円分 $\mathbb{Z}_2$ 拡大の中間体で rank の増える楕円曲線の構成について

松野 一夫* (津田塾大学)

各素数 p に対し, 円分 $\mathbb{Z}_p$ 拡大と呼ばれる有理数体 $\mathbb{Q}$ の無限次拡大 $\mathbb{Q}_\infty^{\mathrm{cyc}}$ が存在する. この拡大は各 $n \geq 0$ に対し p^n 次の中間体 $\mathbb{Q}_n^{\mathrm{cyc}}$ をただ 1 つ持つが (n-th layer と呼ばれる), $\mathbb{Q}$ 上に定義された任意の楕円曲線 E の $\mathbb{Q}_n^{\mathrm{cyc}}$ 上の Mordell-Weil 群の rank は n を動かすとき有界であることが知られている. つまり, ある (E と p に依存する) 整数 $n_0 \geq 0$ が存在し, n_0 番目の中間体 $\mathbb{Q}_{n_0}^{\mathrm{cyc}}$ から先では E の Mordell-Weil rank は増えなくなる (系 1.6 参照). 実際には, 最初から ($\mathbb{Q}_0^{\mathrm{cyc}} = \mathbb{Q}$ から) 全く増えないことも多く, 一般には $\mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}_n^{\mathrm{cyc}}) > \mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}_{n-1}^{\mathrm{cyc}})$ となる例を見つけることすら容易ではない. そのような具体例として, 次の結果を得た.

定理. $p = 2$ とし, $\mathbb{Q}_n^{\mathrm{cyc}}$ を $\mathbb{Q}$ の円分 $\mathbb{Z}_2$ 拡大の n-th layer とする. そのとき, $\mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}_4^{\mathrm{cyc}}) > \mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}_3^{\mathrm{cyc}})$ を満たす $\mathbb{Q}$ 上の楕円曲線 E が無限個存在する.

本稿では, 上で述べた問題の設定や知られている結果などをもう少し詳しく解説 (1 節) した後, 定理の証明の概略を述べる (2 節). 最後の節 (3 節) では, 定理の具体例やその他の p, n に対する計算結果などを紹介する.

1 問題設定

1.1 円分 $\mathbb{Z}_p$ 拡大

K を (有限次) 代数体とする. 素数 p に対し, $\mathrm{Gal}(K_n/K) \cong \mathbb{Z}/p^n\mathbb{Z}$ なる中間体の列

$$K = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_n \subset \cdots \subset K_\infty$$

が存在し, $K_\infty = \bigcup_n K_n$ となる拡大 K_∞/K を K の $\mathbb{Z}_p$ 拡大と呼ぶ. K_∞/K は Galois 拡大であり, その Galois 群は

$$\mathrm{Gal}(K_\infty/K) = \varprojlim_n \mathrm{Gal}(K_n/K) \cong \varprojlim_n \mathbb{Z}/p^n\mathbb{Z} = \mathbb{Z}_p$$

となる. 特に K_∞ は K の無限次アーベル拡大である.

1 の原始 p^n 乗根の 1 つを ζ_{p^n} とするとき, K に ζ_{p^n} を全て添加して得られる拡大 $\bigcup_n K(\zeta_{p^n})/K$ の Galois 群は $\mathbb{Z}_p$ の乗法群 $\mathbb{Z}_p^\times$ の指数有限部分群であり, 商が $\mathbb{Z}_p$ と同型になる部分群をただ 1 つ持つ. つまり, $\bigcup_n K(\zeta_{p^n})$ は (その部分群の固定体として) K の $\mathbb{Z}_p$ 拡大をただ 1 つ含む. この $\mathbb{Z}_p$ 拡大を K の円分 $\mathbb{Z}_p$ 拡大と呼び, (本稿では) K_∞^{cyc} で表す[1]. また, K 上 p^n 次の中間体を K_n^{cyc} で表し, K の円分 $\mathbb{Z}_p$ 拡大の n-th layer と呼ぶ.

*講演および本原稿作成の機会を与えてくださった世話人の皆様に感謝いたします.

[1] p に依存していることが表現できていませんが, 文脈で区別可能かと思います.

Kronecker-Weber の定理により, 有理数体 $\mathbb{Q}$ の $\mathbb{Z}_p$ 拡大は $\bigcup_n \mathbb{Q}(\zeta_{p^n})$ に含まれることがわかる. つまり, $\mathbb{Q}$ の $\mathbb{Z}_p$ 拡大は円分 $\mathbb{Z}_p$ 拡大 $\mathbb{Q}_\infty^{\mathrm{cyc}}$ のみである. より一般に, K が総実ならば円分 $\mathbb{Z}_p$ 拡大が唯一の $\mathbb{Z}_p$ 拡大であると予想されているが (Leopoldt 予想, [11, 予想 2.7] 参照), 総実でない体は各 p に対し無限個の $\mathbb{Z}_p$ 拡大を持つことがわかる ([11, 定理 2.6]).

本稿では主に $\mathbb{Q}$ の円分 $\mathbb{Z}_2$ 拡大を扱うが, その n-th layer は次のような原始元を持つ.

補題 1.1. 各 $n \geq 0$ に対し, 1 の原始 2^{n+2} 乗根 $\zeta_{2^{n+2}}$ を $\zeta_{2^{n+2}}^2 = \zeta_{2^{n+1}}$ が成り立つように取り, $\alpha_n = \zeta_{2^{n+2}} + \zeta_{2^{n+2}}^{-1}$ と置く. このとき, $\mathbb{Q}_n^{\mathrm{cyc}} = \mathbb{Q}(\alpha_n)$ であり,

$$\alpha_n^2 = \alpha_{n-1} + 2 \tag{1}$$

が全ての $n \geq 1$ で成り立つ.

注意. $\zeta_{2^{n+2}} = e^{\pi i/2^{n+1}}$ とすると, $\alpha_n = 2\cos\frac{\pi}{2^{n+1}}$ となる. 特に, $\alpha_1 = \sqrt{2}$, $\alpha_2 = \sqrt{2+\sqrt{2}}$ などとなる.

1.2 円分 $\mathbb{Z}_p$ 拡大と Mordell-Weil 群

E を有限次代数体 K 上に定義された楕円曲線とする. E の K-有理点 (座標が K の元であるような E 上の点) 全体のなす集合を $E(K)$ と書くとき, 次の事実はよく知られている.

定理 1.2 (Mordell-Weil)**.** $E(K)$ は有限生成アーベル群である. 即ち, ある整数 $r \geq 0$ と有限アーベル群 T が存在し, $E(K) \cong \mathbb{Z}^{\oplus r} \oplus T$ となる.

注意. これより, $E(K)$ のことを (E の K 上の) Mordell-Weil 群と呼び, アーベル群としての rank r を Mordell-Weil rank (あるいは単に rank) と呼ぶ.

この定理の主張 (のうち有限生成であること) は, 一般の体上の楕円曲線に対しては成り立たない. 例えば E が $\mathbb{C}$ 上の楕円曲線ならば, ある格子 $L \subset \mathbb{C}$ が存在して $E(\mathbb{C}) \cong \mathbb{C}/L$ となるので, $E(\mathbb{C})$ はアーベル群として有限生成にならない. $\mathbb{Q}$ の代数拡大に限っても, 無限次の拡大体上では一般には成り立たないが, Mazur は次を予想した.

予想 1.3 (Mazur [9])**.** p を素数とし, K_∞^{cyc} を有限次代数体 K の円分 $\mathbb{Z}_p$ 拡大とする. そのとき, K_∞^{cyc} 上の任意の楕円曲線 E に対し, $E(K_\infty^{\mathrm{cyc}})$ は有限生成アーベル群となる.

K_∞^{cyc} 上の楕円曲線 E は (定義方程式の係数が有限次代数体の元となるので) ある中間体 K_m^{cyc} 上定義されていると考えることができ, 予想の主張は $E(K_{m'}^{\mathrm{cyc}}) = E(K_\infty^{\mathrm{cyc}})$ なる $m' \geq m$ が存在することと同値である. 更に, 既に知られているねじれ部分群の有限性 ([9, Proposition 6.2]) を考慮すると, ある $K_{m''}^{\mathrm{cyc}}$ ($m'' \geq m$) から先で E の rank が増えなくなることとも同値となる ([4, Theorem 1.3] 参照). この予想 1.3 は一般にはまだ未解決であるが, $K = \mathbb{Q}$ であり, E も $\mathbb{Q}$ 上に定義されている場合には, 次の結果が知られている.

定理 1.4 (Rohrlich [12])**.** p を素数とし, E を $\mathbb{Q}$ 上の楕円曲線とするとき, $L(E,\chi,1) = 0$ となる導手が p べきの Dirichlet 指標 χ は高々有限個しかない. ただし, $L(E,\chi,s)$ は χ でひねった E の Hasse-Weil L 関数とする.

定理 1.5 (加藤 [5])**.** E を $\mathbb{Q}$ 上の楕円曲線, L をアーベル体とする. χ を $\mathrm{Gal}(L/\mathbb{Q})$ の指標とするとき, $L(E,\chi,1) \neq 0$ であるならば $E(L)$ の χ 部分は有限である.

系 1.6. E が $\mathbb{Q}$ 上の楕円曲線ならば, ある非負整数 n_0 が存在し, 任意の $n \geq n_0$ に対し $\mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}_n^{\mathrm{cyc}}) = \mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}_{n_0}^{\mathrm{cyc}})$ が成り立つ. 特に, $E(\mathbb{Q}_\infty^{\mathrm{cyc}})$ は有限生成である.

なお, 一般の $\mathbb{Z}_p$ 拡大では予想 1.3 の主張は必ずしも成り立たない.

例. $K = \mathbb{Q}(\sqrt{-2})$ とすると, K は虚 2 次体なので任意の p に対し, $\mathbb{Z}_p$ 拡大が無限個存在する.
(1) $p = 3$ は K で $3 = (1+\sqrt{-2})(1-\sqrt{-2})$ と分解するが, $\pi = 1+\sqrt{-2}$ のみが分岐するような $\mathbb{Z}_3$ 拡大がただ 1 つ存在する. それを $K_\infty^{(\pi)}$ で表す. A を方程式 $y^2 = x^3 + x^2 - 3x + 1$ で定義される楕円曲線とし[2], $L = \mathbb{Q}(\sqrt{2-\sqrt{-2}})$ とすると, $A(LK_\infty^{(\pi)})_{\mathrm{tors}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Q}_3/\mathbb{Z}_3$ となる. 特に L の $\mathbb{Z}_3$ 拡大 $LK_\infty^{(\pi)}$ 上では A のねじれ部分群は有限でない. (A は K の整数環に CM を持つ楕円曲線であり, $LK_\infty^{(\pi)}$ は K に A の π 冪等分点を全て添加して得られる体である.)
(2) K の anticyclotomic $\mathbb{Z}_3$ 拡大 ([11, 注意 3.18] 参照) を K_∞^{ac} とし, E を $y^2 + y = x^3 - x^2$ で定義される楕円曲線とすると, $\mathrm{rank}_{\mathbb{Z}} E(K_\infty^{\mathrm{ac}}) = \infty$ である.

1.3 問題と既知の結果

系 1.6 により, 任意の素数 p と任意の $\mathbb{Q}$ 上の楕円曲線 E に対し, $\mathbb{Q}$ の円分 $\mathbb{Z}_p$ 拡大の n-th layer $\mathbb{Q}_n^{\mathrm{cyc}}$ における E の rank が $n \geq n_0$ ならば一定の値となるような $n_0 \geq 0$ が必ず存在する. この n_0 について, Greenberg は次の素朴な問題を提示した ([4, p. 417]).

問題 1.7 (Greenberg)**.** n_0 は E や p と独立に取ることができるか?

ここで $n_0(E,p)$ を $\mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}_\infty^{\mathrm{cyc}}) = \mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}_n^{\mathrm{cyc}})$ となる n の最小値として定義すれば, 上の問題は, E や p を動かすとき $n_0(E,p)$ が取る値は有界か否かを尋ねる問題となる. E を固定して p だけ動かす場合には, Rohrlich の結果 (定理 1.4) を精密化した Chinta の結果 [1] と加藤の結果 (定理 1.5) により, 次の有界性が示される.

定理 1.8 (Chinta)**.** E を固定し p を動かすとき, $\sup_p n_0(E,p) < \infty$ となる.

そこで今度は p を固定し E を動かすとき, $n_0(E,p)$ がどのような値を取り得るか考察したい. まず, $n_0(E,p) = 0$ となる E の存在については, Mazur の control 定理 ([9], [3, Theorem 1.2]) や栗原の結果 ([6]) を用いて容易に具体例を与えることが出来る. 実際, E を $y^2 + y = x^3 - x^2 - 10x - 20$ が定める曲線 (modular 曲線 $X_0(11)$) とすると, 任意の $p \geq 3$ に対し $E(\mathbb{Q}_\infty^{\mathrm{cyc}})$ は有限であり, 特に $n_0(E,p) = 0$ となることがわかる ([3, p. 106], [6, Remark 0.2] 参照). また, $p = 2$ に対しても $E' : y^2 + xy + y = x^3 + x^2 - 10x - 10$ ($X_0(15)$) は $n_0(E',2) = 0$ を満たす ([3, p. 136]).

しかし, $n_0(E,p) > 0$ となる E を見つけるのは一般には容易ではない. なぜなら, もし $n = n_0(E,p) \geq 1$ ならば定義より $\mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}_n^{\mathrm{cyc}}) > \mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}_{n-1}^{\mathrm{cyc}})$ となるが, $E(\mathbb{Q}_n^{\mathrm{cyc}})$ への $\mathrm{Gal}(\mathbb{Q}_n^{\mathrm{cyc}}/\mathbb{Q})$ の作用を考慮すると

$$\mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}_n^{\mathrm{cyc}}) \equiv \mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}_{n-1}^{\mathrm{cyc}}) \pmod{\varphi(p^n)} \tag{2}$$

という合同式が得られるため, $\mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}_n^{\mathrm{cyc}}) \geq p^{n-1}(p-1)$ でなくてはならない. つまり, $n_0(E,p) > 0$ となる E を探すことは, (特定の代数体上で) rank の大きな楕円曲線を探す問題となり, 以下の例のように p と n が極めて小さい場合を除いては, 具体例を与えるのも難しい.

[2] この A は次節でも登場します.

例. (1) E を上の $y^2+y=x^3-x^2-10x-20$ とする. $p=2$ のとき $\mathbb{Q}_1^{\mathrm{cyc}}=\mathbb{Q}(\sqrt{2})$ であるが, E は $\mathbb{Q}(\sqrt{2})$ 上に $(137+77\sqrt{2}, 1996+1309\sqrt{2})$ という位数無限の点を持ち, $\mathrm{rank}_{\mathbb{Z}}E(\mathbb{Q}_1^{\mathrm{cyc}})>0$ であることがわかる. $\mathrm{rank}_{\mathbb{Z}}E(\mathbb{Q})=0$ なので, $n_0(E,2)\geq 1$ である. より強く, 任意の $n\geq 1$ に対して $\mathrm{rank}_{\mathbb{Z}}E(\mathbb{Q}_n^{\mathrm{cyc}})=1$ であることが栗原-大槻 [7] の主定理からわかるので, この場合は $n_0(E,2)=1$ である.
(2) $p=2$, $E: y^2+xy=x^3-115x+392$ とすると, Magma を用いて

$$\mathrm{rank}_{\mathbb{Z}}E(\mathbb{Q})=0<\mathrm{rank}_{\mathbb{Z}}E(\mathbb{Q}_1^{\mathrm{cyc}})=1<\mathrm{rank}_{\mathbb{Z}}E(\mathbb{Q}_2^{\mathrm{cyc}})=3$$

であることが確認できる. 実際, E は

$$\begin{cases} (0, 14\sqrt{2})\in E(\mathbb{Q}_1^{\mathrm{cyc}}), \\ \left(40-36\sqrt{2},\ -20+18\sqrt{2}+(558-402\sqrt{2})\sqrt{2+\sqrt{2}}\right)\in E(\mathbb{Q}_2^{\mathrm{cyc}}) \end{cases}$$

という位数無限の点を持ち, これらは共役とあわせて rank 3 の部分群を生成する. よって $n_0(E,2)\geq 2$ であるが, Mazur の control 定理を用いると $n\geq 2$ のとき $\mathrm{rank}_{\mathbb{Z}}E(\mathbb{Q}_n^{\mathrm{cyc}})=3$ であることがわかるので, $n_0(E,2)=2$ となる ([3, p. 137] 参照).
(3) $p=3$, $E: y^2=x^3+x^2+4x+4$ とする (modular 曲線 $X_0(20)$). $\mathbb{Q}_1^{\mathrm{cyc}}$ は $\mathbb{Q}$ に $\eta=\zeta_9+\zeta_9^{-1}$ を添加して得られる体であり, η の $\mathbb{Q}$ 上の最小多項式は x^3-3x+1 である. ここで,

$$\begin{aligned}(\eta+1)^3+(\eta+1)^2+4(\eta+1)+4&=\eta^3+4\eta^2+9\eta+10\\&=4\eta^2+12\eta+9=(2\eta+3)^2\end{aligned}$$

より, $(\eta+1, 2\eta+3)\in E(\mathbb{Q}_1^{\mathrm{cyc}})$ という有理点が得られる. この点は位数無限であり, $\mathrm{rank}_{\mathbb{Z}}E(\mathbb{Q}_1^{\mathrm{cyc}})>\mathrm{rank}_{\mathbb{Z}}E(\mathbb{Q})=0$ となる. 更に (2) と同様に control 定理を用いた議論で, 任意の $n\geq 1$ に対し $\mathrm{rank}_{\mathbb{Z}}E(\mathbb{Q}_n^{\mathrm{cyc}})=2$ となることが示せるので, $n_0(E,3)=1$ を得る.

もう少し一般に, $\mathbb{Q}_n^{\mathrm{cyc}}$ の $\mathbb{Q}$ 上の拡大次数が 9 以下の場合には, 代数体の 9 次以下の拡大から得られるある Galois 表現を楕円曲線の Mordell-Weil 群で実現する Rohrlich の構成法 [13] を用いて, 次が示せる ([4, p. 418], [8] 参照).

定理 1.9 (Rohrlich)**.** $p^n=[\mathbb{Q}_n^{\mathrm{cyc}}:\mathbb{Q}]\leq 9$ ならば, $\mathrm{rank}_{\mathbb{Z}}E(\mathbb{Q}_n^{\mathrm{cyc}})>\mathrm{rank}_{\mathbb{Z}}E(\mathbb{Q}_{n-1}^{\mathrm{cyc}})$ となる $\mathbb{Q}$ 上の楕円曲線 E が無限個存在する.

系 1.10. 次の各条件を満たす $\mathbb{Q}$ 上の楕円曲線 E がそれぞれ無限個存在する:

$$\text{(i) } n_0(E,2)\geq 3,\quad \text{(ii) } n_0(E,3)\geq 2,\quad \text{(iii) } n_0(E,5)\geq 1,\quad \text{(iv) } n_0(E,7)\geq 1.$$

例. $p=2$, $n=3$ とする. $\mathbb{Q}_3^{\mathrm{cyc}}=\mathbb{Q}(\alpha_3)$ であり (α_3 は補題 1.1 のもの), α_3 の $\mathbb{Q}$ 上の最小多項式は $x^8-8x^6+20x^4-16x^2+2$ である. ここで平面 3 次曲線 C を

$$1-8x+20x^2-16y^2+2xy^2-15(x^3-y^2)=0$$

と定めると, $(0,1)\in C(\mathbb{Q})$ かつ $(\frac{1}{\alpha_3^2}, \frac{1}{\alpha_3^3})\in C(\mathbb{Q}_3^{\mathrm{cyc}})$ であることが容易にわかる. C の方程式を Weierstrass 方程式に変換すると $E: y^2=x^3-2x+1$ という導手 40 の楕円曲線となり, $(\frac{2\alpha_3^3-6\alpha_3}{\alpha_3^3-3\alpha_3-1}, \frac{\alpha_3^6-8\alpha_3^4+15\alpha_3^2-1}{(\alpha_3^3-3\alpha_3-1)^2})\in E(\mathbb{Q}_3^{\mathrm{cyc}})$ という有理点を得る. このとき, $\mathrm{rank}_{\mathbb{Z}}E(\mathbb{Q}_3^{\mathrm{cyc}})>\mathrm{rank}_{\mathbb{Z}}E(\mathbb{Q}_2^{\mathrm{cyc}})$ であり, $n_0(E,2)\geq 3$ であることが示せる (命題 2.9 も見よ).

2　主結果

本稿の主結果は, 前節の Rohrlich の結果 (系 1.10) ではカバーされない, $p = 2$ かつ $n = 4$ の場合に関するものである. 前節の記号を用いた形で主定理を再掲する.

定理 2.1. $\mathbb{Q}_n^{\mathrm{cyc}}$ を $\mathbb{Q}$ の円分 $\mathbb{Z}_2$ 拡大の n-th layer とするとき, $\mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}_4^{\mathrm{cyc}}) > \mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}_3^{\mathrm{cyc}})$ を満たし, $n_0(E, 2) \geq 4$ であるような $\mathbb{Q}$ 上の楕円曲線 E が無限個存在する.

2.1　証明の概略

まず, 定理 2.1 の証明の概略を述べる. 証明において重要となるのは次の楕円曲線である.

定義 2.2. 方程式 $y^2 = x^3 + x^2 - 3x + 1$ によって定義される $\mathbb{Q}$ 上の楕円曲線を A とする.

この曲線 A は, Cremona の表 [2] で `256a1` と呼ばれる導手 256 の曲線であり, $\mathbb{Q}(\sqrt{-2})$ の整数環に CM を持つ. 注意したいのは, $\mathrm{rank}_{\mathbb{Z}} A(\mathbb{Q}_4^{\mathrm{cyc}}) = \mathrm{rank}_{\mathbb{Z}} A(\mathbb{Q}_3^{\mathrm{cyc}})$ が成り立つため, A 自身は定理の主張を満たすものではないということである. この A は, 定理 2.1 の条件を満たす曲線 E を作るために用いられる. その際, 重要となるのが次の事実である.

補題 2.3. $A(\mathbb{Q}) \cong \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ である. 特に A は無限個の $\mathbb{Q}$-有理点を持つ.

この $A(\mathbb{Q})$ の各点に対し, ある $\mathbb{Q}$ 上の曲線を対応させる.

定義 2.4. 有理点 $P = (a, b) \in A(\mathbb{Q}) - \{O\}$ に対し, $c, d \in \mathbb{Q}$ を以下のように定める:

$$\begin{cases} c = a^5 + 11a^4 - 106a^3 - 30a^2 + 205a - 49 - 8b(a^3 - 6a^2 - a + 4), \\ d = 2a^5 + 22a^4 + 12a^3 + 164a^2 - 262a + 126 - 4b(3a^3 + 3a^2 + 11a - 9). \end{cases}$$

補題 2.5. $P = (a, b) \in A(\mathbb{Q}) - \{O\}$ に対し, Weierstrass 方程式 $y^2 = x^3 - 4cx^2 + (2c^2 + cd)x$ が定める曲線が非特異となるための必要十分条件は, $P = (a, b) \neq (1, 0), (0, 1), (-1, -2), (9, 28)$ であること.

略証. この Weierstrass 方程式の判別式は $64c^3(2c - d)(2c + d)^2$ である. $c = 0$ と $b^2 = a^3 + a^2 - 3a + 1$ を連立すると,

$$(a - 9)^2(a^4 - 20a^3 + 34a^2 - 12a + 1)(a^4 - 4a^3 - 14a^2 + 4a + 17) = 0$$

が得られ, $c = 0 \Leftrightarrow (a, b) = (9, 28)$ がわかる. 同様にして, $2c - d = 0 \Leftrightarrow (a, b) = (1, 0), (9, 28)$ および $2c + d = 0 \Leftrightarrow (a, b) = (0, 1), (-1, -2), (9, 28)$ が示される. □

定義 2.6. $\mathcal{B} = \{O, (1, 0), (0, 1), (-1, -2), (9, 28)\} \subset A(\mathbb{Q})$ と置き, $P = (a, b) \in A(\mathbb{Q}) - \mathcal{B}$ に対し, Weierstrass 方程式 $y^2 = x^3 - 4cx^2 + (2c^2 + cd)x$ が定める $\mathbb{Q}$ 上の楕円曲線を E_P とする.

E_P の j 不変量は定数ではないので, P が $A(\mathbb{Q}) - \mathcal{B}$ を動くと無限個の同型でない楕円曲線が現れる. よって, 定理 2.1 は次の命題から直ちに従う.

命題 2.7. 任意の $P \in A(\mathbb{Q}) - \mathcal{B}$ に対し, $\mathrm{rank}_{\mathbb{Z}} E_P(\mathbb{Q}_4^{\mathrm{cyc}}) > \mathrm{rank}_{\mathbb{Z}} E_P(\mathbb{Q}_3^{\mathrm{cyc}})$ が成り立つ.

以下, この命題の証明の概略を述べる. まず, E_P の $\mathbb{Q}_4^{\mathrm{cyc}}$-有理点を 1 つ与える.

補題 2.8. $P=(a,b)\in A(\mathbb{Q})-\mathcal{B}$ に対し,

$$\begin{cases} s=-4a+b+8, \\ t=6a-2b+2, \\ u=-4a^2+ab+20a-3b-24, \\ v=-6a^2+2ab-8a+2b-2 \end{cases}$$

と定め, $\beta=s\alpha_2^3+t\alpha_2^2+u\alpha_2+v\in\mathbb{Q}_2^{\mathrm{cyc}}$ と置く. そのとき, $(c\alpha_4^2, c\alpha_3^{-1}\alpha_4\beta)\in E_P(\mathbb{Q}_4^{\mathrm{cyc}})$.

証明方針. $b^2=a^3+a^2-3a+1$ と $\alpha_n^2=\alpha_{n-1}+2$ を用いて計算する. □

この有理点 $R=(c\alpha_4^2, c\alpha_3^{-1}\alpha_4\beta)$ は明らかに $E_P(\mathbb{Q}_3^{\mathrm{cyc}})$ には属していないが, 任意の $m\geq 1$ に対し mR も $E_P(\mathbb{Q}_3^{\mathrm{cyc}})$ に属さないことが示せれば, $\mathrm{rank}_{\mathbb{Z}}E_P(\mathbb{Q}_4^{\mathrm{cyc}})>\mathrm{rank}_{\mathbb{Z}}E_P(\mathbb{Q}_3^{\mathrm{cyc}})$ となることがわかる. ここで, $\mathrm{Gal}(\mathbb{Q}_4^{\mathrm{cyc}}/\mathbb{Q}_3^{\mathrm{cyc}})$ の生成元を σ とするとき, $\sigma(\alpha_4)=-\alpha_4$, $\sigma(\alpha_3)=\alpha_3$, $\sigma(\beta)=\beta$ であることより,

$$\sigma(R)=(c\alpha_4^2, -c\alpha_3^{-1}\alpha_4\beta)=-R$$

を得る. そこでもし, ある $m\geq 1$ に対し $mR\in E_P(\mathbb{Q}_3^{\mathrm{cyc}})$ となるならば,

$$2mR=mR+mR=mR+\sigma(mR)=m(R+\sigma(R))=O$$

となり, R は位数有限である. しかし, それは次の一般的な命題に矛盾する.

命題 2.9. $\mathbb{Q}$ 上の任意の楕円曲線 E と $n\geq 3$ に対し, $E(\mathbb{Q}_n^{\mathrm{cyc}})_{\mathrm{tors}}=E(\mathbb{Q}_2^{\mathrm{cyc}})_{\mathrm{tors}}$ が成り立つ.

証明概略. $E(\mathbb{Q}_n^{\mathrm{cyc}})_{\mathrm{tors}}\neq E(\mathbb{Q}_{n-1}^{\mathrm{cyc}})_{\mathrm{tors}}$ $(n\geq 3)$ であるとすると, ある素数 ℓ と $k\geq 1$ に対し, 位数 ℓ^k の点 $Q\in E(\mathbb{Q}_n^{\mathrm{cyc}})-E(\mathbb{Q}_{n-1}^{\mathrm{cyc}})$ が存在する. ℓ が奇数のとき, $\mathbb{Q}_n^{\mathrm{cyc}}$ が総実であることより $E(\mathbb{Q}_n^{\mathrm{cyc}})$ の ℓ^k 等分点全体 $E(\mathbb{Q}_n^{\mathrm{cyc}})[\ell^k]$ は位数 ℓ^k の巡回群である. よって, Q は Galois 不変な巡回部分群 $\langle Q\rangle$ を生成し, modular 曲線 $X_0(\ell^k)$ の cusp でない $\mathbb{Q}$-有理点を与える. Mazur の結果 [10, Theorem 1] により, ℓ は $3,5,7,11,13,17,19,37,43,67,163$ のいずれかとなる. 一方, $\mathrm{Gal}(\mathbb{Q}_n^{\mathrm{cyc}}/\mathbb{Q})$ から $\langle Q\rangle$ の自己同型群への自然な写像は単射となるので, $\ell\equiv 1\pmod{2^n}$ であり, $\ell=17$ となることがわかる. しかしその場合, $\mathbb{Q}$ に点 Q の座標を添加する拡大で 17 は分岐することが示せるため, $\mathbb{Q}_n^{\mathrm{cyc}}/\mathbb{Q}$ で 17 が不分岐であることに反する. $\ell=2$ の場合は $E(\mathbb{Q}_n^{\mathrm{cyc}})[2^k]$ が巡回群となるとは限らないが, $X_0(32)$ が $\mathbb{Q}_1^{\mathrm{cyc}}=\mathbb{Q}(\sqrt{2})$ 上に cusp でない有理点を持たないことに矛盾することが示せる. □

よって, 命題 2.7 および定理 2.1 は証明された.

2.2 構成のアイデア

上の 2.1 では, 楕円曲線と有理点を具体的に与えてしまうことによって主定理が証明されることを見た. 次に, その曲線や有理点はどのようにして得られたのかを述べる.

目標は $\mathrm{rank}_{\mathbb{Z}}E(\mathbb{Q}_4^{\mathrm{cyc}})>\mathrm{rank}_{\mathbb{Z}}E(\mathbb{Q}_3^{\mathrm{cyc}})$ を満たす $\mathbb{Q}$ 上の楕円曲線 E を見つけることである. 楕円曲線を定める方法は色々とあるが, ここでは単純に Weierstrass 方程式 $y^2=f(x)$ $(f(x)\in\mathbb{Q}[x],\ \deg f(x)=3)$ を考える. 命題 2.9 により, $x_0\in\mathbb{Q}_3^{\mathrm{cyc}}$ かつ $y_0\notin\mathbb{Q}_3^{\mathrm{cyc}}$ なる点 $(x_0,y_0)\in E(\mathbb{Q}_4^{\mathrm{cyc}})$ が存在するような $f(x)$ を探せば良い. $\mathbb{Q}_4^{\mathrm{cyc}}$ は $\mathbb{Q}_3^{\mathrm{cyc}}$ に $\alpha_4=\sqrt{\alpha_3+2}$ を添加

して得られる 2 次拡大なので, $(\alpha_3+2)f(x_0) \in (\mathbb{Q}_3^{\mathrm{cyc}})^{\times 2}$ となるような $f(x)$ と $x_0 \in \mathbb{Q}_3^{\mathrm{cyc}}$ を探すことになる. ここで, $x_0 = \alpha_3$ かつ $(x+2)|f(x)$, と仮定してしまう. すると, $g(\alpha_3) \in (\mathbb{Q}_3^{\mathrm{cyc}})^{\times 2}$ となるような 2 次式 $g(x) \in \mathbb{Q}[x]$ を探し, $f(x) = (x+2)g(x)$ と置くことになる. 更に, $g(x)$ は 1 次の項を持たない, と仮定してしまうと, $\alpha_3^2 = \alpha_2 + 2$ より $g(\alpha_3) = c\alpha_2 + d$ $(c, d \in \mathbb{Q})$ と表せる. $\mathbb{Q}_3^{\mathrm{cyc}} = \mathbb{Q}_2^{\mathrm{cyc}}(\sqrt{\alpha_2+2})$ であるから, $(\alpha_2+2)(c\alpha_2+d) \in (\mathbb{Q}_2^{\mathrm{cyc}})^{\times 2}$ となれば望み通り $g(\alpha_3) \in (\mathbb{Q}_3^{\mathrm{cyc}})^{\times 2}$ となる. よって, $(\alpha_2+2)(c\alpha_2+d) = \beta^2$ となる $\beta \in \mathbb{Q}_2^{\mathrm{cyc}}$ が存在する $c, d \in \mathbb{Q}$ を探し, $f(x) = (x+2)(cx^2 - 2c + d)$ と置けば良い. ($f(x)$ が重根を持たないための条件も必要となる.)

$\mathbb{Q}_2^{\mathrm{cyc}} = \mathbb{Q}(\alpha_2)$ は 4 次体なので, $\mathbb{Q}_2^{\mathrm{cyc}}$ の任意の元は $\alpha_2^3, \alpha_2^2, \alpha_2, 1$ の $\mathbb{Q}$ 上の 1 次結合として一意的に表される. $\beta = s\alpha_2^3 + t\alpha_2^2 + u\alpha_2 + v$ $(s, t, u, v \in \mathbb{Q})$ および $\beta^2 = w_3\alpha_2^3 + w_2\alpha_2^2 + w_1\alpha_2 + w_0$ $(w_i \in \mathbb{Q})$ とすると, $\alpha_2^4 - 4\alpha_2^2 + 2 = 0$ より,

$$\begin{cases} w_3 = 8st + 2sv + 2tu, \\ w_2 = 14s^2 + 8su + 4t^2 + 2tv + u^2, \\ w_1 = -4st + 2uv, \\ w_0 = -8s^2 - 4su - 2t^2 + v^2 \end{cases}$$

であるが, $\beta^2 = (\alpha_2+2)(c\alpha_2+d) = c\alpha_2^2 + (2c+d)\alpha_2 + 2d$ となるためには

$$\begin{cases} w_3 = 0, \\ 4w_2 - 2w_1 + w_0 = 0 \end{cases} \tag{3}$$

が満たされ, $c = w_2$, $d = \frac{w_0}{2}$ であれば良い. w_i は s, t, u, v の 2 次同次式でなので (3) は射影空間 $\mathbb{P}^3$ 内の 2 つの 2 次曲面の交わりと見なすことができ, 種数 1 の曲線 C が定まる. 更にこの C は, $(c, d) = (1, 2)$ に対応する自明な $\mathbb{Q}$-有理点 $(s, t, u, v) = (0, 0, 1, 2)$ を持つので, $\mathbb{Q}$ 上の楕円曲線となる. C の定義方程式 (3) は具体的には

$$\begin{cases} 4st + sv + tu = 0, \\ 48s^2 + 8st + 28su + 14t^2 + 8tv + 4u^2 - 4uv + v^2 = 0 \end{cases}$$

となるが, これを標準的な方法により Weierstrass 方程式に変換すると, 定義 2.2 の $A : y^2 = x^3 + x^2 - 3x + 1$ が得られる. 補題 2.8 の関係式がその変換の逆となっており, $P = (a, b) \in A(\mathbb{Q}) - \mathcal{B}$ に対して $c = w_2$, $d = \frac{w_0}{2}$ を求めたものが定義 2.4, そしてそれを用いて作った $y^2 = (x+2)(cx^2 - 2c + d)$ を少し変数変換したものが定義 2.6 の E_P ということであった.

3 計算例

この節では, 主定理と関連するいくつかの計算例を紹介する. まず, $P = (0, -1) \in A(\mathbb{Q}) - \mathcal{B}$ に対する楕円曲線 $E = E_P$ を調べる. この点に対する定義 2.4 の c, d は $c = -17$, $d = 90$ となり, E は $y^2 = x^3 + 68x^2 - 952x$ という Weierstrass 方程式で定義される. この曲線は導手が $8027264 = 2^7 \cdot 7 \cdot 17^2 \cdot 31$ であり, $E(\mathbb{Q}) \cong \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ である. 補題 2.8 の有理点は $(-17\alpha_4^2, -17\alpha_3^{-1}\alpha_4(7\alpha_2^3 + 4\alpha_2^2 - 21\alpha_2 - 4)) \in E(\mathbb{Q}_4^{\mathrm{cyc}})$ となり, (命題 2.9 を使っても使わなくても) $\mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}_4^{\mathrm{cyc}}) > \mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}_3^{\mathrm{cyc}})$ であることがわかる. 合同式 (2) より $\mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}_4^{\mathrm{cyc}}) \geq \mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}_3^{\mathrm{cyc}}) + 8$ であるが, E および E のある twist の $\mathbb{Q}_3^{\mathrm{cyc}}$ 上の 2-Selmer 群を Magma で計算することにより,

$\mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}_3^{\mathrm{cyc}}) \leq 2$ かつ $\mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}_4^{\mathrm{cyc}}) \leq 10$ であることがわかる. $(16, 56\sqrt{2}) \in E(\mathbb{Q}_1^{\mathrm{cyc}})$ もあわせると,

$$\mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}_1^{\mathrm{cyc}}) = \mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}_2^{\mathrm{cyc}}) = \mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}_3^{\mathrm{cyc}}) = 2 < \mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}_4^{\mathrm{cyc}}) = 10$$

を得る[3].

別の 3 点 $(-1, 2), (9, -28), (\frac{5}{4}, \frac{7}{8}) \in A(\mathbb{Q}) - \mathcal{B}$ に対応する楕円曲線は順に

$$\begin{aligned} y^2 &= x^3 + 544x^2 - 60928x, \\ y^2 &= x^3 - 426496x^2 + 82924470272x, \\ y^2 &= x^3 - \frac{16337}{256}x^2 + \frac{486695567}{262144}x \end{aligned}$$

となるが, これらの導手はいずれも $(0, -1)$ に対応する曲線と同じ 8027264 である. 実はこれらの曲線は, 次数 2 の同種写像か $\mathbb{Q}_1^{\mathrm{cyc}} = \mathbb{Q}(\sqrt{2})$ 上の同型写像でつながっており, $\mathbb{Q}_n^{\mathrm{cyc}}$ $(n \geq 1)$ 上でのこれらの rank は一致することがわかる. 他の $A(\mathbb{Q}) - \mathcal{B}$ の点でも同様の関係にある点の組を見つけることができる.

前節の構成法は, 作り方からもわかるように, $n_0(E, 2) \geq 4$ を満たす全ての $\mathbb{Q}$ 上の楕円曲線を与える訳ではない. 例えば, $y^2 + y = x^3 + x^2 - 7x + 5$ で定義される曲線 ([2] の `91B1`) を E_1 とすると, x 座標が $-\frac{1}{2}(\alpha_3^7 + \alpha_3^6 - 6\alpha_3^5 - 6\alpha_3^4 + 9\alpha_3^3 + 10\alpha_3^2 - \alpha_3 - 4)$ であるような $\mathbb{Q}_4^{\mathrm{cyc}}$-有理点を持つことが Magma によってわかり, $n_0(E_1, 2) \geq 4$ であることが示せる. 前節の構成法で得られる楕円曲線は位数 2 の $\mathbb{Q}$-有理点を持つが, この E_1 は $E_1(\mathbb{Q})_{\mathrm{tors}} = 0$ であるため, その構成法では得られない例になっている. $E_2 : y^2 + y = x^3 - x^2 - 9x + 9$ も $E_2(\mathbb{Q})_{\mathrm{tors}} = 0$ であるが,

$$\mathrm{rank}_{\mathbb{Z}} E_2(\mathbb{Q}_4^{\mathrm{cyc}}) > \mathrm{rank}_{\mathbb{Z}} E_2(\mathbb{Q}_3^{\mathrm{cyc}}) > \mathrm{rank}_{\mathbb{Z}} E_2(\mathbb{Q}_2^{\mathrm{cyc}})$$

を満たし, $n_0(E_2, 2) \geq 4$ かつ $\mathrm{rank}_{\mathbb{Z}} E_2(\mathbb{Q}_4^{\mathrm{cyc}}) \geq 15$ となっていることがわかる.

E_1, E_2 の rank が $\mathbb{Q}_4^{\mathrm{cyc}}/\mathbb{Q}_3^{\mathrm{cyc}}$ で増えることを確かめる ($\mathbb{Q}_4^{\mathrm{cyc}}$-有理点を見つける) のも容易なことではないが[4], どの曲線が増えるかわからない状態で闇雲に探すのはとても困難である. これらの曲線は, 適当な Dirichlet 指標でひねった L 関数の特殊値を (やはり Magma で) 計算することにより見つけたものである. 加藤の結果 (定理 1.5) により, 特殊値が 0 でなければ rank は増えないが, 特殊値が 0 の場合は Birch, Swinnerton-Dyer 予想により rank が増えると期待される. その計算を導手 3500 以下の曲線に対して実行したところ, $\mathbb{Q}_4^{\mathrm{cyc}}/\mathbb{Q}_3^{\mathrm{cyc}}$ で rank が増えると期待される曲線の同種類[5]は 33 個見つかった (全同種類の個数は 11363). 特に E_1 はその中で導手が最小のものである.

いくつかの p, n に対し, $\mathbb{Q}_n^{\mathrm{cyc}}/\mathbb{Q}_{n-1}^{\mathrm{cyc}}$ で rank が増えると期待される楕円曲線を同じ範囲で探したところ, その同種類の個数は以下の表 (横が p で縦が n, $-$ は未計算) のようになった.

	2	3	5	7	11	13	17	19
1	6285	1348	305	58	9	1	0	0
2	1246	99	0	0	−	−	−	−
3	290	0	−	−	−	−	−	−
4	33	−	−	−	−	−	−	−
5	1	−	−	−	−	−	−	−

[3]任意の $n \geq 4$ に対し $\mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}_n^{\mathrm{cyc}}) = 10$ となっていると想像されますが, 示してはいません.

[4]Magma を使うと見つけられるということも驚きなのですが.

[5]楕円曲線の rank および L 関数の特殊値が 0 となるか否かは同種類の中で変わりません.

この中で,

$$E_3 : y^2 = x^3 - x^2 - 685x + 7134 \quad (\texttt{1324b1}),$$
$$E_4 : y^2 + xy = x^3 + 36x - 81 \quad (\texttt{651d1}),$$
$$E_5 : y^2 = x^3 - x^2 - 40x + 108 \quad (\texttt{1304a1})$$

は $n_0(E_3, 2) \geq 5$, $n_0(E_4, 11) \geq 1$, $n_0(E_5, 13) \geq 1$ を満たすと期待されるが, 具体的な有理点はまだ見つけられていない.

参考文献

[1] G. Chinta, *Analytic ranks of elliptic curves over cyclotomic fields*, J. Reine Angew. Math. **544** (2002), 13–24.

[2] J. E. Cremona, Algorithms for Modular Elliptic Curves, 2nd edition, Cambridge University Press, 1997.

[3] R. Greenberg, *Iwasawa theory for elliptic curves*, In: Arithmetic Theory of Elliptic Curves, 51–144, Lecture Notes in Math., 1716, Springer, Berlin, 1999.

[4] R. Greenberg, *Introduction to Iwasawa theory for elliptic curves*, In: Arithmetic Algebraic Geometry, 407–464, IAS/Park City Math. Series, 9, Amer. Math. Soc., Providence, RI, 2001.

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

[6] M. Kurihara, *On the Tate-Shafarevich groups over cyclotomic fields of an elliptic curve with supersingular reduction I*, Invent. Math. **149** (2002), 195–224.

[7] M. Kurihara and R. Otsuki, *On the growth of Selmer groups of an elliptic curve with supersingular reduction in the* $\mathbf{Z}_2$*-extension of* $\mathbf{Q}$, Pure Applied Math. Quat. **2** (2006), 557–568.

[8] K. Matsuno, *A note on the growth of Mordell-Weil ranks of elliptic curves in cyclotomic* $\mathbb{Z}_p$*-extensions*, Proc. Japan Acad. Ser. A Math. Sci. **79** (2003), 101–104.

[9] B. Mazur, *Rational points of abelian varieties with values in towers of number fields*, Invent. Math. **18** (1972), 183–266.

[10] B. Mazur, *Ratoinal isogenies of prime degree*, Invent. Math. **44** (1978), 129–162.

[11] 落合理, 岩澤理論とその展望 (上), 岩波書店, 2014.

[12] D. E. Rohrlich, *On L-functions of elliptic curves and cyclotomic towers*, Invent. Math. **75** (1984), 409–423.

[13] D. E. Rohrlich, *Realization of some Galois representations of low degree in Mordell-Weil groups*, Math. Research Letters **4** (1997), 123–130.