

RATIONAL POINTS ON QUADRATIC TWISTS OF AN ELLIPTIC CURVE

東北大理 佐藤 篤

1 序

k を有限次代数体とし, E/k を Weierstrass 方程式 $y^2 = f(x)$ で与えられた楕円曲線とする ($f(x) \in k[x]$ は 3 次式). 各 $d \in k^\times/k^{\times 2}$ に対し, E_d/k を $dy_d^2 = f(x_d)$ で与えられる楕円曲線とする. これは $k(\sqrt{d})/k$ に関する E の quadratic twist と呼ばれるものである (ただし $d \not\equiv 1 \pmod{k^{\times 2}}$ の場合). 与えられた $d \in k^\times/k^{\times 2}$ に対し, Mordell-Weil 群 $E_d(k)$ を計算する前にその階数 $r_d = \text{rank } E_d(k)$ が正か否かを知ることは易しくはない. 例えば, $r_d > 0$ となるような $d \in k^\times/k^{\times 2}$ の, 体 $k(\sqrt{d})$ の (類数のような) 数論的な不変量を用いた特徴づけは, 一般には知られていない.

以下, 全体を通し, $\mathbb{P}^1(k) = k \cup \{\infty\}$ の部分集合 Ξ に対し, 集合 $\{P \in E(\bar{k}) ; x(P) \in \Xi\}$ を $x^{-1}(\Xi)$ と書くことにする. $\Xi = \mathbb{P}^1(k)$ の場合には集合 $x^{-1}(\mathbb{P}^1(k))$ は次のような表示をもつ:

$$x^{-1}(\mathbb{P}^1(k)) = \{P \in E(\bar{k}) ; \{P, -P\} \text{ is } \text{Gal}(\bar{k}/k)\text{-stable}\} = \bigcup_{d \in k^\times/k^{\times 2}} \theta_d(E_d(k)).$$

ここで, $\theta_d : E_d \rightarrow E$ は $x = x_d, y = \sqrt{d}y_d$ によつて与えられる $k(\sqrt{d})$ 上の同型である. なお, 上の union は次の意味で殆んど disjoint である:

$$\theta_d(E_d(k)) \cap \theta_{d'}(E_{d'}(k)) = E[2](k) \quad \text{if } d \not\equiv d' \pmod{k^{\times 2}}.$$

さて, $H_{\mathbb{P}^1} : \mathbb{P}^1(\bar{k}) \rightarrow \mathbb{R}$ を standard absolute (exponential) height とし, $H_x = H_{\mathbb{P}^1} \circ x : E(\bar{k}) \rightarrow \mathbb{R}$ を x に関する height とする. このとき, 容易にわかるように,

$$(\ddagger) \quad \sharp\{P \in x^{-1}(\mathbb{P}^1(k)) ; H_x(P) \leq T\} \asymp T^{2[k:\mathbb{Q}]} \quad \text{as } T \rightarrow \infty.$$

一方, 各 $d \in k^\times/k^{\times 2}$ に対し, canonical height の理論より

$$(\dagger) \quad \#\{P \in \theta_d(E_d(k)) ; H_x(P) \leq T\} \asymp (\log T)^{r_d/2} \quad \text{as } T \rightarrow \infty$$

となることがわかる. これらを見比べることにより, $r_d > 0$ なる $d \in k^\times/k^{\times 2}$ が無数に多く存在することが直ちにわかる ([ST] やその中の文献にあるように, 楕円曲面のいくつかの section を specialize することにより, より精密な結果を得ることもできる). さらに, $\bigcup_{d \in k^\times/k^{\times 2}} \theta_d(E_d(k)_{\text{tor}})$ が有限集合であるということを使うと, 有限個の $d \in k^\times/k^{\times 2}$ を除いて $\theta_d(E_d(k)_{\text{tor}}) = E[2](k)$ が成り立つこともわかる. よって条件 $r_d > 0$ は, 有限個の例外を除けば, 条件 $\theta_d(E_d(k)) \neq E[2](k)$ と同値になる. つまり,

$$\mathcal{K} = \{k(P) ; P \in x^{-1}(\mathbb{P}^1(k))\}, \quad \mathcal{K}_+ = \{k(\sqrt{d}) ; d \in k^\times/k^{\times 2}, r_d > 0\}$$

と置くと,

$$\mathcal{K}_+ \subseteq \mathcal{K}, \quad \#\mathcal{K}_+ = \infty, \quad \#(\mathcal{K} - \mathcal{K}_+) < \infty.$$

代数体の類数と不定方程式の解との関係は長い間に渡って研究されており, その中には楕円曲線を用いたものも数多くある. ここでは本田平氏による結果 [H1] を引用する.

命題 1.1 (本田) $f(x) = 4x^3 - 27n^2$ (n は 0 でない有理整数) とし, ξ を次の 3 つの条件をみたす有理整数とする:

$$(C0) \quad \sqrt{f(\xi)} \notin \mathbb{Q}.$$

$$(C1) \quad F_\xi(z) = z^3 - \xi z + n \in \mathbb{Z}[z] \text{ は } \mathbb{Q} \text{ 上既約.}$$

$$(C2) \quad (\xi, 3n) = 1.$$

このとき, 2 次体 $\mathbb{Q}(\sqrt{f(\xi)})$ の類数は 3 の倍数.

容易にわかるように, 条件 (C0), (C1) をみたさない $\xi \in \mathbb{Z}$ はいずれも有限個しか存在しない:

$$\#\{\xi \in \mathbb{Z} ; \sqrt{f(\xi)} \in \mathbb{Q}\} = \#\{(\xi, \eta) \in \mathbb{Z}^2 ; \eta^2 = f(\xi), \eta \geq 0\} < \infty,$$

$$\#\{\xi \in \mathbb{Z} ; F_\xi(z) \text{ is reducible over } \mathbb{Q}\} = \#\{(\zeta^2 + n\zeta^{-1} ; \zeta \in \mathbb{Z}, \zeta \neq 0\} \cap \mathbb{Z} < \infty.$$

従って, 条件 (C0)–(C2) をみたすような $\xi \in \mathbb{Z}$ 全体のなす集合を Ξ と置くと, 任意の $P \in x^{-1}(\Xi)$ に対して $3|h_{\mathbb{Q}(P)}$ が成り立ち, また, 集合 $x^{-1}(\Xi)$ の “大きさ” は次のように評価される:

$$\#\{P \in x^{-1}(\Xi) ; H_x(P) \leq T\} \sim 2\#\{\xi \in \mathbb{Z} ; (\xi, 3n) = 1, |\xi| \leq T\} \asymp T \quad \text{as } T \rightarrow \infty.$$

これと漸近公式 (‡), (†) を見比べることにより, $x^{-1}(\mathbb{P}^1(\mathbb{Q}))$ の点 P の中で $\mathbb{Q}(P)$ の類数が 3 で割り切れるものは少なからずあることがわかる.

以上の結果の拡張として次が得られた:

定理 1.2 $f(x) = 4x^3 - 27n^2$ (n は 0 でない k 内の整数) とし, Ξ^* を次の 2 つの条件をみたす $\xi \in k$ 全体のなす集合とする:

(C1)* $F_\xi(z) = z^3 - \xi z + n \in k[z]$ は k 上既約.

(C2)* $3n$ の k 内の全ての素因子 $\mathfrak{p}$ に対し, $\text{ord}_{\mathfrak{p}}(\xi) \leq 0$.

このとき:

(i) 任意の $P \in x^{-1}(\Xi^*)$ に対し, 体 $k(P)$ の類数は 3 の倍数.

(ii) $k = \mathbb{Q}$ の場合には,

$$\#\{P \in x^{-1}(\Xi^*) ; H_x(P) \leq T\} = \frac{24}{\pi^2} \left(\prod_{\substack{p \text{ prime} \\ p|3n}} \frac{p}{p+1} \right) T^2 + O(T \log T) \quad \text{as } T \rightarrow \infty.$$

この定理の証明は 4 節と 5 節で与える. 雑な言い方をすると, 定理前半の証明は Weak Mordell-Weil Theorem の証明に深く関係したものであり, 本田氏の方法を幾何学的にしたものとみなすことができる.

上の定理と

$$\#\{P \in x^{-1}(\mathbb{P}^1(\mathbb{Q})) ; H_x(P) \leq T\} = \frac{24}{\pi^2} T^2 + O(T \log T) \quad \text{as } T \rightarrow \infty$$

($k = \mathbb{Q}$ の場合の (‡) の正確な形) とにより次を得る:

系 1.3 $k = \mathbb{Q}$ の場合, $\mathbb{Q}(P)$ の類数が 3 で割り切れるような点 $P \in x^{-1}(\mathbb{P}^1(\mathbb{Q}))$ の全体は $x^{-1}(\mathbb{P}^1(\mathbb{Q}))$ の中で正の密度をもつ:

$$\liminf_{T \rightarrow \infty} \frac{\#\{P \in x^{-1}(\mathbb{P}^1(\mathbb{Q})) ; 3|h_{\mathbb{Q}(P)}, H_x(P) \leq T\}}{\#\{P \in x^{-1}(\mathbb{P}^1(\mathbb{Q})) ; H_x(P) \leq T\}} \geq \prod_{\substack{p \text{ prime} \\ p|3n}} \frac{p}{p+1}.$$

いま, $\mathcal{K}$ の 2 つの部分集合

$$\mathcal{K}_3 = \{k(P) ; P \in x^{-1}(\mathbb{P}^1(k)), 3|h_{k(P)}\}, \quad \mathcal{K}(\Xi^*) = \{k(P) ; P \in x^{-1}(\Xi^*)\}$$

を考える. このとき, 以上で述べた結果は $\mathcal{K}_3 \cap \mathcal{K}_+$ が $\mathcal{K}_+$ の中で (適当な意味で) 正の “密度” をもっているということを示唆しているように思われる. 実際, 定理の前半は $\mathcal{K}(\Xi^*) \subseteq \mathcal{K}_3$ が成り立つということに他ならないし, 後半より

$$\#\mathcal{K}(\Xi^*) = \infty, \quad \#(\mathcal{K}(\Xi^*) - \mathcal{K}_+) < \infty$$

が従う. これは $x^{-1}(\Xi^*)$ が $x^{-1}(\mathbb{P}^1(\mathbb{Q}))$ の十分大きな部分集合であるということを述べている. しかしながら, このことから $\mathcal{K}(\Xi^*)$ の $\mathcal{K}$ の中での大きさを評価することはできない.

2 準備

本節では quadratic twist と同種写像から生じる体の拡大について, よく知られている事実を列挙する.

2.1 Quadratic Twist

k を有限次代数体とし, E/k を楕円曲線とする. $d \in k^\times/k^{\times 2}$ に対し, $\chi_d : \text{Gal}(\bar{k}/k) \rightarrow \text{Aut}(E)$ を次により定義される準同型写像とする:

$$\chi_d(\sigma) = \begin{cases} 1 & \text{if } \sqrt{d}^\sigma = \sqrt{d} \\ -1 & \text{if } \sqrt{d}^\sigma = -\sqrt{d} \end{cases}.$$

このとき, 楕円曲線 E_d/k と $k(\sqrt{d})$ 上の同型写像 $\theta_d : E_d \rightarrow E$ で

$$\chi_d(\sigma) = \theta_d^\sigma \circ \theta_d^{-1} \quad \text{for all } \sigma \in \text{Gal}(\bar{k}/k)$$

となるようなものが存在する. 楕円曲線 E_d と同型写像 θ_d は d により k 上の同型の差を除いて一意的に定まり, E_d は E の $k(\sqrt{d})/k$ に関する quadratic twist と呼ばれる (ただし, $d \not\equiv 1 \pmod{k^{\times 2}}$ の場合. $d \equiv 1 \pmod{k^{\times 2}}$ の場合には E_d は E と k 上同型になる). さらに, θ_d による $E_d(k)$ の像は $E(k(\sqrt{d}))$ の中で

$$\theta_d(E_d(k)) = \{P \in E(k(\sqrt{d})) ; P^\sigma = \chi_d(\sigma)P \text{ for all } \sigma \in \text{Gal}(\bar{k}/k)\}$$

と特徴づけられる. これより

$$\bigcup_{d \in k^\times/k^{\times 2}} \theta_d(E_d(k)) = \{P \in E(\bar{k}) ; \{P, -P\} \text{ is } \text{Gal}(\bar{k}/k)\text{-stable}\}$$

ならびに

$$\theta_d(E_d(k)) \cap \theta_{d'}(E_{d'}(k)) = E[2](k) \quad \text{if } d \not\equiv d' \pmod{k^{\times 2}}$$

を得る.

E が $y^2 = f(x)$ なる形の Weierstrass 方程式 ($f(x) \in k[x]$ は 3 次式) により与えられているときには, E_d の方程式として $dy_d^2 = f(x_d)$ をとることができて, そのとき同型写像 $\theta_d: E_d \rightarrow E$ は $x = x_d$, $y = \sqrt{d} y_d$ により与えられる.

2.2 同種写像から生じる体の拡大

k を有限次代数体, E/k (resp. $\bar{E}/k$) を $y^2 = f(x)$ (resp. $v^2 = g(u)$) なる形の Weierstrass 方程式 ($f(x) \in k[x]$, $g(u) \in k[u]$ は 3 次式) で与えられた楕円曲線とし, $\lambda: \bar{E} \rightarrow E$ を k 上の同種写像とする. また, $\text{Ker } \lambda$ は $\bar{E}(k)$ に含まれ, $l = \deg \lambda$ は奇素数であると仮定する. このとき, 有理関数 $\lambda_x(u), \lambda_y(u) \in k(u)$ が存在して, λ は

$$x = \lambda_x(u), \quad y = \lambda_y(u)v$$

により与えられる. l が奇数であることより, $\lambda_x(u)$ と $\lambda_y(u)$ は条件

$$(\lambda_x^{(1)}(u), \lambda_y^{(2)}(u)) = (\lambda_y^{(1)}(u), \lambda_x^{(2)}(u)) = 1$$

および

$$\deg \lambda_x^{(1)}(u) = l, \quad \deg \lambda_y^{(1)}(u) = \frac{3(l-1)}{2}, \quad \deg \lambda^{(2)}(u) < \frac{l}{2}$$

をみたす多項式 $\lambda_x^{(1)}(u), \lambda_y^{(1)}(u), \lambda^{(2)}(u) \in k[u]$ を用いて

$$\lambda_x(u) = \frac{\lambda_x^{(1)}(u)}{\lambda^{(2)}(u)^2}, \quad \lambda_y(u) = \frac{\lambda_y^{(1)}(u)}{\lambda^{(2)}(u)^3}$$

と表せることがわかる.

$\xi \in k$ に対し,

$$\Lambda_\xi(u) = \lambda_x^{(1)}(u) - \xi \lambda^{(2)}(u)^2 \in k[u]$$

と置く. このとき, $(x, y) = (\xi, \eta)$ により与えられる $P \in x^{-1}(\mathbb{P}^1(k)) - E[2](k)$ に対し,

$$\lambda^{-1}(P) = \left\{ (u, v) = \left(\zeta, \frac{\eta}{\lambda_y(\zeta)} \right) ; \zeta \in \bar{k}, \Lambda_\xi(\zeta) = 0 \right\}$$

が成り立つ ($\Lambda_\xi(\zeta) = 0$ は $\lambda_y^{(1)}(\zeta) \neq 0$ と $\lambda^{(2)}(\zeta) \neq 0$ を含むことに注意). よって $\Lambda_\xi(u)$ は重根をもたず, $k(\lambda^{-1}(P))$ は $\Lambda_\xi(u)$ の $k(P) = k(\eta)$ 上の分解体になる.

$P \in E(\bar{k})$ に対し, 写像

$$\text{Gal}(k(\lambda^{-1}(P))/k(P)) \longrightarrow \text{Ker } \lambda, \quad \sigma \longmapsto Q^\sigma - Q$$

(Q は $\lambda^{-1}(P)$ 内の任意の点) は単射準同型になる. l は素数であるから, $k(\lambda^{-1}(P))/k(P)$ は $P \in \lambda(\overline{E}(k(P)))$ か否かに従って 1 次か l 次の巡回拡大になり, 任意の $Q \in \lambda^{-1}(P)$ に対して $k(\lambda^{-1}(P)) = k(P, Q)$ が成り立つ. さらに, 容易にわかるように:

補題 2.1 上の記号と仮定の下で, x -座標が ξ であるような $P \in x^{-1}(\mathbb{P}^1(k)) - E[2](k)$ に対して次の条件は同値:

- (a) $\lambda^{(2)}(\zeta) \neq 0$ なる $\zeta \in k$ が存在して, $\xi = \lambda_x(\zeta)$.
- (b) $\Lambda_\xi(u)$ は k 上可約.
- (c) $k(\lambda^{-1}(P)) = k(P)$.

3 命題 1.1 の証明

本節では, 命題 1.1 の本田氏による証明の概略を述べる. [H1] に述べられているように, 彼の証明は楕円曲線の同種写像を用いるものである. $\overline{E}/\mathbb{Q}$ を Weierstrass 方程式 $v^2 = 4nu^3 + 1$ で与えられる楕円曲線とし, $\lambda: \overline{E} \rightarrow E$ を

$$x = \frac{1 + nu^3}{u^2}, \quad y = \frac{2 - nu^3}{u^3} v$$

により与えられる $\mathbb{Q}$ 上の同種写像とする. すると, $\deg \lambda = 3$ であつて, $\text{Ker } \lambda = \{(u, v) = (0, 1), (0, -1)\} \cup \{O\}$ は $\overline{E}(\mathbb{Q})$ に含まれるから, 2.2 節の議論を適用することができる. $\lambda_x^{(1)}(u)$, $\lambda_x^{(2)}(u)$ としてはそれぞれ $1 + nu^3$, u をとることができて, このとき

$$\Lambda_\xi(u) = nu^3 - \xi u^2 + 1$$

となる. x -座標が ξ であるような $P \in x^{-1}(\mathbb{Q})$ に対し, 条件 (C0) は $[\mathbb{Q}(P) : \mathbb{Q}] = 2$ と同値である. また, 補題 2.1 と

$$F_\xi(z) = z^3 \Lambda_\xi\left(\frac{1}{z}\right)$$

により, $f(\xi) \neq 0$ なる仮定の下では, 条件 (C1) は $[\mathbb{Q}(\lambda^{-1}(P)) : \mathbb{Q}(P)] = 3$ と同値になる. なお, E は $3n$ を割らないような素点においては good reduction をもつことを注意しておく.

[命題 1.1 の証明] ([H1], [H2] による.) ξ を条件 (C0)–(C2) をみたす有理整数とし, P を $x^{-1}(\{\xi\})$ 内の点とする. $K = \mathbb{Q}(P) = \mathbb{Q}(\sqrt{f(\xi)})$, $K' = \mathbb{Q}(\lambda^{-1}(P))$ と置くと, 仮定 (C0), (C1) により $[K : \mathbb{Q}] = 2$, $[K' : K] = 3$ である. $f(\xi)$ は 3 次式 $F_\xi(z)$ の判別式であるから, K' は $F_\xi(z)$ の $\mathbb{Q}$ 上の分解体であり, 従って $K'/\mathbb{Q}$ は 6 次の dihedral な拡大になる. さて, K'/K が不分岐であることを示そう. K'' を K' の 3 次の部分体とする. もし K の素イデアル — その下にある素数を p とする — が K' において分岐したとすると, p は K'' において完全分岐しなければならない. 従って, 適当な $\alpha \in \mathbb{Z}$ に対して $F_\xi(z)$ は

$$F_\xi(z) \equiv (z - \alpha)^3 \pmod{p}$$

と p を法として分解されなければならない. この両辺を比べることにより, $p | (\xi, n)$ または $3 | \xi$ が成り立つことがわかるが, これは仮定 (C2) に反する. $\square$

注意 3.1 本田氏の元々の結果 [H1, Proposition 10] は命題 1.1 だけではなくその逆に当たる “2 次体 K の類数が 3 の倍数ならば, K は適当な n と条件 (C0)–(C2) をみたす $\xi \in \mathbb{Z}$ によって $\mathbb{Q}(\sqrt{f(\xi)})$ と表せる” ことも示している ($f(x)$ ならびに 3 条件は n に依ることに注意).

4 定理 1.2 の証明 (その 1)

本節では定理 1.2, (i) の証明を与える. 楕円曲線の同種写像を考え, そこから生じる体の拡大に注目するという点は命題 1.1 の証明と同様である.

前と同様に, $\overline{E}/k$ を Weierstrass 方程式 $v^2 = 4nu^3 + 1$ により与えられる楕円曲線とし, $\lambda : \overline{E} \rightarrow E$ を

$$x = \frac{1 + nu^3}{u^2}, \quad y = \frac{2 - nu^3}{u^3} v$$

により与えられる k 上の同種写像とする. このとき, $\deg \lambda = 3$ ならびに $\text{Ker } \lambda \subseteq \overline{E}(k)$ が成り立ち, 2.2 節の議論が適用できる.

$$\Lambda_\xi(u) = nu^3 - \xi u^2 + 1$$

となることも 3 節と同様である. 補題 2.1 により, x -座標が ξ であるような $P \in x^{-1}(\mathbb{P}^1(k)) - E[2](k)$ に対し, 条件 (C1)* は $[k(\lambda^{-1}(P)) : k(P)] = 3$ と同値である. いま,

$$U = nu, \quad V = \frac{n(v+1)}{2}$$

と置くと, $\overline{E}/k$ の別な Weierstrass 方程式

$$(*) \quad V^2 - nV = U^3$$

(この方程式の判別式は $-27n^4$) が得られ, この座標に関して

$$\text{Ker } \lambda = \{(U, V) = (0, 0), (0, n)\} \cup \{O\}$$

となる.

さて, $(x, y) = (\xi, \eta)$ で与えられるような $x^{-1}(\Xi^*)$ 内の点 P を固定し,

$$K = k(P) = k(\eta), \quad K' = k(\lambda^{-1}(P)), \quad G = \text{Gal}(K'/K)$$

と置く. このとき $[K : k] \leq 2$ であって, 仮定 (C2)* より $P \notin E[2](k)$ となるから, $[K' : K] = 3$. また, 任意の $Q \in \lambda^{-1}(P)$ に対し, $K' = K(Q)$ であって,

$$Q^\sigma - Q \in \text{Ker } \lambda \quad \text{for all } \sigma \in G.$$

定理 1.2, (i) は次の命題から直ちに従う:

命題 4.1 記号や仮定は上の通りとするととき, 拡大 K'/K は全ての有限素点で不分岐.

以下しばらく, 次のような記号を用いる:

$\mathfrak{P}$ K の素イデアル.

$\mathfrak{P}'$ K' における $\mathfrak{P}$ の素因子 (のひとつ).

κ' $\mathfrak{P}'$ の剰余体.

$D \subseteq G$ $\mathfrak{P}'/\mathfrak{P}$ の分解群.

$I \subseteq D$ $\mathfrak{P}'/\mathfrak{P}$ の惰性群.

命題 4.1 の証明の第 1 段として, $\overline{E}$ の modulo $\mathfrak{P}'$ での reduction を考える. すなわち,

$$\overline{E}(K') \longrightarrow (\overline{E} \bmod \mathfrak{P}')(\kappa'), \quad Q \longmapsto Q \bmod \mathfrak{P}'$$

を Weierstrass 方程式 (*) に関する modulo $\mathfrak{P}'$ での reduction とし, $\overline{E}(K')$ の 2 つの部分集合

$$\overline{E}_0(K'; \mathfrak{P}') = \{Q \in \overline{E}(K') ; Q \bmod \mathfrak{P}' \in (\overline{E} \bmod \mathfrak{P}')_{\text{ns}}(\kappa')\},$$

$$\overline{E}_1(K'; \mathfrak{P}') = \{Q \in \overline{E}(K') ; Q \bmod \mathfrak{P}' = O \bmod \mathfrak{P}'\}$$

を考える. 方程式 (*) は minimal とは限らないから, 上の 2 つの部分集合は $\overline{E}, K'$ や $\mathfrak{P}'$ から一意的に定まっているわけではない. しかしながら, $\overline{E}_0(K'; \mathfrak{P}')$ が $\overline{E}(K')$ の部分群になることや, 写像 $\overline{E}_0(K'; \mathfrak{P}') \rightarrow (\overline{E} \bmod \mathfrak{P}')_{\text{ns}}(\kappa')$ が準同型でその核が $\overline{E}_1(K'; \mathfrak{P}')$ になることは容易に確かめられる. $\overline{E}_0(K'; \mathfrak{P}')$ や $\overline{E}_1(K'; \mathfrak{P}')$ は $\overline{E}(K')$ の中で U -座標の $\mathfrak{P}'$ -進付値による次のような特徴づけをもつ:

補題 4.2 上の記号の下で,

$$\overline{E}_0(K'; \mathfrak{P}') = \begin{cases} \{(U, V) = (\zeta, \omega) ; \text{ord}_{\mathfrak{P}'}(\zeta^3 + n^2) \leq 0\} \cup \{O\} & \text{if } \mathfrak{P}' | 3n \\ \overline{E}(K') & \text{otherwise} \end{cases}$$

ならびに

$$\overline{E}_1(K'; \mathfrak{P}') = \{(U, V) = (\zeta, \omega) ; \text{ord}_{\mathfrak{P}'}(\zeta) < 0\} \cup \{O\}$$

が成り立つ.

[証明] 後者の等式は明らか. 前者を示す.

$\mathfrak{P}' \nmid 3n$ の場合には, 楕円曲線 $\overline{E}$ は $\mathfrak{P}'$ で good reduction をもち, $\overline{E}_0(K'; \mathfrak{P}') = \overline{E}(K')$ が成り立つ.

以下, $\mathfrak{P}' | 3n$ とする. このとき, $(U, V) = (\zeta, \omega)$ で与えられるような $Q \in \overline{E}(K') - \{O\}$ に対し, 条件 $Q \notin \overline{E}_0(K'; \mathfrak{P}')$ は

$$\text{ord}_{\mathfrak{P}'}(\zeta) \geq 0, \quad \text{ord}_{\mathfrak{P}'}(3\zeta^2) > 0, \quad \text{ord}_{\mathfrak{P}'}(2\omega - n) > 0$$

と同値である. ここで,

$$(2\omega - n)^2 = 4\zeta^3 + n^2 = 3\zeta^3 + (\zeta^3 + n^2)$$

が成り立つことより, 条件 $\text{ord}_{\mathfrak{P}'}(2\omega - n) > 0$ は $\text{ord}_{\mathfrak{P}'}(\zeta^3 + n^2) > 0$ で置き換えてよい. さらに, 条件 $\text{ord}_{\mathfrak{P}'}(\zeta^3 + n^2) > 0$ より $\text{ord}_{\mathfrak{P}'}(\zeta) \geq 0$ ならびに $\text{ord}_{\mathfrak{P}'}(3\zeta^2) > 0$ が従うから, $Q \notin \overline{E}_0(K'; \mathfrak{P}')$ と $\text{ord}_{\mathfrak{P}'}(\zeta^3 + n^2) > 0$ は同値になり, 求める等式を得る. $\square$

第 2 段として, $\lambda^{-1}(P) \cap \overline{E}_0(K'; \mathfrak{P}') \neq \emptyset$ であることを示す.

補題 4.3 記号や仮定は上の通りとすると, $\lambda^{-1}(P)$ 内の少なくともひとつの点は $\overline{E}_0(K'; \mathfrak{P}')$ に含まれる.

[証明] $\mathfrak{P} \nmid 3n$ の場合には明らか.

以下, $\mathfrak{P} \mid 3n$ とする. $\lambda^{-1}(P) = \{Q_1, Q_2, Q_3\}$ とし, Q_i の U -座標を ζ_i とする. このとき, 3 次式

$$n^2 \Lambda_\xi \left(\frac{U}{n} \right) = U^3 - \xi U^2 + n^2 \in k[U]$$

は

$$U^3 - \xi U^2 + n^2 = (U - \zeta_1)(U - \zeta_2)(U - \zeta_3)$$

と分解される. この両辺を比べることにより,

$$\zeta_1 + \zeta_2 + \zeta_3 = \xi$$

となることがわかる. よって, 仮定 (C2)* により $\text{ord}_{\mathfrak{P}'}(\zeta_{i_0}) \leq 0$ となるような $i_0 \in \{1, 2, 3\}$ が存在し, このとき

$$\text{ord}_{\mathfrak{P}'}(\zeta_{i_0}^3 + n^2) = \text{ord}_{\mathfrak{P}'}(\xi \zeta_{i_0}^2) = \text{ord}_{\mathfrak{P}'}(\xi) + 2 \text{ord}_{\mathfrak{P}'}(\zeta_{i_0}) \leq 0.$$

すなわち, $Q_{i_0} \in \overline{E}_0(K'; \mathfrak{P}')$. □

注意 4.4 実際には, $\mathfrak{P} \nmid n$ ならば $\lambda^{-1}(P) \subseteq \overline{E}_0(K'; \mathfrak{P}')$ となることが示せる.

第 3 段として, $\mathfrak{P}$ が K' において不分解 (i.e., $D = G$) という仮定の下で, $\mathfrak{P}$ が K' において不分岐 (i.e., $I = \{1\}$) であることを示す.

補題 4.5 上の記号と仮定の下で, さらに $\mathfrak{P}$ が K' において不分解であるとする. このとき, $\mathfrak{P}$ は K' において不分岐.

[証明] $D = G$ なる仮定の下では, 素イデアル $\mathfrak{P}'$ は K' におけるただひとつの $\mathfrak{P}$ の素因子であるから, $\overline{E}_0(K'; \mathfrak{P}')$ や $\overline{E}_1(K'; \mathfrak{P}')$ of $\overline{E}(K')$ は G -不変である. よって, 任意の $Q \in \overline{E}_0(K'; \mathfrak{P}')$ に対し,

$$Q^\sigma - Q \in \overline{E}_1(K'; \mathfrak{P}') \quad \text{for all } \sigma \in I$$

が成り立つ.

Q を $\lambda^{-1}(P) \cap \overline{E}_0(K'; \mathfrak{P}')$ — 補題 4.3 により, この集合は空ではない — 内の点とする. このとき $\text{Ker } \lambda \cap \overline{E}_1(K'; \mathfrak{P}') = \{O\}$ より,

$$Q^\sigma = Q \quad \text{for all } \sigma \in I.$$

他方, $K' = K(Q)$ であるから, $I = \{1\}$ でなければならない. □

$D \neq G$ ならば $D = \{1\}$ 従って $I = \{1\}$ となるから, これで命題 4.1 が示せたことになる.

注意 4.6 $\mathfrak{P}|n$ の場合には, reduction を使わなくても $D = \{1\}$ となることが示せる.

最後に, 条件 (C2)* の幾何学的な意味について触れておく. いま,

$$X = x, \quad Y = \frac{y+n}{2}$$

と置くと, E/k の Weierstrass 方程式

$$Y^2 - nY = X^3 - 7n^2$$

が得られる. K を k の有限次拡大とする. K の素イデアル $\mathfrak{P}$ に対し,

$$E(K) \longrightarrow (E \bmod \mathfrak{P})(\kappa), \quad P \longmapsto P \bmod \mathfrak{P}$$

を上の方方程式に関する modulo $\mathfrak{P}$ での reduction とする (κ は $\mathfrak{P}$ の剰余体). 先と同様に $E(K)$ の部分集合 $E_0(K; \mathfrak{P})$ を定める:

$$E_0(K; \mathfrak{P}) = \{P \in E(K) ; P \bmod \mathfrak{P} \in (E \bmod \mathfrak{P})_{\text{ns}}(\kappa)\}.$$

このとき, 容易にわかるように

$$E_0(K; \mathfrak{P}) = \begin{cases} \{(X, Y) = (\xi, \eta) ; \text{ord}_{\mathfrak{P}}(\xi) \leq 0\} \cup \{O\} & \text{if } \mathfrak{P}|3n \\ E(K) & \text{otherwise} \end{cases}$$

が成り立つ. つまり, $E(K) \cap x^{-1}(k)$ の点 P が $\bigcap_{\mathfrak{P}} E_0(K; \mathfrak{P})$ に含まれるためにはその X -座標 (= x -座標) ξ が条件 (C2)* をみたすことが必要かつ十分である.

5 定理 1.2 の証明 (その 2)

本節では, 定理 1.2, (ii) の証明を与える.

まず, Euler の函数に似た, ある種の数論的函数の部分和に関する漸近公式を示す. この公式は新潟大の秋山茂樹氏に教えて頂いた [A].

命題 5.1 N を正の有理整数とし, 数論的関数 φ_N と ψ_N を

$$\begin{aligned}\varphi_N(m) &= \#\{i \in \mathbb{Z} ; 0 < i \leq m, (Ni, m) = 1\}, \\ \psi_N(m) &= \#\{i \in \mathbb{Z} ; 0 < i \leq m, (i, Nm) = 1\}\end{aligned}$$

により定義する. このとき,

$$\sum_{m \leq T} \varphi_N(m) = c_N T^2 + O(T \log T), \quad \sum_{m \leq T} \psi_N(m) = c_N T^2 + O(T \log T) \quad \text{as } T \rightarrow \infty.$$

ここで,

$$c_N = \frac{3}{\pi^2} \prod_{\substack{p \text{ prime} \\ p|N}} \frac{p}{p+1}.$$

注意 5.2 (i) $N = 1$ の場合には, φ_1 と ψ_1 は共に Euler の関数 に一致する. このときには, 上の漸近公式はよく知られているものになる ($c_1 = 3/\pi^2$ とみなす).

(ii) 関数 φ_N, ψ_N ならびに定数 c_N は N の素因子のみによって定まる.

(iii) 容易にわかるように,

$$\begin{aligned}\varphi_N(m) &= \#\{\xi \in \mathbb{Q} ; \xi \geq 1, \text{ord}_p(\xi) \leq 0 \text{ for all } p \in S, H_{\mathbb{P}^1}(\xi) = m\}, \\ \psi_N(m) &= \#\{\xi \in \mathbb{Q} ; 0 < \xi \leq 1, \text{ord}_p(\xi) \leq 0 \text{ for all } p \in S, H_{\mathbb{P}^1}(\xi) = m\}.\end{aligned}$$

ここで, S は N の素因子の集合を表す.

系 5.3 素数の有限集合 S に対し,

$$\#\{\xi \in \mathbb{Q} ; \text{ord}_p(\xi) \leq 0 \text{ for all } p \in S, H_{\mathbb{P}^1}(\xi) \leq T\} = c_S T^2 + O(T \log T) \quad \text{as } T \rightarrow \infty.$$

ただし,

$$c_S = \frac{12}{\pi^2} \prod_{p \in S} \frac{p}{p+1}.$$

命題 5.1 を証明する前に, いくつかの補題を示しておく. 以下, 正の有理整数 j に対し, 整数 $j/(j, N)$ を j^* で表すことにする. この記号の下で, φ_N や ψ_N は Möbius の関数を使って次のように表すことができる:

補題 5.4

$$\varphi_N(m) = \sum_{j|m} \mu(j) \frac{m}{j^*}, \quad \psi_N(m) = \sum_{j|Nm} \mu(j) \left\lfloor \frac{m}{j} \right\rfloor.$$

ここで, μ は Möbius の関数.

[証明]

$$\varphi_N(m) = \sum_{i=1}^m \sum_{j|(Ni, m)} \mu(j), \quad \psi_N(m) = \sum_{i=1}^m \sum_{j|(i, Nm)} \mu(j)$$

より,

$$\varphi_N(m) = \sum_{j|m} \mu(j) \sum_{\substack{i \leq m \\ j^* | i}} 1 = \sum_{j|m} \mu(j) \frac{m}{j^*}, \quad \psi_N(m) = \sum_{j|Nm} \mu(j) \sum_{\substack{i \leq m \\ j | i}} 1 = \sum_{j|Nm} \mu(j) \left\lfloor \frac{m}{j} \right\rfloor.$$

□

命題 5.1 の定数 c_N は Möbius の函数と次のように関係している:

補題 5.5

$$\sum_{j=1}^{\infty} \frac{\mu(j)}{jj^*} = c_N.$$

[証明] 容易にわかるように, 函数 $\mu(\cdot)(\cdot, N)$ は乗法的である:

$$\mu(jj')(jj', N) = \mu(j)(j, N) \cdot \mu(j')(j', N) \quad \text{whenever } (j, j') = 1.$$

よって級数

$$\sum_{j=1}^{\infty} \frac{\mu(j)}{jj^*} = \sum_{j=1}^{\infty} \frac{\mu(j)(j, N)}{j^2}$$

(この級数は絶対収束する) は Euler 積に分解され,

$$\prod_p \left(\sum_{e=0}^{\infty} \frac{\mu(p^e)(p^e, N)}{p^{2e}} \right) = \prod_p \left(1 - \frac{(p, N)}{p^2} \right) = \prod_{p|N} \left(1 - \frac{1}{p} \right) \cdot \prod_{p \nmid N} \left(1 - \frac{1}{p^2} \right) = c_N$$

に一致する.

□

[命題 5.1 の証明] 補題 5.4 より,

$$\sum_{m \leq T} \varphi_N(m) = \sum_{m \leq T} m \sum_{j|m} \frac{\mu(j)}{j^*} = \sum_{j \leq T} \frac{\mu(j)}{j^*} \sum_{\substack{m \leq T \\ j|m}} m$$

ならびに

$$\sum_{m \leq T} \psi_N(m) = \sum_{m \leq T} m \sum_{j|Nm} \frac{\mu(j)}{j} + O \left(\sum_{m \leq T} \sigma_0(m) \right) = \sum_{j \leq NT} \frac{\mu(j)}{j} \sum_{\substack{m \leq T \\ j^* | m}} m + O(T \log T)$$

となることがわかる. ここで, $\sigma_0(m)$ は m の約数の個数を表し, 後者の等式を導く際には

$$\left| \sum_{j|Nm} \mu(j) \right| \leq \sigma_0(Nm) \leq \sigma_0(N)\sigma_0(m)$$

を用いた. 故に

$$\begin{aligned} \sum_{\substack{m \leq T \\ j|m}} m &= \sum_{m \leq T/j} jm = \frac{j}{2} \left[\frac{T}{j} \right] \left(\left[\frac{T}{j} \right] + 1 \right) = \frac{T^2}{2j} + O(T), \\ \sum_{\substack{m \leq T \\ j^*|m}} m &= \sum_{m \leq T/j^*} j^*m = \frac{j^*}{2} \left[\frac{T}{j^*} \right] \left(\left[\frac{T}{j^*} \right] + 1 \right) = \frac{T^2}{2j^*} + O(T) \end{aligned}$$

ならびに

$$\left| \sum_{j \leq T} \frac{\mu(j)}{j^*} \right| \leq N \sum_{j \leq T} \frac{1}{j} \sim N \log T, \quad \left| \sum_{j \leq NT} \frac{\mu(j)}{j} \right| \leq \sum_{j \leq NT} \frac{1}{j} \sim \log T$$

より,

$$\sum_{m \leq T} \varphi_N(m) = \frac{1}{2} \sum_{j \leq T} \frac{\mu(j)}{jj^*} T^2 + O(T \log T), \quad \sum_{m \leq T} \psi_N(m) = \frac{1}{2} \sum_{j \leq NT} \frac{\mu(j)}{jj^*} T^2 + O(T \log T).$$

他方, 容易にわかるように,

$$\sum_{j \leq T} \frac{\mu(j)}{jj^*} = \sum_{j=1}^{\infty} \frac{\mu(j)}{jj^*} + O\left(\frac{1}{T}\right), \quad \sum_{j \leq NT} \frac{\mu(j)}{jj^*} = \sum_{j=1}^{\infty} \frac{\mu(j)}{jj^*} + O\left(\frac{1}{T}\right).$$

よって補題 5.5 より求める漸近公式を得る. □

次に, 条件 (C1)* をみたさない $\xi \in k$ の個数を評価する.

命題 5.6 記号や仮定は 2.2 節の通りとすると,

$$\#\{\xi \in k ; \Lambda_{\xi}(u) \text{ is reducible over } k, H_{\mathbb{P}^1}(\xi) \leq T\} \asymp T^{2[k:\mathbb{Q}]/l} \quad \text{as } T \rightarrow \infty.$$

系 5.7 定理 1.2 と同じ記号と仮定の下で,

$$\#\{\xi \in k ; F_{\xi}(z) \text{ is reducible over } k, H_{\mathbb{P}^1}(\xi) \leq T\} \asymp T^{2[k:\mathbb{Q}]/3} \quad \text{as } T \rightarrow \infty.$$

定理 1.2, (ii) は系 5.3 と系 5.7 から直ちに従う.

[命題 5.6 の証明] 補題 2.1 より,

$$\#\{\xi \in k ; \Lambda_\xi(u) \text{ is reducible over } k, H_{\mathbb{P}^1}(\xi) \leq T\} \asymp \#\{\zeta \in k ; (H_{\mathbb{P}^1} \circ \lambda_x)(\zeta) \leq T\}.$$

他方, $\lambda_x(u)$ は次数 l の有理関数であるから,

$$H_{\mathbb{P}^1} \circ \lambda_x \asymp H_{\mathbb{P}^1}^l \quad \text{on } \mathbb{P}^1(\bar{k}).$$

よって 1 節の漸近公式 (‡) より主張を得る. □

注意 5.8 もし代数体 k の素イデアルの有限集合 S に対して

$$\#\{\xi \in k ; \text{ord}_{\mathfrak{p}}(\xi) \leq 0 \text{ for all } \mathfrak{p} \in S, H_{\mathbb{P}^1}(\xi) \leq T\} \asymp T^{2[k:\mathbb{Q}]} \quad \text{as } T \rightarrow \infty$$

となることが示せたならば,

$$\#\{P \in x^{-1}(\Xi^*) ; H_x(P) \leq T\} \asymp T^{2[k:\mathbb{Q}]} \quad \text{as } T \rightarrow \infty$$

ならびに

$$\liminf_{T \rightarrow \infty} \frac{\#\{P \in x^{-1}(\mathbb{P}^1(k)) ; 3|h_{k(P)}, H_x(P) \leq T\}}{\#\{P \in x^{-1}(\mathbb{P}^1(k)) ; H_x(P) \leq T\}} > 0$$

を得ることができる.

参考文献

- [A] S. Akiyama, private communication.
- [H1] T. Honda, Isogenies, rational points and section points of group varieties, Japan J. Math. **30** (1960), 84–101.
- [H2] ———, On real quadratic fields whose class numbers are multiples of 3, J. Reine Angew. Math. **233** (1968), 101–102.
- [L] S. Lang, *Fundamentals of Diophantine Geometry*, Springer, New York, 1983.
- [S] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Math. **106**, Springer, New York, 1985.

- [ST] C. L. Stewart and J. Top, On ranks of twists of elliptic curves and power-free values of binary forms, J. Amer. Math. Soc. **8** (1995), 943–973.

980-8578 仙台市青葉区荒巻字青葉
東北大学大学院理学研究科数学専攻
e-mail: atsushi@math.tohoku.ac.jp