数理解析研究所講究録 1376 巻 2004 年 85-91

Torsion subgroups of elliptic curves in elementary abelian 2-extensions of $\mathbf{Q}$

東北大学大学院理学研究科　藤田 育嗣 (Yasutsugu Fujita)
Mathematical Institute of Tohoku University

1 序

E を有理数体 $\mathbf{Q}$ 上定義された楕円曲線とするとき，Mazur の定理により，群 $E(\mathbf{Q})_{\mathrm{tors}}$ は次のいずれかに同型である：

$$\begin{array}{ll} \mathbf{Z}/N\mathbf{Z}, & N=1,\ldots,10,12, \\ \mathbf{Z}/2\mathbf{Z}\oplus\mathbf{Z}/2N\mathbf{Z}, & N=1,2,3,4. \end{array}$$

F を $\mathbf{Q}$ の最大初等アーベル 2 拡大体，即ち，$F:=\mathbf{Q}(\{\sqrt{m}:m\in\mathbf{Z}\})$ とすると，楕円曲線 $E/\mathbf{Q}$ の F 上の torsion 部分群 $E(F)_{\mathrm{tors}}$ は，高々 31 種類しかないことが知られている：

定理 1.1. ([3, Theorem])　E を $\mathbf{Q}$ 上定義された楕円曲線とし，$F:=\mathbf{Q}(\{\sqrt{m};m\in\mathbf{Z}\})$ とおく．このとき $E(F)_{\mathrm{tors}}$ は次の 31 種類の群のいずれかに同型である：

$$\begin{array}{ll} \mathbf{Z}/2^{a+b}\mathbf{Z}\oplus\mathbf{Z}/2^{a}\mathbf{Z}, & a=1,2,3,\ b=0,1,2,3, \\ \mathbf{Z}/2^{a+b}\mathbf{Z}\oplus\mathbf{Z}/2^{a}\mathbf{Z}\oplus\mathbf{Z}/3\mathbf{Z}, & a=1,2,3,\ b=0,1, \\ \mathbf{Z}/2^{a}\mathbf{Z}\oplus\mathbf{Z}/2^{a}\mathbf{Z}\oplus\mathbf{Z}/5\mathbf{Z}, & a=1,2,3, \\ \mathbf{Z}/2^{a}\mathbf{Z}\oplus\mathbf{Z}/2^{a}\mathbf{Z}\oplus\mathbf{Z}/3\mathbf{Z}\oplus\mathbf{Z}/3\mathbf{Z}, & a=1,2,3 \end{array}$$

または $\{O\}$, $\mathbf{Z}/3\mathbf{Z}$, $\mathbf{Z}/3\mathbf{Z}\oplus\mathbf{Z}/3\mathbf{Z}$, $\mathbf{Z}/5\mathbf{Z}$, $\mathbf{Z}/7\mathbf{Z}$, $\mathbf{Z}/9\mathbf{Z}$, $\mathbf{Z}/15\mathbf{Z}$.

しかしこれらの 31 種類の群すべてが $E(F)_{\mathrm{tors}}$ として実現されるかどうかは知られていない．

ここでは, $E(F)_{\mathrm{tors}}$ としてちょうど 20 種類の可能性があることを示す．

定理 1. E を $\mathbf{Q}$ 上の楕円曲線とし，$F := \mathbf{Q}(\{\sqrt{m};\, m \in \mathbf{Z}\})$ とおく．このとき $E(F)_{\mathrm{tors}}$ は次の 20 種類の群のいずれかに同型である：

$$\begin{array}{ll} \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2N\mathbf{Z}, & N = 1,2,3,4,5,6,8, \\ \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/4N\mathbf{Z}, & N = 1,2,3,4, \\ \mathbf{Z}/2N\mathbf{Z} \oplus \mathbf{Z}/2N\mathbf{Z}, & N = 3,4 \end{array}$$

または $\{O\}$, $\mathbf{Z}/3\mathbf{Z}$, $\mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/3\mathbf{Z}$, $\mathbf{Z}/5\mathbf{Z}$, $\mathbf{Z}/7\mathbf{Z}$, $\mathbf{Z}/9\mathbf{Z}$, $\mathbf{Z}/15\mathbf{Z}$. しかもこれらの各群を $E(F)_{\mathrm{tors}}$ として実現するような $\mathbf{Q}$ 上の楕円曲線 E が存在する．

記号． $F := \mathbf{Q}(\{\sqrt{m};\, m \in \mathbf{Z}\})$;

$\mathcal{O}_F$: F の代数的整数のなす環;

E^D: E の D-quadratic twist (D: square-free な整数).

A を有限生成アーベル群, p を素数とするとき,

A_{tors}: A の torsion 部分群,

$A_{(p)}$: A_{tors} の p シロー部分群,

$A_{(2')}$: A_{tors} の奇数位数の元の集合

とかく．

2 巡回群でない場合

E を $\mathbf{Q}$ 上定義された楕円曲線とする．$E(\mathbf{Q})_{\mathrm{tors}}$ が巡回群でない場合には, torsion 部分群 $E(F)_{\mathrm{tors}}$ は完全に分類できる．

定理 2.1. [1, Theorem 1] E を

$$E : y^2 = x(x+M)(x+N), \quad M, N \in \mathbf{Z},\ M > N,$$

で定義された $\mathbf{Q}$ 上の楕円曲線とする．$\gcd(M,N)$ を square-free な整数 または 1 と仮定する．このとき $E(F)_{\mathrm{tors}}$ は次のように分類される：

(a) $E(\mathbf{Q})_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}$ のとき，$E(F)_{\mathrm{tors}} \simeq \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/16\mathbf{Z}$.

(b) $E(\mathbf{Q})_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/6\mathbf{Z}$ のとき，$E(F)_{\mathrm{tors}} \simeq \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/12\mathbf{Z}$.

(c) $E(\mathbf{Q})_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$ のとき，$E(F)_{\mathrm{tors}} \simeq \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}$ または $\mathbf{Z}/8\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}$. この場合，$M, N$ ともに squares であると仮定してよい．このとき，$E(F)_{\mathrm{tors}}$

$\simeq \mathbf{Z}/8\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}$ となるための必要十分条件は，$M-N$ が square となる（このことは $E^{-1}(\mathbf{Q})_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$ なることと同値である）ことである．

(d) $E(\mathbf{Q})_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$ のとき，$E(F)_{\mathrm{tors}} \simeq \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$, $\mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}$, $\mathbf{Z}/8\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}$, $\mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/12\mathbf{Z}$ または $\mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/16\mathbf{Z}$.　この場合，$E(F)_{\mathrm{tors}} \simeq \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$ となるための必要十分条件は，すべての square-free な整数 D に対して $E^D(\mathbf{Q})_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$ となることである．そうでないとき，$E(F)_{\mathrm{tors}}$ は $E^D(\mathbf{Q})_{\mathrm{tors}} \not\simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$ なる D に対して $E^D(\mathbf{Q})_{\mathrm{tors}}$ ($E^D(\mathbf{Q})_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$ なる場合にはさらに $E^{-D}(\mathbf{Q})_{\mathrm{tors}}$) の type(s) のみに依存して決まる．

定理 2.1 の証明は, 主に次の 3 つの補題を使ってなされる.

補題 2.2. ([2, Theorem 4.2, p. 85])　k を標数が $2,3$ でない体，E を

$$E : y^2 = x(x+\alpha)(x+\beta), \quad \alpha, \beta \in k,$$

で定義された k 上の楕円曲線とする．このとき, 点 $P=(x,y) \in E(k)$ が $E(k)$ に 2 等分点をもつための必要十分条件は, x, $x+\alpha$, $x+\beta$ がすべて k で squares となることである.

補題 2.3. [1, Lemma 3.1]　$R := \mathbf{Z}[\{\sqrt{m}\,;\, m \in \mathbf{Z}\}]$ とおく. 非負整数 d に対し, $\mathcal{O}_F$ の元 a の $\mathbf{Q}$ 上の次数が 2^d ならば, $2^d a \in R$ となる.

補題 2.4. [1, Lemma 3.2]　$\mathcal{O}_F$ の元 a, 奇素数 l, 非負整数 i に対し, $\mathcal{O}_F$ において, もし $l^i\sqrt{l}$ が a^2 を割り切るならば, l^{i+1} もまた a^2 を割り切る.

注意 2.5.　$E(\mathbf{Q})_{\mathrm{tors}}$ が巡回群でない場合には, より一般に F に含まれる任意の代数体 K に対して, $E/\mathbf{Q}$ の torsion 部分群 $E(K)_{\mathrm{tors}}$ を M, N を使って分類することができる ([1, Section 5]). 特に, $E(\mathbf{Q})_{\mathrm{tors}}$ と $E(F)_{\mathrm{tors}}$ の "間" の各 type を $E(K)_{\mathrm{tors}}$ として実現するような楕円曲線 $E/\mathbf{Q}$ と体 $K = \mathbf{Q}(\sqrt{D_1}, \ldots, \sqrt{D_n})$ $(n \leq 4)$ が存在する.

3　巡回群の場合

本節では, 定理 1.1 に現れる群で定理 1 にあげられていないものは $E(F)_{\mathrm{tors}}$ として実現され得ないことを示す.

次の補題は, 補題 2.3 と 2.4 を使えば容易に示される.

補題 3.1. 任意の 0 でない整数 D に対し, $\sqrt{D\sqrt{-1}}$ は F で square でない.

$E(F) \supset \mathbf{Z}/2\mathbf{Z}$ ならば $E(\mathbf{Q}) \supset \mathbf{Z}/2\mathbf{Z}$ であることに注意すれば, 補題 2.2 と 3.1 を使って次が示される.

命題 3.2. $E(\mathbf{Q})_{\mathrm{tors}}$ が巡回群ならば, $E(F) \not\supset \mathbf{Z}/8\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}$ が成り立つ.

除くべき群は, 残り 4 types である.

命題 3.3. E を $\mathbf{Q}$ 上の楕円曲線とするとき, $E(F)_{\mathrm{tors}}$ は次のいずれとも同型になり得ない:

$$\mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/32\mathbf{Z},\ \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/24\mathbf{Z},\ \mathbf{Z}/12\mathbf{Z} \oplus \mathbf{Z}/12\mathbf{Z},\ \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/20\mathbf{Z}.$$

証明は, 次の補題を使って, 次数 2 の $\mathbf{Q}$-isogeny により $E(\mathbf{Q}) \supset \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$ なる場合に帰着させることによってなされる.

補題 3.4. $E(\mathbf{Q})_{\mathrm{tors}}$ が巡回群のとき, $E(F) \supset \mathbf{Z}/4\mathbf{Z}$ であるための必要十分条件は, $E^D(\mathbf{Q}) \supset \mathbf{Z}/4\mathbf{Z}$ となるような D (square-free な整数または 1) が存在することである.

例えば, もし $E(F)_{\mathrm{tors}} \simeq \mathbf{Z}/12\mathbf{Z} \oplus \mathbf{Z}/12\mathbf{Z}$ と仮定すると, 補題 3.4 によって $E(\mathbf{Q})$ は位数 4 の点 P を含むと仮定してよい. $E' := E/\langle [2]P \rangle$ とおくと,

$$E'(\mathbf{Q}) \supset \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z} \quad \text{かつ} \quad E'(F) \supset \mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/3\mathbf{Z}$$

となるが, これは定理 2.1 に反する. 従って $E(F)_{\mathrm{tors}} \not\simeq \mathbf{Z}/12\mathbf{Z} \oplus \mathbf{Z}/12\mathbf{Z}$ が分かる.

4 定理 1 に現れる群の例

[3] ですでに,

$$\mathbf{Z}/5\mathbf{Z},\ \mathbf{Z}/7\mathbf{Z},\ \mathbf{Z}/9\mathbf{Z},\ \mathbf{Z}/15\mathbf{Z},\ \mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/3\mathbf{Z},\ \mathbf{Z}/6\mathbf{Z} \oplus \mathbf{Z}/6\mathbf{Z}$$

の各 type を $E(F)_{\mathrm{tors}}$ として実現するような楕円曲線 $E/\mathbf{Q}$ の存在が分かっている. また, 楕円曲線 $E_1 : y^2 + y = x^3 + x^2$ (導手 43) は $E_1(\mathbf{Q})_{\mathrm{tors}} = \{O\}$ を満たし, かつ, その $\mathbf{Q}$-isogeny 類には $\mathbf{Q}$ 同型類が一つしか存在しないので $E_1(F)_{\mathrm{tors}} = \{O\}$ であり, 楕円曲線 $E_3 : y^2 = x^3 - 4$ は $E_3(\mathbf{Q})_{\mathrm{tors}} \simeq \mathbf{Z}/3\mathbf{Z}$ を満たし, かつ, すべての square-free な整数 D に対し $E_3^D(\mathbf{Q})_{\mathrm{tors}} = \{O\}$ を満たすので $E_3(F)_{\mathrm{tors}} \simeq \mathbf{Z}/3\mathbf{Z}$ である. これらのことは次の補題から即座に分かる.

補題 4.1. E を $\mathbf{Q}$ 上定義された楕円曲線をするとき, 異なる整数 $D_1, \ldots, D_m$ (square-free または 1) が存在して次を満たす:

$$E(F)_{(2')} \simeq E^{D_1}(\mathbf{Q})_{(2')} \oplus \cdots \oplus E^{D_m}(\mathbf{Q})_{(2')}.$$

さらに, 各群 $E^{D_i}(\mathbf{Q})_{(2')}$ は $E(F)_{(2')}$ のある $\mathbf{Q}$ 有理部分群と同型である.

さらに定理 2.1 において,

$$\mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z},\ \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z},\ \mathbf{Z}/8\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z},\ \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/12\mathbf{Z},\ \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/16\mathbf{Z}$$

の各 type を $E(F)_{\mathrm{tors}}$ として実現するような楕円曲線 $E/\mathbf{Q}$ の存在も分かっている. 従って後は,

$$\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/10\mathbf{Z},\ \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/6\mathbf{Z},\ \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/12\mathbf{Z},$$
$$\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z},\ \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z},\ \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z},\ \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/16\mathbf{Z}$$

について, 同じく $E/\mathbf{Q}$ の存在を言えばよい.

(i) $E(F)_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/10\mathbf{Z}$. $E/\mathbf{Q}$ を $E(\mathbf{Q})_{\mathrm{tors}} \simeq \mathbf{Z}/10\mathbf{Z}$ なる楕円曲線とすると, 定理 1.1 と命題 3.2, 3.3 より $E(F)_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/10\mathbf{Z}$ であることが分かる.

(ii) $E(F)_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/6\mathbf{Z}$. $E: y^2 = x^3 + 1$ とすると, $E(\mathbf{Q})_{\mathrm{tors}} = \langle (2,3) \rangle \simeq \mathbf{Z}/6\mathbf{Z}$ であり, すべての square-free な整数 D に対し $E^D(\mathbf{Q})_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z}$ が成り立つので, 補題 3.4 より $E(F)_{(2)} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$ であり, 補題 4.1 より, $E(F)_{(2')} \simeq \mathbf{Z}/3\mathbf{Z}$ であることが分かる. 従って, $E(F)_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/6\mathbf{Z}$ である.

ここで, 簡単な補題を準備する (証明は補題 2.2 を使えば容易になされる).

補題 4.2. E を

$$E: y^2 = x(x + a + b\sqrt{c})(x + a - b\sqrt{c}), \quad a, b \in \mathbf{Z},\ c: \text{square-free な整数},$$

で与えられた $\mathbf{Q}$ 上の楕円曲線とし, $Q_1 := (-a - b\sqrt{c}, 0)$, $R_1 := (-a + b\sqrt{c}, 0)$ とおく. このとき, $Q_1 \in 2E(F)$ (これは $R_1 \in 2E(F)$ と同値である) ならば $c = -1$ である.

(iii) $E(F)_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/12\mathbf{Z}$. $E: y^2 = x(x^2 + 1177x + 50186)$ とすると, $E(\mathbf{Q})_{\mathrm{tors}} = \langle (0,0) \rangle \simeq \mathbf{Z}/12\mathbf{Z}$ である. $f(x) := x^2 + 1177x + 50186$ とおけ

ば, $f(x)$ の判別式 1184585 の square-free part は -1 ではないので, 補題 4.2 より $E(F) \not\supset \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$ である. 従って, $E(F)_{\text{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/12\mathbf{Z}$ が分かる.

(iv) $E(F)_{\text{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$. $E : y^2 = x(x^2-2)$ とすると, $E(\mathbf{Q})_{\text{tors}} \simeq \mathbf{Z}/2\mathbf{Z}$ であり, すべての square-free な整数 D に対し $E^D(\mathbf{Q})_{\text{tors}} \simeq \mathbf{Z}/2\mathbf{Z}$ が成り立つ. 従って, 補題 3.4 と 4.1 から $E(F)_{\text{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$ が分かる.

(v) $E(F)_{\text{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$. $E : y^2 = x(x-1+2\sqrt{-2})(x-1-2\sqrt{-2})$ とすると, $E(\mathbf{Q})_{\text{tors}} = \langle P_2 \rangle \simeq \mathbf{Z}/4\mathbf{Z}$ $(P_2 := (3,6))$ であり, 補題 4.2 より $Q_1 := (1-2\sqrt{-2}, 0) \notin 2E(F)$ が分かるので, $E(F) \not\supset \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$ である. $1+\sqrt{-2}$ は F で square ではないので, 補題 2.2 から $P_2 \notin 2E(F)$ が分かり. 同様にして $P_2 + Q_1 \notin 2E(F)$ も分かるので, $E(F) \not\supset \mathbf{Z}/8\mathbf{Z}$ である. よって, $E(F)_{(2)} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$ が分かる. すべての square-free な整数 D に対し $E^D(\mathbf{Q}) \not\supset \mathbf{Z}/3\mathbf{Z}$ となることは, [4] の Theorem (III) を使えば容易に示される. 従って, 補題 4.1 から $E(F)_{\text{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$ が分かる.

(vi) $E(F)_{\text{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}$. $E : y^2 = x(x-62+6\sqrt{-7})(x-62-6\sqrt{-7})$ とすると, $E(\mathbf{Q})_{\text{tors}} = \langle P_3 \rangle \simeq \mathbf{Z}/8\mathbf{Z}$ $(P_3 = (32, 192))$ であり, 補題 4.2 より $Q_1 := (62-6\sqrt{-7}, 0) \notin 2E(F)$ が分かるので, $E(F) \not\supset \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$ である. $5-\sqrt{-7}$ は F で square ではないので, 補題 2.2 から $P_3 \notin 2E(F)$ が分かり, 同様にして $P_3 + Q_1 \notin 2E(F)$ も分かるので, $E(F) \not\supset \mathbf{Z}/16\mathbf{Z}$ である. よって, $E(F)_{(2)} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}$ が分かる. 従って, 定理 1.1 より $E(F)_{\text{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}$ が分かる.

(vii) $E(F)_{\text{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/16\mathbf{Z}$. $E : y^2 = x(x^2-47x+16^3)$ とすると, $E(\mathbf{Q})_{\text{tors}} = \langle (16^2, 15 \cdot 16^2) \rangle \simeq \mathbf{Z}/8\mathbf{Z}$ である. $E(F)_{\text{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/16\mathbf{Z}$ であることは次の事実から従う:

> $E(\mathbf{Q})_{\text{tors}} = \langle P \rangle \simeq \mathbf{Z}/8\mathbf{Z}$ とするとき, もし $E' := E/\langle [4]P \rangle$ が $E'(\mathbf{Q})_{\text{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}$ を満たすならば, $E(F)_{\text{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/16\mathbf{Z}$ である.

参考文献

[1] Y. Fujita, Torsion subgroups of elliptic curves with non-cyclic torsion over $\mathbf{Q}$ in elementary abelian 2-extensions of $\mathbf{Q}$, preprint.

[2] A. W. Knapp, *Elliptic Curves*, Princeton Univ. Press, Princeton, NJ, 1992.

[3] M. Laska and M. Lorenz, Rational points on elliptic curves over $\mathbf{Q}$ in elementary abelian 2-extensions of $\mathbf{Q}$, J. Reine Angew Math. 355 (1985), 163–172.

[4] D. Qiu and X. Zhang, Explicit classification for torsion subgroups of rational points of elliptic curves, Acta Math. Appl. Sinica (English Ser.) 18 (2002), 539–548.