。

#### §4. Galois cohomology についての準備

円分体  $K$  の類数 (a  $p$ -part) の予想される値で押さえられるといふことは Kolyvagin は証明した (cf. 市村氏の紹介), この  $\text{idea}$  は完全系列

$$K^\times/p^N \rightarrow \bigoplus \mathbb{Z}/p^N \rightarrow \text{Pic } \mathcal{O}_K/p^N \rightarrow 0 \quad (\text{Pic } \mathcal{O}_K: \text{ideal 類群})$$

を用い,  $K^\times/p^N$  の中に定義された  $k(n)$  という元が  $\bigoplus \mathbb{Z}/p^N$  の大部分を消してしもう。ということからできていた。ここでは  $\pm$  の完全系列の役割を果たす完全系列を作りたい。  $E, K, p, S$  などとは §3 の通りとする。

まず自然数  $m$  に対し  $\text{Selmer 群}$  をいっそのように

$$\text{Sel}(E/k)[m] := \text{Ker}(H^1(k, E[m]) \rightarrow \prod_{\text{all } v} H^1(k_v, E))$$

と定義する。定義から次の完全系列を得る。

$$(4.1) \quad 0 \rightarrow E(k)/m \rightarrow \text{Sel}(E/k)[m] \rightarrow {}_m\text{III}(E/k) \rightarrow 0$$

Remark. Galois cohomology の一般論により  $\text{Sel}(E/k)[m]$  は有限群である。従って weak Mordell Weil の定理と  ${}_m\text{III}(E/k)$  の有限性が出る。

次の完全系列の成り図式を考える。

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & \\
 & & \uparrow & & \uparrow & & \\
 & & \bigoplus_{p^N} H^1(k_v, E) & \longrightarrow & \text{Sel}(E/k)[p^N]^\vee & \longrightarrow & 0 \\
 & \nearrow & \uparrow & & \uparrow & & \\
 H^1(k, E[p^N]) & \longrightarrow & \prod H^1(k_v, E[p^N]) & \longrightarrow & H^1(k, E[p^N])^\vee & \longrightarrow & 0 \\
 & & \uparrow & & & & \\
 & & \prod E(k_v)/p^N & & & & \\
 & & \uparrow & & & & \\
 & & 0 & & & & 
 \end{array}$$

ここに横の完全列は Tate-Poitou の exact sequence,  $p$  について  
 の仮定から最後が全射となる。たゞは Kummer sequence から得  
 られる完全系列である。上の図式から次の完全列を得る。

$$(4.2) \quad H^1(k, E[p^N]) \rightarrow \bigoplus_{\text{all } v} {}_{p^N} H^1(k_v, E) \rightarrow \text{Sel}(E/k)[p^N]^\vee \rightarrow 0$$

これがこの § の最初に書いた ideal 類群の完全列と同じ役割  
 を果たす完全列である。

Remark  $p$  が admissible でないとき、(4.2) の 2 つめの写像は全  
 射にはならない。しかしこの余核の位数を  $N$  による倍数で押

とえることがでる。

### §5. 定理の証明

$y_k \in p^a E(K) \setminus p^{a+1} E(K)$  とする。  $y_k = p^a \cdot y'_k$   $y'_k \in E(K)$  と書く。(4.1)により  $y'_k$  は  $\text{Sel}(E/K)[p^N]$  の中で生成する部分群  $\in \langle y_k \rangle$  と書く。この目標は次を証明することである。

Theorem 3.  $A = \text{Sel}(E/K)[p^N] / \langle y_k \rangle$  とおくと

$$(1) \quad p^a \cdot A = 0$$

$$(2) \quad \# A \leq p^{2a}$$

まずこの定理から Th.1 のほとんどのと Th.2 が出ることを示そう。 $E(K)$  は有限生成 abel 群だから、ほとんどの  $p$  について  $a=0$  である。このような  $p$  に対して (1) は  $\text{Sel}(E/K)[p^N] = \langle y_k \rangle$  を導く。従って (4.1) により  $E(K)/p$  は  $y_k$  で生成され、 $\text{rank } E(K) = 1$ 。次に (2) はこのことより  $\# \text{III}(E/K)[p^a] \leq p^{2a}$  を導く。なお admissible でない  $p$  について、もっと悪い評価だが  $\# A \in N$  による数で押さえることがでる。かくて  $\text{III}(E/K)$  の有限性が出るのである。

Th.3 の証明の概略に進もう。 $\varepsilon \in L(E/\mathbb{Q}, s)$  の関数等式の符号とし、(4.2) の  $\varepsilon$ -part を  $T_\varepsilon$

$$(4.2)^\varepsilon \quad H^1(K, E[p^N])^\varepsilon \xrightarrow{\psi_1} \bigoplus_{p|N} H^1(K_p, E)^\varepsilon \xrightarrow{\psi_2} (\text{Sel}(E/K)[p^N])^{\vee\varepsilon} \rightarrow 0$$

を考える。 $x_1 \in (A^\vee)^\varepsilon$  をとり  $(\text{Sel}(E/K)[p^N])^{\vee\varepsilon}$  の元と見る。こ

のと  $\text{Cebotarev density theorem}$  により 次のような  $K$  の素点  $v_1$

$E$  とする ことが出来る。

1)  $v_1$  の下にある素数  $\ell_1$  とする ( $(\ell_1) = v_1 \cap \mathbb{Z}$ ) と  $\ell_1 \in S$

2)  $\psi_2(0, \dots, 0, u_1, 0, 0, \dots) = x_1$ , ここに  $(0, \dots, 0, u_1, 0, 0, \dots)$  は  $(v_1)$

$v_1$  の上にある  $u_1$  があり他はすべて 0 の  $\bigoplus_{p \mid N} H^1(K_v, E)^E$  の元。1)

から  $p \mid N$  の巡回群と見るが  $u_1$  はこの群の生成元。

3)  $(y_k)_{v_1} \notin p^{a+1} E(K_{v_1})$

このように  $v_1, \ell_1 \in E$  とする Key Prop. から  $\psi_2(k|\ell_1) = (0, \dots, 0, c_1, 0, 0, \dots)$  ここに  $\text{ord}_p(c_1) = \text{ord}_p(\widetilde{k|\ell_1}_{v_1}) = \text{ord}_p(k|\ell_1)_v = \text{ord}_p((y_k)_v) = a$  ( $\text{ord}_p$  は位数  $p^N$  の巡回群の元に対し  $p$  2 何回割れるかにより 0 から  $N$  までの整数を対応させる写像) 従って  $(4.2)^E$  により  $p^a x_1 = 0$ , 特には  $p^a A^E = 0$  である。

次に  $k(\ell_1) \in p^b H^1(K, E[p^N])$  とするより最大  $a, b \in \mathbb{Z}$  とする。

(つまり  $b$  は  $x_1, \ell_1$  による)  $a, b$  を使えば  $p^{a-b} x_1 = 0$  を示せる。—E part には  $a, b$  に関する完全系列を考へる。

$$(4.2)^{-E}: H^1(K, E[p^N])^{-E} \xrightarrow{\psi_1} \bigoplus_{p \mid N} H^1(K_v, E)^{-E} \xrightarrow{\psi_2} (\text{Sel}(E/K)[p^N])^{V-E} \rightarrow 0$$

$x_1' \in (A^V)^{-E}$  とする  $\check{\text{Cebotarev density}}$  により  $a, b$  なる  $v_1'$  とする ことが出来る。

1)  $v_1'$  の下にある素数  $\ell_1'$  とする  $\ell_1' \in S$

2)  $\psi_2(0, \dots, 0, u_1', 0, 0, \dots) = x_1'$  ここに  $u_1'$  は  $p \mid N$  の巡回群  $H^1(K_{v_1'}, E)^{-E} \simeq \mathbb{Z}/p^N$  の生成元 (i.e.  $\text{ord}_p u_1' = 0$ )

3)  $kl_1)_{v_1'} \notin P^{b+1} H^1(K_{v_1'}, E[P^N])$  (i.e.  $\text{ord}_p(kl_1)_{v_1'} = b$ )

4)  $k(l_1') = 0$

このとき  $kl_1 l_1')$  を考え  $\S 3$  の Key Prop. から  $\text{ord}_p(k\widetilde{l_1 l_1'})_{v_1} = \text{ord}_p(kl_1')_{v_1} = 0$ , 従,  $\Psi_1(kl_1 l_1') = (0, \dots, 0, \underset{(v_1')}{k\widetilde{l_1 l_1'})_{v_1}}, 0, 0, \dots)$ .  
 さらに Key Prop. により  $\text{ord}_p(k\widetilde{l_1 l_1'})_{v_1'} = \text{ord}_p(kl_1)_{v_1'} = b$ . 完全列  $(4.2)^{-\varepsilon}$  を考え  $p^b x_1' = 0$  を導く. 特に  $p^b A^{-\varepsilon} = 0$  である.  $b \leq a$  である, したがって  $\varepsilon$ -part とあわせて Th. 3 (1) が示された. (1) が示されたことにより  $\text{III}(E/K)_{p^N}$  は有限群である.

$N \geq a$  にはこれは  $A \simeq \text{III}(E/K)_{p^N}$  であることに注意してある.

(2) を示すには上の操作をくり返すのである.  $A^V$  の構造は  $(A^V)^{\varepsilon} \simeq A_1 \oplus \dots \oplus A_r$ ,  $A_i \simeq (\mathbb{Z}/p^{n_i})^{\oplus 2}$ ,  $(A^V)^{-\varepsilon} \simeq A_1' \oplus \dots \oplus A_r'$ ,  $A_i' \simeq (\mathbb{Z}/p^{n_i'})^{\oplus 2}$  とあり,  $x_1, \dots, x_r \in A_1, \dots, A_r$  の元で位数が  $p^{n_1}, \dots, p^{n_r}$  となる,  $x_1', \dots, x_r' \in A_1', \dots, A_r'$  の元で位数が  $p^{n_1'}, \dots, p^{n_r'}$  となる.  $\varepsilon$  の操作を続ける. すなわち  $x_1, x_1'$  に対して上のようにな  $l_1, l_1'$  をとる. さらに  $kl_1 l_1') \in P^c H^1(K, E[P^N])$  となるような最大の  $c$  をとる. このとき  $p^{b-c} x_1' = 0$ . さらに上と同様に  $l_2$  をうまくとり,  $kl_1 l_1' l_2)$  を考えることにし  $p^c x_2 = 0$  を示すことを得てくる. これをくり返せば,  $p^{a-b} x_1 = 0, p^{b-c} x_1' = 0, p^{c-d} x_2 = 0, p^{d-e} x_2' = 0, \dots$ , 従,  $a-b \geq n_1, b-c \geq n_1', c-d \geq n_2, \dots$ . 故に  $\sum n_i + \sum n_i' \leq a$ . よ,  $\# A \leq p^{2a}$  となる.

## References

- [1] V. A. Kolyvagin, Euler systems (preprint)
- [2] V. A. Kolyvagin, Finiteness of  $E(\mathbb{Q})$  and  $\text{III}(E, \mathbb{Q})$  for a subclass of Weil curves, Math. USSR Izvestija Vol 32 (1989) (英译)
- [3] K. Rubin, The Main Conjecture, appendix to Cyclotomic fields I and II by S. Lang (second edition) GTM 121
- [4] K. Rubin, Tate - Shafarevich groups and L-functions of elliptic curves with complex multiplication, Invent. math. 89 (1987)
- [5] B. Gross, Kolyvagin's work on modular elliptic curves (preprint)
- [6] D. Husemöller, Elliptic curves GTM 111
- [7] J. H. Silverman, The arithmetic of elliptic curves GTM 106
- [8] F. Thaine, On the ideal class groups of real abelian number fields, Ann. of Math. 128 (1988)