Elliptic analogue of irregular prime numbers for the p^n-division fields of the curves $y^2 = x^3 - (s^4 + t^2)x$

慶應義塾大学・理工学部大学院理工学研究科 * 松村　英樹
Hideki Matsumura
Faculty of Sciences and Technology
Keio University

-

概要

素数 p が非正則素数であるとは，p 円分体 $\mathbb{Q}(\zeta_p) = \mathbb{Q}(\mathbb{G}_m[p])$ の類数が p で割り切れることである．本研究では，非正則素数の楕円曲線の等分体に対する類似を考える．より正確には，有理数体上の楕円曲線 E の p^n 等分体 $\mathbb{Q}(E[p^n])$ の類数の p 可除性を研究する．西来路 · 山内，平之内，大下及び Prasad–Shekhar らにより，$\mathbb{Q}(E[p^n])$ の類数の p 進付値の様々な下界が得られている．彼らの研究は，E の Mordell–Weil rank が 2 以上の場合に p^n 等分体の類数が多くの場合に p の正冪で割り切れることを示唆している．本研究では，整数 s, t に対し，$y^2 = x^3 - (s^4 + t^2)x$ で定義される楕円曲線の族 $\{E_{s,t}\}$ を扱う．本稿の主結果では，全ての素数 $p \geq 5$ と自然数 n に対し，次の 2 つの性質を満たす $\{E_{s,t}\}$ の無限部分族を構成する：Mordell–Weil rank が 1 であり，p^n 等分体の類数が p^{2n} で割り切れる．我々の構成した楕円曲線の族はある条件を満たす $s^4 + t^2$ 型の素数でパラメトライズされているが，そのような素数の無限性は Friedlander–Iwaniec の定理により保証される．本研究は，臺信直人氏，平川義之輔氏との共同研究である．

1　主定理とその背景

本節では本研究の意義を説明する．

まず，古典的な非正則素数の性質を振り返ることから始める．整数論において，イデアル類群は古くから研究されてきた重要な対象である．イデアル類群は，Kummer により Fermat の最終定理の文脈で研究された．

定義 1.1. 素数 p が非正則素数であるとは，p 円分体 $\mathbb{Q}(\zeta_p) = \mathbb{Q}(\mathbb{G}_m[p])$ の類数が p で割り切れることである．ここで，ζ_p は 1 の原始 p 乗根，$\mathbb{G}_m$ は乗法群，$\mathbb{G}_m[p]$ は $\mathbb{G}_m$ の p ねじれ部分群である．非正則ではない素数を正則素数という．

Kummer は，奇素数 p が非正則であることと p が Bernoulli 数 $B_2, B_4, \ldots, B_{p-3}$ の分子のいずれかを割り切ることが同値であることを証明した．さらに，[15] において奇素数 p が正則素数のとき，方程式 $x^p + y^p = z^p$ は正整数解を持たないことを証明した．

正則素数が無限に存在するかどうかは未解決であるが，非正則素数が無限に存在することは Jensen [13] により証明されている．その後，Carlitz [2] は非正則素数の無限性の簡潔な証明を与えた．また，Carlitz は Euler 数に対して非正則素数の概念を拡張し（E 非正則素数），E 非正則素数の無限性を証明した．その後，Ernvall [7, 8] は，剰余指標 χ に属する一般 Bernoulli 数に対して非正則素数を拡張し（χ 非正則素数），χ 非正則素数の無限性を考えた．$M \in \mathbb{Z}_{\geq 1}$ と素数 p に対し，h を $\mathbb{Q}(\zeta_{Mp})$ の類数，h^+ を $\mathbb{Q}(\zeta_{Mp})$ の最大実部分体の類数とする．$h = h^- h^+$ と書くと，h^- が p で割り切れることと，M が conductor で割り切れ，p が χ 非正則となる

〒223-8522 神奈川県横浜市港北区日吉 3-14-1

ような指標 χ が存在することが同値である．従って，χ 非正則素数の無限性から，以下の主張が導かれる：

各 $M \in \mathbb{Z}_{\geq 1}$ に対して，$\mathbb{Q}(\mathbb{G}_m[Mp])$ の類数が p で割り切れるような素数 p は無限個存在する．

任意の可換群スキーム G と整数 N に対して G の N 等分体が定まるので，$\mathbb{G}_m$ をその他の可換群スキームに置き換えることで非正則素数の類似を定式化することができる．本稿では，代表的な可換群スキームである楕円曲線の p^n 等分体に関する非正則素数類似を考える．

E を $\mathbb{Q}$ 上の楕円曲線とする．$\mathbb{Q}$ の代数閉包 $\overline{\mathbb{Q}}$ を 1 つ取り固定する．E は $y^2 = x^3 + ax + b$ $(a, b \in \mathbb{Q})$ という方程式で定義され，右辺は $\overline{\mathbb{Q}}$ 上に重根を持たない．また，Moredell–Weil の定理より，E の $\mathbb{Q}$ 有理点全体の集合 $E(\mathbb{Q})$ は有限生成 Abel 群をなし，$r(E) := \mathrm{rank}(E(\mathbb{Q}))$ を E の Mordell–Weil rank という．楕円曲線 E と自然数 $N \in \mathbb{N}$ に対し，$E(\overline{\mathbb{Q}})$ の N ねじれ点全体のなす E の部分群を $E[N]$ で表す．E の N 等分体とは，$\mathbb{Q}$ に E の N ねじれ点の座標を添加した体であり，$K_{E,N} := \mathbb{Q}(E[N])$ で表す．$h_{E,N}$ を $K_{E,N}$ の類数とする．

このとき，以下の問題を考える．

問題 1.2. p が素数を走るとき，固定された $\mathbb{Q}$ 上の楕円曲線 E に対して，$h_{E,p}$ は平均して何回 p で割り切れるか？

問題 1.2 に関しては，Ray–Weston [20, Theorem 5.1, 5.2] が部分的な解答を与えている．一方，$\mathbb{G}_m$ の場合と異なり $\mathbb{Q}$ 上には同型でない楕円曲線が無限個存在するため，以下の問題も考えらえれる．

問題 1.3. E が $\mathbb{Q}$ 上の楕円曲線を走るとき，固定された素数 p に対して，$h_{E,p}$ は平均して何回 p で割り切れるか？

問題 1.3 に関しては，Ray–Weston [20, Theorem 4.4] がある予想のもとで部分的解答を得ている．また，小さな p に関しては問題 1.3 に関する無条件な結果も存在する．例えば，$p = 2$ の場合は Li [17, Theorem 1.4] と Bhargava–Shankar [1, Theorem 1.1] を組み合わせることで無条件な結果を得ることができる．

問題 1.2 も問題 1.3 も $h_{E,p}$ の p 可除性に関する確率論的な側面に関する問題だが，以下のような，h_{E,p^n} の p 進付値に関する決定論的な評価に関する結果も存在する．

定理 1.4 ([12, 18, 19, 21, 22])**.** 楕円曲線 E，素数 p，自然数 n に関するある仮定の下で，

$$\mathrm{ord}_p(h_{E,p^n}) \geq 2n(r(E) - 1) - (\text{explicit term} \geq 0).$$

ここで，左辺は h_{E,p^n} の p 進付値である．

注意 1.5.

1. 楕円曲線 E が与えられたとき，上記の (explicit term) は計算可能である．
2. 平之内は，任意の奇素数 $p < 10^6$ と自然数 $n \geq 1$ に対して $\mathrm{ord}_p(h_{E,p^n}) \geq 2n$ となるような楕円曲線 E の具体例を与えた（[12, p. 2, 3]）．
3. Goldfeld と Katz–Sarnak による予想（[10, 14]）より，ほとんど全ての楕円曲線 E は $r(E) \leq 1$ を満たすことが示唆されるが，$r(E) \leq 1$ ならば，定理 1.4 の不等式の右辺は 0 以下になり，$\mathrm{ord}_p(h_{E,p^n})$ の非自明な下界を与えることができない．

注意 1.5 (3) を踏まえて，本研究では，次のような問題を考えた．

問題 1.6 (今回の問題)**.** 固定された p と n に対し，$r(E) \leq 1$ かつ $\mathrm{ord}_p(h_{E,p^n}) > 0$ となるような楕円曲線 E は無限個存在するか？

我々の主定理では，少なくとも $p \geq 5$ の場合は上記の問題に肯定的な回答を与えた．h_{E,p^n} の p 可除性に関する結果はいくつか存在するが，著者達の知る限り，$r(E) \leq 1$ かつ $\mathrm{ord}_p(h_{E,p^n}) > 0$ となるような楕円曲線 E の無限族を構成した文献は存在しなかった．

以下では，$p \geq 5$ を仮定する．また，$E^{(l)}$ を $y^2 = x^3 - lx$ で定義される楕円曲線とする．本稿の主定理を述べる．

定理 1.7 ([5, Theorem 1.3])**.** $p \geq 5$ とする．このとき，以下の条件を満たすような素数 l は無限個存在する．

1. $r(E^{(l)}) = 1$.
2. $\mathrm{ord}_p(h_{E^{(l)},p^n}) \geq 2n$.

2　証明の概略

この節では，定理 1.7 の証明の概略を述べる．まず，定理 1.7 を満たす素数 l のレシピを与える．

定理 2.1 ([5])**.** $p \geq 5$ とし，以下の条件を満たす素数 l を任意に固定する．

1. $l = s^4 + t^2$ となるような $s, t \in \mathbb{Z}$ が存在する．
2. $t \equiv \pm 3 \pmod 8$.
3. $s \equiv 0 \pmod{p^{n+1}}$.

このとき，$r(E^{(l)}) = 1$ かつ $\mathrm{ord}_p(h_{E^{(l)},p^n}) \geq 2n$ が成立する．

注意 2.2.

1. l を素数とする．$l = s^4 + t^2$ となるような $s, t \in \mathbb{Z}$ が存在することを仮定すると，$P_{s,t} := (-s^2, st) \in E^{(l)}(\mathbb{Q})$ は位数無限大の有理点である．これは，l が平方因子を持たないことと [26, Proposition X.6.1 (a)] より，$E^{(l)}(\mathbb{Q})$ のねじれ部分群が
$$E^{(l)}(\mathbb{Q})_{\mathrm{tors}} = \langle (0,0) \rangle \simeq \mathbb{Z}/2\mathbb{Z}$$
であり，l は素数より $y_{P_{s,t}} = st \neq 0$ であることから従う．ここで，$y_{P_{s,t}}$ は $P_{s,t}$ の y 座標である．また，$l \equiv 9 \pmod{16}$（例えば，$t \equiv \pm 3 \pmod 8$）とすると，2 降下法（cf. [26, Proposition X.6.1, Proposition X.6.2]）により，$r(E^{(l)}) \leq 1$ となることを証明できる．従って，定理 2.1 の条件を満たす素数 l に対し，$r(E^{(l)}) = 1$ である．従って，あとは $\mathrm{ord}_p(h_{E^{(l)},p^n}) \geq 2n$ さえ示せば，定理 2.1 が従う．
2. Friedlander–Iwaniec の定理 [9] より，上記の 3 条件を満たす素数 l は無限個存在する．

注意 2.2 (2) を踏まえると，定理 1.7 は定理 2.1 から直ちに従うことが分かる．

$E^{(l)}$ は 2 と l の外で良い還元を持つので，Néron–Ogg–Shafarevich の判定法より，以下の系が従う：

命題 2.3. $n \geq 1$, $p \geq 5$ とし，l, l' を定理 2.1 の条件を満たす素数とする．このとき，$l \neq l'$ ならば，$K_{E^{(l)},p^n} \not\simeq K_{E^{(l')},p^n}$ である．

従って，今回構成した楕円曲線族の等分体を考えることで得られる代数体の族は, 互いに同型でない無数の代数体を含んでいる．

今回用いた Néron–Ogg–Shafarevich 判定法は，以下のような主張である：

定理 2.4 ([23])**.** v を素数，A を $\mathbb{Q}_v$ 上の Abel 多様体，$\mathcal{A}$ を A の $\mathbb{Z}_v$ 上の Néron モデル，$\mathcal{A}_v$ を $\mathcal{A}$ の special fiber，$\mathcal{A}_v^0$ を $\mathcal{A}_v$ の単位元を含む連結成分とする．このとき，以下は同値である：

1. A は良い還元を持つ．
2. v と互いに素な任意の $N \in \mathbb{Z}$ に対し，A の N 等分点のなす群 $A[N]$ は不分岐である．
3. $\gcd(N, v[\mathcal{A}_v : \mathcal{A}_v^0]) = 1$ かつ $A[N]$ が不分岐となるような $N \in \mathbb{Z}$ が存在する．

命題 *2.3* の証明. $\mathcal{E}$ を $E^{(l)}$ の $\mathbb{Z}_l$ 上の Néron モデル, $\mathcal{E}_l$ を $\mathcal{E}$ の special fiber，$\mathcal{E}_l^0$ を $\mathcal{E}_l$ の単位元を含む連結成分とする．$E^{(l)}$ の極小判別式は $2^6 l^3$ であり，$l \neq 2$ なので，[25, p. 365] の表より，E の還元型は Type III となる．従って $[\mathcal{E}_l : \mathcal{E}_l^0] = 2$ である． $E^{(l)}$ は l で悪い還元を持ち，$l \neq p$ なので，$\gcd(p^n, 2l) = 1$ である．従って，定理 2.4 (3) $\Rightarrow$ (1) より，$\mathbb{Q}(E^{(l)}[p^n])/\mathbb{Q}$ は l で分岐し，定理 2.4 (1) $\Rightarrow$ (2) より， $\mathbb{Q}(E^{(l)}[p^n])/\mathbb{Q}$ は 2,

l, p, ∞ の外で不分岐である．従って，$l \neq l'$ ならば， $K_{E^{(l)},p^n} \not\simeq K_{E^{(l')},p^n}$ である． □

以下では，定理 2.1 の証明の概略を述べる．定理 2.1 の証明の鍵は，臺信による以下の定理である．

定理 2.5 ([4])**.** p を素数，$n \in \mathbb{N}$, a, $b \in \mathbb{Q}$, $4a^3 + 27b^2 \neq 0$ とする．E を $y^2 = x^3 + ax + b$ で定義される p で極小な楕円曲線とし，以下の条件を仮定する．

(Add) $p \geq 5$.

(Mult) 任意の素数 l に対し，$\mathrm{ord}_l(j(E)) < 0$ ならば $p \nmid \mathrm{ord}_l(j(E))$ である．ここで，$j(E)$ は E の j 不変量である．

(Irr) $E[p]$ は既約 $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ 加群である．

(Res) $H^1(K_{E,p^n}/\mathbb{Q}, E[p^n]) = 0$.

(LG) $\mathrm{ord}_p(x_P) < 0$ かつ $\mathrm{ord}_p(x_P/y_P) \geq n+1$ となるような有理点 $P \in E(\mathbb{Q}) \setminus pE(\mathbb{Q})$ が存在する．ここで，x_P, y_P はそれぞれ P の x 座標，y 座標である．

このとき，$\mathrm{ord}_p(h_{E,p^n}) \geq 2n$ が成立する．

注意 2.6. 定理 2.5 の各条件の意味について説明する．

1. (Add) は，加法的かつ潜在的に良い還元を持つ素数での E の Selmer 群 $\mathrm{Sel}(\mathbb{Q}, E[p^n])$ の元の不分岐性に関する条件である．
2. (Mult) は，潜在的に乗法的還元を持つ素数での $\mathrm{Sel}(\mathbb{Q}, E[p^n])$ の元の不分岐性に関する条件である．
3. (Irr) は，大域的な法 p Galois 表現 $E[p]$ の既約性に他ならない．
4. (Res) は ，制限写像
$$H^1(\mathbb{Q}, E[p^n]) \xrightarrow{\mathrm{res}} H^1(K_{E,p^n}, E[p^n])^{\mathrm{Gal}(K_{E,p^n}/\mathbb{Q})} = \mathrm{Hom}_{\mathrm{Gal}(K_{E,p^n}/\mathbb{Q})}(\mathrm{Gal}(\overline{\mathbb{Q}}/K_{E,p^n}), E[p^n])$$
が単射であるという条件に他ならない．
5. (LG) は，大域的には「p で割れない」が局所的には「p^n で割り切れる」E の有理点の存在を導く．

注意 2.7. 臺信 [4] は $p = 3$ の場合も，追加の条件のもとで同様の結果を得ている．

定理 2.1 の証明の概略を説明する．定理 2.1 の通りに l, s, t を定め，$E_{s,t} := E^{(l)}$ とすると，これは
$$y^2 = x^3 - (s^4 + t^2)x$$
で定義される楕円曲線である．$E_{s,t}$ に対し，定理 2.5 の 5 つの条件は次のように確かめられる：

1. (Add) は定理の仮定 $p \geq 5$ に他ならない．
2. (Mult) は $j(E_{s,t}) = 1728 \in \mathbb{Z}$ より従う．
3. (Irr) は Dieulefait–González-Jiménez–Jiménez Urroz による (Irr) の判定法 [6, Theorem 7] より従う．
4. (Res) は $p \geq 5$ 及び (Irr) より従う．ここで，Lawson–Wuthrich による (Res) の判定法 [16, Theorem 2] を用いる．
5. (LG) は後述の命題 2.8 より従う．

命題 2.8 (Cf. [5, Theorem 3.1, Proposition 3.6])**.** p を奇素数，$n \in \mathbb{N}$, $P_{s,t} := (-s^2, st) \in E_{s,t}(\mathbb{Q})$ とし，以下を仮定する．

1. s と t は互いに素である．
2. $s^4 + t^2$ は 4 乗自由である．
3. $s \equiv 0 \pmod{p^{n+1}}$.

このとき，$P = 2P_{s,t}$ は定理 2.5 の条件 (LG) を満たす．

ここで，定理 2.1 の仮定を満たす s, t は命題 2.8 の 3 つの仮定を全て満たしていることに注意せよ．従って，あとは命題 2.8 さえ示せば，所望の定理 2.1 が従う．

命題 2.8 の証明の概略を述べる．

$P := 2P_{s,t}$ とおく．

まず，2 倍点公式より，

$$x_P = \left(\frac{2s^4 + t^2}{2st}\right)^2$$

であり，s と t は互いに素，p は奇素数かつ $s \equiv 0 \pmod{p^{n+1}}$ なので

$$\mathrm{ord}_p(x_P) = -2\,\mathrm{ord}_p(st) \leq -2(n+1) < 0$$

が従う．よって，

$$\mathrm{ord}_p(y_P) = \frac{1}{2}\,\mathrm{ord}_p(x_P^3 - (x^4 + t^2)x_P) = \frac{3}{2}\,\mathrm{ord}_p(x_P) = -3\,\mathrm{ord}_p(st) < 0$$

となる．以上より，

$$\mathrm{ord}_p(x_P/y_P) = \mathrm{ord}_p(st) \geq n + 1$$

が従う．

また，以下の主張より $P := 2P_{s,t} \notin pE_{s,t}(\mathbb{Q})$ が従う：

$P_{s,t} = mQ$ となる $m \geq 1$ と $Q \in E_{s,t}(\mathbb{Q})$ が存在するならば $m^2 = \hat{h}(P_{s,t})/\hat{h}(Q) < p^2$ である．

ここで，$P \in E(\mathbb{Q})$ に対し，$\hat{h}(P)$ は P の canonical height である．これは，Silverman による $\hat{h}(P_{s,t})$ の上界の評価 [24, Theorem 1.1] と Voutier–Yabuta による $y^2 = x^3 + ax$ 型の楕円曲線に対する $\hat{h}(Q)$ の下界の評価 [27, Theorem 1.2] から従う．

3　今後の課題

最後に，今後の課題を述べる．

本研究では，Mordell-Weil rank が 1 であり，p^n 等分体の類数が p^{2n} で割り切れる楕円曲線の無限族を構成した．我々の構成した楕円曲線の族はある条件を満たす $s^4 + t^2$ 型の素数でパラメトライズされているが，そのような素数の無限性は Friedlander–Iwaniec の定理により保証される．そこで，定理 1.7 をその他の 2 パラメータの素数でパラメトライズされた楕円曲線族に拡張することが今後の課題である．より具体的には，以下の問題について，現在調査中である．

$C^{(l)}$ を $y^3 = x^2 - 3lx$ で定義される楕円曲線とする．

著者達は，MAGMA による数値実験により，以下を予想した．

予想 3.1. l を $l \equiv 2 \pmod 3$ を満たす素数とすると，$\mathrm{rank}(C^{(l)}(\mathbb{Q})) = 1$ である．

予想 3.1 は一般 Riemann 予想のもとで $l < 1000$ に対して検証済みである．

$l = s^3 + 3t^3$ を $s \equiv 2 \pmod 3$ を満たす素数とすると，$C^{(l)}$ は位数無限大の有理点 $Q_{s,t} := (3s^3, -3st)$ を持ち，$\mathrm{rank}(C^{(l)}(\mathbb{Q})) \geq 1$ となる．$s^3 + 3t^3$ 型の素数の無限性は Heath-Brown–Moroz [11] により保証されている．$C^{(l)}$ の 3 ねじれ有理点は $(0,0)$, $(3l,0)$ のみであるので，$\mathrm{rank}(C^{(l)}(\mathbb{Q})) = 1$ を証明するためには，$C^{(l)}$ の 3-Selmer 群の $\mathbb{F}_3$-rank が 2 になることを証明すれば十分である．3 降下法 ([3]) を用いて $C^{(l)}$ の 3-Selmer 群の $\mathbb{F}_3$-rank が 2 になることを証明できるはずであり，本研究と同様に，楕円曲線上の加法定理や canonical height の評価を用いて (LG) を満たすような s と t の条件を見つけることで所望の楕円曲線の無限族の候補を得られると期待している．

謝辞

本稿の執筆及び講演の機会及び快適な Zoom 講演のサポートを頂いた世話人の山崎義徳先生，安福悠先生に深く感謝申し上げます．本稿の元となる論文 [5] の共著者の平川義之輔氏，臺信直人氏にも，貴重な共同研究の機会を頂いたことを，深く感謝いたします．また，本稿の執筆にあたり原稿に目を通して頂いた坂内健一先生，有益なコメントを頂いた平川氏，臺信氏，金村佳範氏に感謝いたします．本研究は日本学術振興会科研費 18H05233, 21J13502 及び 21K13779 の援助を受けたものです．また，本稿の執筆，並びに集会での講演は，国際共同利用・共同研究拠点である京都大学数理解析研究所の援助を受けたものです．

参考文献

[1] Manjul Bhargava and Arul Shankar, *Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves*, Ann. of Math. (2) **181** (2015), no. 1, 191–242, DOI 10.4007/annals.2015.181.1.3. MR3272925

[2] L. Carlitz, *Note on irregular primes*, Proc. Amer. Math. Soc. **5** (1954), 329–331, DOI 10.2307/2032249. MR61124

[3] Henri Cohen and Fabien Pazuki, *Elementary 3-descent with a 3-isogeny*, Acta Arith. **140** (2009), no. 4, 369–404, DOI 10.4064/aa140-4-6. MR2570111

[4] Naoto Dainobu, *Ideal class groups of division fields of elliptic curves and everywhere unramified rational points* (2023), available at `arXiv:2304.05035`.

[5] Naoto Dainobu, Yoshinosuke Hirakawa, and Hideki Matsumura, *Elliptic analogue of irregular prime numbers for the p^n-division fields of the curves $y^2 = x^3 - (s^4 + t^2)x$* (2022), available at `arXiv:2205.08946`.

[6] Luis Dieulefait, Enrique González-Jiménez, and Jorge Jiménez Urroz, *On fields of definition of torsion points of elliptic curves with complex multiplication*, Proc. Amer. Math. Soc. **139** (2011), no. 6, 1961–1969, DOI 10.1090/S0002-9939-2010-10621-4. MR2775372

[7] Reijo Ernvall, *Generalized Bernoulli numbers, generalized irregular primes, and class number*, Ann. Univ. Turku. Ser. A I **178** (1979), 72. MR533377

[8] ———, *Generalized irregular primes*, Mathematika **30** (1983), no. 1, 67–73, DOI 10.1112/S002557930001041X. MR720950

[9] John Friedlander and Henryk Iwaniec, *The polynomial $X^2 + Y^4$ captures its primes*, Ann. of Math. (2) **148** (1998), no. 3, 945–1040, DOI 10.2307/121034. MR1670065

[10] Dorian Goldfeld, *Conjectures on elliptic curves over quadratic fields*, Number theory, Carbondale 1979 (Proc. Southern Illinois Conf., Southern Illinois Univ., Carbondale, Ill., 1979), Lecture Notes in Math., vol. 751, Springer, Berlin, 1979, pp. 108–118. MR564926

[11] D. R. Heath-Brown and B. Z. Moroz, *On the representation of primes by cubic polynomials in two variables*, Proc. London Math. Soc. (3) **88** (2004), no. 2, 289–312, DOI 10.1112/S0024611503014497. MR2032509

[12] Toshiro Hiranouchi, *Local torsion primes and the class numbers associated to an elliptic curve over $\mathbb{Q}$*, Hiroshima Math. J. **49** (2019), no. 1, 117–127, DOI 10.32917/hmj/1554516039. MR3936649

[13] K. L. Jensen, *Om talteoretiske Egenskaber ved de Bernoulliske Tal*, Nyt Tidsskr. Mat. **B 26** (1915), no. 1, 73–83.

[14] Nicholas M. Katz and Peter Sarnak, *Zeroes of zeta functions and symmetry*, Bull. Amer. Math. Soc. (N.S.) **36** (1999), no. 1, 1–26, DOI 10.1090/S0273-0979-99-00766-1. MR1640151

[15] E. E. Kummer, *Allgemeiner Beweis des Fermatschen Satzes, daßdie Gleichung $x^\lambda + y^\lambda = z^\lambda$ durch ganze Zahlen unlösbar ist, für alle diejenigen Potenz-Exponenten λ welche ungerade Primzahlen sind und in den Zählern der ersten $1/2(\lambda)$ Bernoullischen zahlen als Factoren nicht vorkommen*, J. Reine Angew. Math. **40** (1850), 130–138, DOI 10.1515/crll.1850.40.130 (German). MR1578681

[16] Tyler Lawson and Christian Wuthrich, *Vanishing of some Galois cohomology groups for elliptic curves*, Elliptic curves, modular forms and Iwasawa theory, Springer Proc. Math. Stat., vol. 188, Springer, Cham, 2016, pp. 373–399, DOI 10.1007/978-3-319-45032-2_11. MR3629657

[17] Chao Li, *2-Selmer groups, 2-class groups and rational points on elliptic curves*, Trans. Amer. Math. Soc. **371** (2019), no. 7, 4631–4653, DOI 10.1090/tran/7373. MR3934463

[18] Tatsuya Ohshita, *Asymptotic lower bound of class numbers along a Galois representation*, J. Number Theory **211** (2020), 95–112, DOI 10.1016/j.jnt.2019.09.024. MR4074549

[19] Dipendra Prasad and Sudhanshu Shekhar, *Relating the Tate-Shafarevich group of an elliptic curve with the class group*, Pacific J. Math. **312** (2021), no. 1, 203–218, DOI 10.2140/pjm.2021.312.203. MR4298799

[20] Anwesh Ray and Tom Weston, *Class group statistics for torsion fields generated by elliptic curves* (2022), available at `https://arxiv.org/abs/2204.09757`.

[21] Fumio Sairaiji and Takuya Yamauchi, *On the class numbers of the fields of the p^n-torsion points of certain elliptic curves over $\mathbb{Q}$*, J. Number Theory **156** (2015), 277–289, DOI 10.1016/j.jnt.2015.04.004. MR3360340

[22] ———, *On the class numbers of the fields of the p^n-torsion points of elliptic curves over $\mathbb{Q}$*, J. Théor. Nombres Bordeaux **30** (2018), no. 3, 893–915 (English, with English and French summaries). MR3938633

[23] Jean-Pierre Serre and John Tate, *Good reduction of abelian varieties*, Ann. of Math. (2) **88** (1968), 492–517, DOI 10.2307/1970722. MR236190

[24] Joseph H. Silverman, *The difference between the Weil height and the canonical height on elliptic curves*, Math. Comp. **55** (1990), no. 192, 723–743, DOI 10.2307/2008444. MR1035944

[25] ———, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994. MR1312368

[26] ———, *The arithmetic of elliptic curves*, 2nd ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. MR2514094

[27] Paul Voutier and Minoru Yabuta, *Lang's conjecture and sharp height estimates for the elliptic curves* $y^2 = x^3 + ax$, Int. J. Number Theory **9** (2013), no. 5, 1141–1170, DOI 10.1142/S1793042113500176. MR3077706