楕円曲線に付随する L 関数の特殊値の代数的部分の p 進付値

(足立大雅氏 (九州大) と椎井亮太氏 (九州大) との共同研究による結果を含む)

都立大整数論セミナー

2025 年 4 月 18 日

株式会社光電製作所 野本 慶一郎

講演スライド

はじめに

KODEN 株式会社光電製作所

- 本講演では, 楕円曲線に付随する L 関数の特殊値の代数的部分の p 進付値に関する研究成果を二つ紹介する.
- 一つ目は, 素数 p をパラメータにもつ楕円曲線 $y^2 = x^3 + px$ の階数が 2 であることの必要十分条件が, 漸化式

$$f_{n+1}(t) = -12(t+1)(t+2)f_n'(t) + (4n+1)(2t+3)f_n(t) - 2n(2n-1)(t^2+3t+3)f_{n-1}(t)$$

を用いて与えられるという結果である. これは代数的部分の p 進付値が正となる条件を, 保型形式等を用いて書き換えることによって達成される.
- 二つ目は, 楕円曲線の 2 次ツイストで階数が 0 となる無限族を構成するという結果である. これは代数的部分の 2 進付値の下界及び等号成立条件を, Zhao's method という手法を用いて精密に調べることで達成される.
- まずは, 代数的部分の定義について説明を行う.

楕円曲線の階数

KODEN 株式会社光電製作所

- $\mathbb{Q}$ 上の楕円曲線とは，種数 1 の $\mathbb{Q}$ 上定義された非特異射影代数曲線 E で基点 $O \in E(\mathbb{Q})$ をもつものをいう．適切な変換により，以下の Weierstrass 方程式で表される．

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (a_1, a_2, a_3, a_4, a_6 \in \mathbb{Q})$$

- $\mathbb{Q}$ 有理点全体の集合 $E(\mathbb{Q})$ にはアーベル群の構造が入り，さらに有限生成であることが知られている (Mordell–Weil の定理):

$$E(\mathbb{Q}) \simeq \mathbb{Z}^{\oplus r} \oplus E(\mathbb{Q})_{\mathsf{tors}} \quad (E(\mathbb{Q})_{\mathsf{tors}} : \text{捻れ部分群})$$

- 一般に，$E(\mathbb{Q})$ の階数 $r = \operatorname{rank} E(\mathbb{Q})$ を計算することは難しく，具体的な楕円曲線に対してその階数を決定するだけでも整数論における大きな結果とされる．
- Birch and Swinnerton-Dyer (BSD) 予想は，階数が解析的に計算できることを主張する．

株式会社光電製作所

- 以下, $L(E/\mathbb{Q}, s)$ は $E/\mathbb{Q}$ に付随する Hasse–Weil L 関数を表す.

Conjecture (Birch and Swinnerton-Dyer 予想)

E を $\mathbb{Q}$ 上定義された楕円曲線とする. このとき, 以下を満たす定数 $c \neq 0$ が存在する:

$$L(E/\mathbb{Q}, s) = c(s-1)^{\mathrm{rank}\, E(\mathbb{Q})} + (\text{higher order terms}).$$

さらに, 定数 c は以下のように表される:

$$c = \frac{\Omega_E \cdot \prod_{\ell:\text{prime}} c_\ell \cdot \mathrm{Reg}(E) \cdot \#\text{Ш}(E/\mathbb{Q})}{\#E(\mathbb{Q})^2_{\mathrm{tors}}}.$$

ここで, Ω_E は周期, c_ℓ は素数 ℓ における局所玉河数, $\mathrm{Reg}(E)$ はレギュレータ, Ш$(E/\mathbb{Q})$ は Tate–Shafarevich 群である.

代数的部分の定義

- BSD 予想より, 以下の値

$$\frac{L(E/\mathbb{Q},1)}{\Omega_E}$$

は 0 または Tate–Shafarevich 群の位数等の数論的量で記述されることが期待される.

- 特に代数的数であることが予想されるため, このような値を $L(E/\mathbb{Q},1)$ の代数的部分と呼ぶ.

```
Elliptic Curve defined by y^2 + x*y = x^3 - 3*x + 1 over Rational Field

L(E/Q, 1)         = 0.749277221052284
Omega             = 2.24783166315685
L(E/Q, 1)/Omega = 0.333333333333333
```

代数的部分に関する remark

代数的部分の代数性

- いくつかの場合には, 代数的部分が実際に代数的数であることが示されている.
- 例えば, $\mathbb{Q}$ 上の楕円曲線に対しては Manin–Drinfeld により, 虚数乗法をもつ代数体上の楕円曲線に対しては Damerell により証明されている.

代数的部分の定め方

- 代数的部分は代数的数倍の違いを除いて定まる値である. 実際, 周期は楕円曲線のモデルに依存する量である. したがって, モデルの選び方及び代数的部分の定め方には注意しなければならない.
- しかし, 本講演では深入りしないことにする.

代数的部分の p 進付値と漸化式

対象とする楕円曲線

- ここでは, 素数 p をパラメータにもつ $\mathbb{Q}$ 上の楕円曲線

$$E_p : y^2 = x^3 + px$$

の階数 $\operatorname{rank} E_p(\mathbb{Q})$ を決定することを目標とする.

- 2-descent を用いることで, 以下の評価が得られる:

$$\operatorname{rank} E_p(\mathbb{Q}) \leq \operatorname{rank} E_p(\mathbb{Q}) + \dim_2 Ш(E_p/\mathbb{Q})[2] = \begin{cases} 0 & (p \equiv 7, 11 \bmod 16), \\ 1 & (p \equiv 3, 5, 13, 15 \bmod 16), \\ 2 & (p \equiv 1, 9 \bmod 16). \end{cases}$$

rank の候補

- ここで, $Ш(E_p/\mathbb{Q})$ の有限性を仮定すると, 2-parity 予想の帰結として以下を得る:

$$(-1)^{\mathrm{rank}\, E_p(\mathbb{Q})} = \varepsilon(E_p/\mathbb{Q}) = \begin{cases} +1 & p \equiv 1, 7, 9, 11 \bmod 16, \\ -1 & p \equiv 3, 5, 13, 15 \bmod 16 \end{cases}$$

- したがって $Ш(E_p/\mathbb{Q})$ の有限性の下で以下の等式を得る.

$$\mathrm{rank}\, E_p(\mathbb{Q}) = \begin{cases} 0 & (p \equiv 7, 11 \bmod 16), \\ 1 & (p \equiv 3, 5, 13, 15 \bmod 16), \\ 0, 2 & (p \equiv 1, 9 \bmod 16). \end{cases}$$

- よって, $p \equiv 1, 9 \bmod 16$ の場合の階数の決定が問題となる.

代数的部分の p 進付値を調べる必要性

- 以下, $p \equiv 1, 9 \bmod 16$ を仮定する.
- $L(E_p/\mathbb{Q}, 1)$ の代数的部分を次のようにおく:

$$S_p := \frac{\#E_p(\mathbb{Q})_{\mathrm{tors}}^2 \cdot L(E_p/\mathbb{Q}, 1)}{\Omega_{E_p} \cdot \prod_\ell c_\ell} = \frac{\Gamma(1/4)^2}{\pi^{1/2} p^{1/4}} L(E_p/\mathbb{Q}, 1) \in \mathbb{Q}.$$

- 代数的部分 S_p は, 0 または $\text{Ш}(E_p/\mathbb{Q})$ の位数と予想されている量である.
- このとき BSD 予想を仮定すれば以下が成り立つ.

$$S_p = 0 \iff L(E_p/\mathbb{Q}, 1) = 0 \iff \operatorname{rank} E_p(\mathbb{Q}) \neq 0 \ (= 2).$$

代数的部分の整数性

- さらに, $L(E_p/\mathbb{Q},1)$ の不等式評価をすることで $S_p < p$ であることが分かる.
- したがって, $S_p \in \mathbb{Z}$ であることが示せれば以下の同値が成り立つ.

$$S_p \equiv 0 \bmod p \iff S_p = 0 \iff L(E_p/\mathbb{Q},1) = 0 \overset{\text{BSD}}{\iff} \operatorname{rank} E_p(\mathbb{Q}) \neq 0 \ (= 2).$$

Remark

- 実際に $S_p \in \mathbb{Z}$ であることを示すには様々な方法があるが, 例えば全ての素数 q について q 進付値 $v_q(S_p)$ が非負であることを証明する, という手法を取ることができる.
- この手法には, 本講演の後半で触れる Zhao's method という手法が有効である.

KODEN 株式会社光電製作所

- S_p が p の倍数であること，すなわち p 進付値が正であることを簡単な漸化式で表現した．

Theorem (N., 2022[1])

$p \equiv 1, 9 \bmod 16$ とする．このとき $E_p : y^2 = x^3 + px$ に対する BSD 予想の下で

$$\operatorname{rank} E_p(\mathbb{Q}) = 2 \iff f_{3(p-1)/8}(0) \equiv 0 \bmod p$$

が成り立つ．ここで，$f_n(t) \in \mathbb{Z}[t]$ は以下の漸化式により定まる多項式である．

$$f_{n+1}(t) = -12(t+1)(t+2)f_n'(t) + (4n+1)(2t+3)f_n(t) - 2n(2n-1)(t^2+3t+3)f_{n-1}(t)$$

ただし，初期値は $f_0(t) = 1, f_1(t) = 2t + 3$ である．

[1] K. Nomoto. “The rank of a CM elliptic curve and a recurrence formula”. In: *Journal of Number Theory* 238 (2022), pp. 60–81.

数値例

表：多項式 $f_0(t), \ldots, f_9(t)$

n	$f_n(t)$
0	1
1	$2t + 3$
2	$-6t^2 - 18t - 9$
3	$12t^3 + 54t^2 + 108t + 81$
4	$60t^4 + 360t^3 + 1296t^2 + 2268t + 1377$
5	$-1512t^5 - 11340t^4 - 30456t^3 - 34992t^2 - 13122t + 2187$
6	$21816t^6 + 196344t^5 + 687204t^4 + 1178064t^3 + 1027890t^2 + 433026t + 80919$
7	$-280368t^7 - 2943864t^6 - 13273632t^5 - 33315300t^4 - 50473044t^3 - \cdots - 5189751$
8	$3319056t^8 + 39828672t^7 + 209221056t^6 + 628386336t^5 + \cdots + 82097793$
9	$-32283360t^9 - 435825360t^8 - 2479253184t^7 - 7727493312t^6 - \cdots + 1702205523$

数値例

表：定数項が p の倍数かどうか

p	$p \mid f_{3(p-1)/8}(0)$	p	$p \mid f_{3(p-1)/8}(0)$	p	$p \mid f_{3(p-1)/8}(0)$
17		257		521	
41		281	○	569	
73	○	313		577	
89	○	337	○	593	○
97		353	○	601	○
113	○	401		617	○
137		409		641	
193		433		673	
233	○	449		761	
241		457		769	

KODEN 株式会社光電製作所

- 本結果は, Villegas–Zagier による「素数 p に対する三乗和問題」についての結果に基づく.
- この問題は, 素数 p が有理数の三乗和で表せるか, すなわち $\mathbb{Q}$ 上の楕円曲線 $A_p : x^3 + y^3 = p$ が非自明な $\mathbb{Q}$ 有理点をもつかという問いであり, 彼らは以下の結果を残している.

Theorem (Rodríguez-Villegas–Zagier, 1995[2])

$p \equiv 1 \bmod 9$ と仮定する. このとき A_p に対する BSD 予想の下で

$$\mathrm{rank}\, A_p(\mathbb{Q}) = 2 \iff p \mid a_{(p-1)/3}(0).$$

が成り立つ. ただし, $a_n(t) \in \mathbb{Z}[t]$ は以下の漸化式で定まる多項式である $(a_0(t) = 1, a_1(t) = -3t^2)$.

$$a_{n+1}(t) = -(1 - 8t^3)a_n'(t) - (16n + 3)t^2 a_n(t) - 4n(2n - 1)t a_{n-1}(t).$$

[2] F. Rodríguez-Villegas and D. Zagier. "Which primes are sums of two cubes?" In: 15 (1995), pp. 295–306.

■ 彼らの証明は一部非自明な箇所があり，自身で結果の再現を試みたところ，彼らの得た漸化式と異なるものを得た．

Theorem (N., 2022[3])

$p \equiv 1 \bmod 9$ と仮定する．このとき A_p に対する BSD 予想の下で

$$\mathrm{rank}\, A_p(\mathbb{Q}) = 2 \iff p \mid x_{(p-1)/3}(0).$$

が成り立つ．ただし，$x_n(t) \in \mathbb{Z}[t]$ は以下の漸化式で定まる多項式である $(x_0(t) = 1, x_1(t) = 0)$.

$$x_{n+1}(t) = -2(1-8t^3)x_n'(t) - 8nt^2x_n(t) - n(2n-1)tx_{n-1}(t).$$

[3] Nomoto, “The rank of a CM elliptic curve and a recurrence formula”.

表：$a_n(t)$ と $x_n(t)$ の比較

n	$a_n(t)$	$x_n(t)$
0	1	1
1	$-3t^2$	0
2	$9t^4 + 2t$	$-t$
3	$-27t^6 - 18t^3 - 2$	2
4	$81t^8 + 108t^5 + 36t^2$	$-33t^2$
5	$-243t^{10} - 540t^7 - 360t^4 + 152t$	$76t$
6	$729t^{12} + 2430t^9 + 2700t^6 - 16440t^3 - 152$	$-339t^3 - 152$
7	$-2187t^{14} + 10206t^{11} - 17010t^8 + 1311840t^5 + 24240t^2$	$4314t^2$
8	$6561t^{16} + 40824t^{13} + \cdots - 99234720t^7 - 2974800t^4 + 6848t$	$-72687t^4 - 3424t$
9	$-19683t^{18} - 157464t^{15} - 489888t^{12} + \cdots - 578304t^3 - 6848$	$228168t^3 + 6848$

証明の概要

$$
\begin{tikzcd}[column sep=huge]
\operatorname{rank} E_p(\mathbb{Q}) = 2 \arrow[d, Leftrightarrow, "\text{BSD}"'] & \\
L(E_p/\mathbb{Q}, 1) = 0 \arrow[d, Leftrightarrow] & L(\psi^{2k-1}, k) = 0 \quad (\exists\, k \in \mathbb{Z}) \arrow[d, Leftrightarrow] \\
S_p = 0 \arrow[d, Leftrightarrow] & L_k = 0 \arrow[d, Rightarrow] \\
S_p \equiv 0 \bmod p \arrow[r, leftrightarrow, "p\text{ 進 }L\text{ 関数の補間公式による}", "\text{代数的部分の合同式}"'] & L_k \equiv 0 \bmod p \arrow[d, Leftrightarrow, "\text{代数的部分の微分値表示}"] \\
 & f_{3(p-1)/8}(0) \equiv 0 \bmod p
\end{tikzcd}
$$

p 進 L 関数の補間公式による代数的部分の合同式

KODEN 株式会社光電製作所

■ S_p が p の倍数であることと L_k が p の倍数であることの同値性は, 以下の命題から得られる.

Propisition

$$S_p \equiv \pm \left(\frac{p-1}{4}\right)!^2 2^{4k-5} 3^{3k-3} L_k \bmod p.$$

(証明の概要)

E_p は ($\mathbb{Z}[i]$ により) 虚数乗法をもつので, $L(E_p/\mathbb{Q}, s)$ はある Hecke L 関数で表示できる.
具体的には, E_1 に付随する Hecke 指標 ψ とある 4 次指標 χ_p が存在して以下が成り立つ.

$$L(E_p/\mathbb{Q}, s) = L(\psi\chi_p, s)$$

この 4 次指標 χ_p は, $\mathbb{Z}[i]$ のイデアル $\mathfrak{a} = (\alpha)$ $((\mathfrak{a}, 4p) = 1)$ に対して以下を満たす:

$$\chi_p(\mathfrak{a}) \equiv \left(\frac{\alpha}{\overline{\alpha}}\right)^{k-1} \bmod p \quad (k-1 = 3(p-1)/4)$$

KODEN 株式会社光電製作所

(証明の概要続き)

このとき, 別の Hecke L 関数の特殊値 $L(\psi^{2k-1}, k)$, 及びその代数的部分 L_k を考えると, 図のようにして以下の性質が成り立つことが分かる.

1. S_p と L_k を補間するような p 進 L 関数が存在すること
2. その間に mod p の合同式が存在すること

$$
\begin{tikzcd}
L(\psi\chi_p,1) = \displaystyle\sum_{(\mathfrak{a},4p)=1} \chi_p(\mathfrak{a}) \frac{1}{\overline{\psi}(\mathfrak{a}) N\mathfrak{a}^s}\Bigg|_{s=0} \arrow[d, dashed, "\text{代数的部分}"] & \displaystyle\sum_{(\mathfrak{a},4)=1} \left(\frac{\alpha}{\overline{\alpha}}\right)^{k-1} \frac{1}{\overline{\psi}(\alpha) N\mathfrak{a}^s}\Bigg|_{s=0} = L(\psi^{2k-1},k) \arrow[d, dashed, "\text{代数的部分}"'] \\
S_p \arrow[r, leftrightarrow, "\text{mod } p \text{ 関係式}"] & L_k
\end{tikzcd}
$$

主張の合同式は, p 進 L 関数の補間公式を具体的に書き下すことによって得られる.

代数的部分 L_k の微分値表示

KODEN
株式会社光電製作所

■ $L(\psi^{2k-1}, k)$ の代数的部分 L_k を漸化式で表示するためには以下の公式を必要とする.

Propisition (N., 2022[4])

$\theta_2(z) := \sum_{n\in\mathbb{Z}+1/2} e^{\pi i n^2 z}$ とおくと以下が成り立つ:

$$L(\psi^{2k-1}, k) = \begin{cases} \dfrac{2^{3k-9/2}\pi^k}{(k-1)!}\left|\partial_{1/2}^{(N)}\theta_2(z)|_{z=i}\right|^2 & (k = 2N+1) \\ 0 & (k = 2N) \end{cases}$$

微分作用素	保型性	正則性
Maass–Shimura operator ∂_k	保つ	保たない
Ramanujan–Serre operator ϑ_k	保つ	保つ

[4] Nomoto, "The rank of a CM elliptic curve and a recurrence formula".

代数的部分 L_k の微分値表示

KODEN 株式会社光電製作所

- ∂_k-微分値を ϑ_k-微分値に変更するため, Modified Cohen–Kuznetsov 級数を利用する.

$$f_\partial(z,X) := \sum_{n=0}^{\infty} \frac{\partial_k^{(n)} f(z)}{(k)_n} \frac{X^n}{n!} \quad (z \in \mathbb{H}, X \in \mathbb{C}, f \in M_k(\Gamma))$$

$$f_\vartheta(z,X) := e^{-E_2^*(z)X/12} f_\partial(z,X) = \sum_{n=0}^{\infty} \frac{F_n(z)}{(k)_n} \frac{X^n}{n!}$$

- ポイントは $E_2^*(i) = 0$ を満たすことである. このことから $\partial_k^{(n)} f(z)|_{z=i} = F_n(i)$ となる:

Propisition (Rodríguez-Villegas–Zagier, 1993[5])

$f \in M_k(\Gamma)$ に対して, $F_n \in M_{k+2n}(\Gamma)$ は以下の漸化式を満たす ($F_0 = f, F_1 = \vartheta_k f$).

$$F_{n+1} = \vartheta_{k+2n} F_n - \frac{n(n+k-1)}{144} E_4 F_{n-1}.$$

[5] F. Rodríguez-Villegas and D. Zagier. "Square roots of central values of Hecke L-series". In: (1993), pp. 81–89.

代数的部分の 2 進付値と Zhao’s method

代数的部分の p 進付値を調べるもう一つの理由

- 講演の前半では, 代数的部分が 0 であるかどうか調べるためにその p 進付値を調べた.
  しかし, 代数的部分の p 進付値を調べる意義は他にも存在する.

Conjecture (p 部分 BSD 予想 (rank 0 case))

E を $\mathbb{Q}$ 上定義された楕円曲線とする. このとき $L(E/\mathbb{Q},1) \neq 0$ ならば以下が成り立つ:

$$v_p\left(\frac{L(E/\mathbb{Q},1)}{\Omega_E}\right) = \sum_{\ell:\mathrm{prime}} v_p(c_\ell) + v_p(\#Ш(E/\mathbb{Q})) - 2v_p(\#E(\mathbb{Q})_{\mathrm{tors}})$$

- p 部分 BSD 予想に対しては, 岩澤理論的アプローチを取るのが主流であるが,
  小さな素数 (e.g. $p = 2, 3$) は例外として扱われることがほとんどである.

- したがって, 本研究では代数的部分の 2 進付値を別手法で調べる.

本研究で扱う楕円曲線とその理由

- 本研究では, $\mathbb{Q}$ 上の楕円曲線 E の二次ツイストに対する代数的部分の 2 進付値を調べる.
- 二次ツイストを対象とする理由としては, 例えば Goldfeld 予想がある.

Conjecture (Goldfeld 予想)

square-free な整数 d に対して, $\mathbb{Q}(\sqrt{d})$ に付随する E の二次ツイストを $E^{(d)}$ と書く.
このとき以下が成り立つ:

$$\mathrm{density}(d) = \begin{cases} 1/2 & (\mathrm{rank}\, E^{(d)}(\mathbb{Q}) = 0), \\ 1/2 & (\mathrm{rank}\, E^{(d)}(\mathbb{Q}) = 1), \\ 0 & (\text{otherwise}). \end{cases}$$

- rank が 0 になる d の条件, つまり代数的部分が 0 にならない条件を調べることが必要となる.
  したがって, 代数的部分の p 進付値が有限かどうか決定することも重要な課題である.

計算対象を Hasse–Weil L 関数から保型 L 関数へ

保型形式との対応

- N を E の導手とするとき, E の $\mathbb{Q}$ 同種類には, ある $\mathbb{Q}$ 上の正規化 Hecke 固有形式 $f = \sum a_n q^n \in S_2(\Gamma_0(N))^{\mathrm{new}}$ が対応する:

$$L(E/\mathbb{Q}, s) = L(f, s).$$

二次ツイストとの関係

- m を $(m, N) = 1$ を満たす square-free な正の奇数, $\varepsilon \in \{\pm 1\}$ とする．このとき

$$L(E^{(\varepsilon m)}/\mathbb{Q}, s) = L(f, \chi_M, s)$$

が成り立つ．ここで, χ_M は原始的な二次 Dirichlet 指標であり, その導手 M は次で与えられる.

$$M = \begin{cases} m & (\varepsilon m \equiv 1 \bmod 4), \\ 4m & (\varepsilon m \equiv 3 \bmod 4). \end{cases}$$

保型 L 関数の特殊値の代数的部分を定義する

- Hecke 固有形式 $f \in S_2(\Gamma_0(N))^{\mathrm{new}}$ の周期格子 $\mathcal{L}_f$ を次のように定める.

$$\mathcal{L}_f := \left\{ \int_\gamma f(q)\frac{dq}{q} \,\middle|\, \gamma \in H_1(X_0(N)(\mathbb{C}), \mathbb{Z}) \right\} \subset \mathbb{C}.$$

- $\mathcal{L}_f$ に含まれる最小の正の実数を Ω_f^+, 虚部が最小の純虚数を Ω_f^- とおく.
  このとき適切な仮定の下で周期格子は以下のような表示をもつ.

$$\mathcal{L}_f = \Omega_f^+\mathbb{Z} + \Omega_f^-\mathbb{Z} \quad \text{または} \quad \mathcal{L}_f = \Omega_f^+\mathbb{Z} + \frac{\Omega_f^+ + \Omega_f^-}{2}\mathbb{Z}.$$

Theorem (Drinfeld–Manin)

$$\frac{L(f, \chi_M, 1)}{\Omega_f^{\mathrm{sgn}(\chi_M)}} \in \overline{\mathbb{Q}}.$$

KODEN 株式会社光電製作所

■ $M = 4^n m = 4^n q_1 \cdots q_r$ $(n \in \{0,1\}, q_i$: 異なる奇素数$)$ と書く．このとき以下のようにおく．

$$\mathfrak{v}_m := \min\{v_2(a_{q_1}-2), \ldots, v_2(a_{q_r}-2)\}, \quad \mathcal{S}_i := \{q : \text{奇素数} \mid q \nmid N, v_2(a_q - 2) = i\}.$$

Theorem (N–Adachi–Shii, 2023[6])

素因数の個数 r に依らない定数 c が存在して，全ての i に対して $q_i \in \mathcal{S}_0 \cup \mathcal{S}_1 \cup \mathcal{S}_2$ ならば

$$v_2\left(\frac{L(f,\chi_M,1)}{\Omega_f^{\mathrm{sgn}(\chi_M)}}\right) \geq \mathfrak{v}_m \cdot r + c.$$

さらに，無限個の M に対して等号が成立する．したがってそのような M に対して $E^{(\varepsilon m)}(\mathbb{Q})$, $Ш(E^{(\varepsilon m)}/\mathbb{Q})$ はいずれも有限群である．

(※) 定数 c は explicit に記述できる．さらに等号成立条件が explicit に記述できる場合もある．

[6] T. Adachi, K. Nomoto, and R. Shii. *The 2-adic valuations of the algebraic central L-values for quadratic twists of weight 2 newforms*. 2024. URL: https://arxiv.org/abs/2403.11474.

- 先行研究[7][8][9][10][11]では全て $\varepsilon m \equiv 1 \bmod 4$ の場合しか扱っておらず, $\varepsilon m \equiv 3 \bmod 4$ の場合に計算されている例は知られていない.
- $\varepsilon m \equiv 1 \bmod 4$ の場合でも, より sharp な下界や緩い等号成立条件を与えている場合がある.

[7] S. Zhai. "Non-vanishing theorems for quadratic twists of elliptic curves". In: *Asian Journal of Mathematics* 20.3 (2016), pp. 475–502.
[8] S. Zhai. "On the weak forms of the 2-part of Birch and Swinnerton-Dyer conjecture". In: *Mathematical Proceedings of the Cambridge Philosophical Society* 168.1 (2020), pp. 197–209.
[9] L. Cai, C. Li, and S. Zhai. "On the 2-part of the Birch and Swinnerton-Dyer conjecture for quadratic twists of elliptic curves". In: *Journal of the London Mathematical Society (2)* 101.2 (2020), pp. 714–734.
[10] S. Zhai. "A lower bound result for the central L-values of elliptic curves". In: *Journal of Number Theory* 207 (2020), pp. 356–366.
[11] S. Zhai. *The Birch–Swinnerton-Dyer exact formula for quadratic twists of elliptic curves*. 2021. URL: https://arxiv.org/abs/2102.11798.

等号成立の具体例

KODEN 株式会社光電製作所

- $\varepsilon = +1$ とする．また，$f \in S_2(\Gamma_0(34))$ を以下の Fourier 級数をもつ固有形式とする:
$$f = q + q^2 - 2q^3 + q^4 - 2q^6 - 4q^7 + q^8 + q^9 + O(q^{10})$$
- この f に対応する楕円曲線は $E_f : y^2 + y = x^3 - 3x + 1$ (Cremona label: 34a1) である．
- $m = q_1 \cdots q_r$ に対して，$q_i \in \mathcal{S}_0 \cup \mathcal{S}_1 \cup \mathcal{S}_2$ かつ $\mathrm{sgn}(\chi_{q_i}) = +1$ $(\forall i)$ ならば
$$v_2\left(\frac{L(f, \chi_m, 1)}{\Omega_f^{\mathrm{sgn}(\chi_m)}}\right) \geq \mathfrak{v}_m \cdot r + \min\left\{1 + \delta_{\mathfrak{v}_m, 0}, v_2\left(\frac{L(f,1)}{\Omega_f^+}\right)\right\}.$$
- さらに，$q_i \in \mathcal{S}_1$ $(\forall i)$ が成り立つとき等号が成立する．つまり
$$q_i \equiv 1 \bmod 4, \quad a_{q_i} \equiv 0 \bmod 4$$
が成り立つとき代数的部分の 2 進付値はちょうど r となる (e.g. $q_i = 5$).
- Chebotarev の密度定理よりそのような素数 q_i は無限個存在する．

等号成立の具体例

[5, 29, 37, 61, 109, 173, 181, 197, 269, 277, 317, 397, 541, 653, 677, 709, 821, 853, 877, 941, 997, 1013, 1061, 1093, 1117, 1213, 1229, 1493, 1621, 1637, 1669, 1693, 1741, 1877, 1901, 1933, 1949, 2029, 2069, 2213, 2221, 2237, 2309, 2341, 2357, 2437, 2477, 2557, 2621, 2693, 2749, 2861, 2917, 3037, 3253, 3301, 3373, 3389, 3461, 3533, 3541, 3581, 3677, 3701, 3709, 3733, 3797, 3853, 3917, 3989, 4253, 4261, 4349, 4357, 4397, 4493, 4517, 4549, 4597, 4621, 4733, 4789, 4933, 4957, 5021, 5077, 5197, 5309, 5333, 5413, 5437, 5477, 5501, 5573, 5581, 5701, 5717, 5741, 5749, 5821, 5981, 6029, 6229, 6301, 6317, 6389, 6397, 6421, 6637, 6653, 6661, 6701, 6709, 6829, 6997, 7069, 7109, 7213, 7237, 7253, 7333, 7349, 7477, 7517, 7541, 7589, 7621, 7741, 7757, 7789, 7877, 7933, 7949, 8053, 8069, 8221, 8269, 8293, 8429, 8461, 8573, 8597, 8629, 8677, 8693, 8741, 8837, 9013, 9109, 9157, 9173, 9221, 9277, 9293, 9413, 9421, 9629, 9661, 9781, 9829, 9901, 9973, 10037, 10061, 10069, 10093, 10333, 10477, 10501, 10597, 10613, 10733, 10781, 10789, 10853, 10909, 11149, 11197, 11213, 11261, 11317, 11549, 11597, 11621, 11701, 11821, 11941, 12101, 12109, 12149, 12269, 12277, 12301, 12373, 12413, 12421, 12437, 12517, 12541, 12637, 12653, 12757, 12781, 12821, 12829, 12893, 12917, 13093, 13229, 13469, 13597, 13709, 13781, 13877, 13901, 13933, 13997, 14149, 14173, 14341, 14389, 14461, 14549, 14557, 14717, 14797, 14813, 14821, 14869, 14957, 15101, 15269, 15277, 15373, 15413, 15493, 15541, 15629, 15749, 15773, 15901, 15973, 16189, 16229, 16349, 16381, 16453, 16493, 16901, 17029, 17317, 17333, 17573, 17581, 17669, 17789, 17957, 17981, 17989, 18013, 18061, 18077, 18133, 18149, 18229, 18253, 18269, 18397, 18493, 18541, 18637, 18661, 18757, 18773, 18797, 19013, 19037, 19069, 19181, 19213, 19237, 19301, 19309, 19373, 19421, 19477, 19709, 19717, 19853, 19861, 19997, 20021, 20029, 20101, 20117, 20173, 20261, 20269, 20389, 20509, 20533, 20717, 20981, 21221, 21277, 21341, 21397, 21493, 21517, 21613, 21661, 21757, 21821, 21893, 22037, 22093, 22157, 22229, 22277, 22349, 22469, 22501, 22549, 22573, 22613, 22621, 22637, 22709, 22717, 22741, 22853, 22877, 22973, 23021, 23029, 23117, 23293, 23557, 23669, 23773, 23789, 23909, 23981, 24061, 24077, 24109, 24133, 24181, 24197, 24317, 24373, 24469, 24509, 24517, 24677, 24749, 24781, 24877, 24917, 25013, 25189, 25301, 25357, 25469, 25541, 25693, 25733, 25741, 25981, 26021, 26141, 26237, 26293, 26309, 26357, 26557, 26693, 26701, 26717, 26821, 27061, 27109, 27197, 27397, 27509, 27581, 27653, 27733, 27749, 27773, 27917, 27941, 28181, 28277, 28349, 28429, 28549, 28597, 28621, 28669, 28837, 29077, 29101, 29269, 29437, 29501, 29573, 29789, 29917]

等号成立の具体例

■ そのような素数を任意個取り，それらを掛け合わせた整数を $m = q_1 \cdots q_r$ としたとき，以下が成り立つ．

- $$v_2\left(\frac{L(f,\chi_m,1)}{\Omega_f^+}\right) = v_2\left(\frac{L(E^{(m)}/\mathbb{Q},1)}{\Omega_E^+}\right) = r,$$
- $\operatorname{rank} E^{(m)}(\mathbb{Q}) = 0,$
- $\#Ш(E^{(m)}/\mathbb{Q}) < \infty.$

```
【m = 5】
L(E^(m)/Q, 1)                  = 2.01052176031805
L(E^(m)/Q, 1)/Omega            = 0.894427190999916
L(E^(m)/Q, 1)*sqrt(m)/Omega = 2.00000000000000

【m = 5 * 29】
L(E^(m)/Q, 1)                  = 2.24006710916749
L(E^(m)/Q, 1)/Omega            = 0.996545758244879
L(E^(m)/Q, 1)*sqrt(m)/Omega = 12.0000000000000

【m = 5 * 29 * 37】
L(E^(m)/Q, 1)                  = 0.245509842828783
L(E^(m)/Q, 1)/Omega            = 0.109220742305938
L(E^(m)/Q, 1)*sqrt(m)/Omega = 8.00000000000000

【m = 5 * 29 * 37 * 61】
L(E^(m)/Q, 1)                  = 1.69745297050511
L(E^(m)/Q, 1)/Omega            = 0.755151285715589
L(E^(m)/Q, 1)*sqrt(m)/Omega = 432.000000000000
```

KODEN 株式会社光電製作所

- $r \in \mathbb{P}^1(\mathbb{Q})$ に対して

$$\langle r \rangle := \langle r \rangle_f := 2\pi i \int_{i\infty}^{r} f(z)dz$$

とおき, modular symbol と呼ぶ.

Propisition

$\tau(\chi_M) = \sum \chi_M(a) e^{2\pi i a/M}$ を Gauss 和とする. このとき以下が成り立つ.

$$\tau(\chi_M) \frac{L(f, \chi_M, 1)}{\Omega_f^{\mathrm{sgn}(\chi_M)}} = \sum_{k \in (\mathbb{Z}/M\mathbb{Z})^\times} \chi_M(k) \frac{1}{\Omega_f^{\mathrm{sgn}(\chi_M)}} \left\langle \frac{k}{M} \right\rangle$$

証明の概要の前に：先行研究との違い

KODEN 株式会社光電製作所

- $\langle r\rangle^+ := \mathrm{Re}\langle r\rangle, \langle r\rangle^- := \mathrm{Im}\langle r\rangle$ とおく．このとき $\langle r\rangle^\pm/\Omega_f^\pm$ は代数的数となる．(複号同順)
- さらに次が成り立つ．

$$\sum_{k\in(\mathbb{Z}/M\mathbb{Z})^\times} \chi_M(k)\frac{1}{\Omega_f^{\mathrm{sgn}(\chi_M)}}\left\langle \frac{k}{M}\right\rangle = \sum_{k\in(\mathbb{Z}/M\mathbb{Z})^\times} \chi_M(k)\frac{1}{\Omega_f^{\mathrm{sgn}(\chi_M)}}\left\langle \frac{k}{M}\right\rangle^{\mathrm{sgn}(\chi_M)}$$

左辺：各項が代数的とは限らず
評価できる対象が限られる

右辺：各項が代数的であり
より幅広く精密な評価が可能

証明の概要: Zhao's method

■ 約数の個数に関する帰納法を利用して, 代数的部分の p 進付値を評価・決定する手法.

$$\tau(\chi_M)\frac{L(f,\chi_M,1)}{\Omega_f^{\mathrm{sgn}(\chi_M)}} = \sum_{k\in(\mathbb{Z}/M\mathbb{Z})^\times} \chi_M(k)\frac{1}{\Omega_f^{\mathrm{sgn}(\chi_M)}}\left\langle \frac{k}{M}\right\rangle^{\mathrm{sgn}(\chi_M)} =: \mathcal{T}_M$$

② 本質的に D に対する
代数的部分になっている ↓

↓ ① 計算しやすい右辺を
M の約数 D を用いて微修正

$$\sum_{q\mid\frac{M}{D}}(a_q-2\chi_D(q))\times\tau(\chi_D)\frac{L(f,\chi_D,1)}{\Omega_f^{\mathrm{sgn}(\chi_D)}} = \sum_{k\in(\mathbb{Z}/M\mathbb{Z})^\times} \chi_D(k)\frac{1}{\Omega_f^{\mathrm{sgn}(\chi_D)}}\left\langle \frac{k}{M}\right\rangle^{\mathrm{sgn}(\chi_D)} =: \mathcal{T}_{D,M}$$

証明の概要: Zhao's method

- 約数の個数に関する帰納法を利用して, 代数的部分の p 進付値を評価・決定する手法.

和を取ることで容易に
2 進付値の評価が可能

本質的に $\dfrac{L(f,\chi_D,1)}{\Omega_f^{\mathrm{sgn}(\chi_D)}}$ に等しく,
帰納法の仮定を使用可能

$$\sum_{D|M} \mathcal{T}_{D,M} = \mathcal{T}_{1,M} + \sum_{\substack{D|M \\ D\neq 1,M}} \mathcal{T}_{D,M} + \mathcal{T}_M$$

本質的に $\dfrac{L(f,1)}{\Omega_f^{+}}$ に等しい

本質的に $\dfrac{L(f,\chi_M,1)}{\Omega_f^{\mathrm{sgn}(\chi_M)}}$ に等しい

まとめ

結果 1: 代数的部分の p 進付値と漸化式

- 楕円曲線 $y^2 = x^3 + px$ の階数が 2 であることの必要十分条件を, 漸化式

$$f_{n+1}(t) = -12(t+1)(t+2)f_n'(t) + (4n+1)(2t+3)f_n(t) - 2n(2n-1)(t^2+3t+3)f_{n-1}(t)$$

  により定まる多項式の定数項 $f_{3(p-1)/8}(0)$ が p の倍数であることとして与えた.
- その証明は, 代数的部分の p 進付値が正となる条件を, 別の特殊値 $L(\psi^{2k-1}, k)$ の代数的部分の p 進付値の条件に置き換えることによって達成される.

結果 2: 代数的部分の 2 進付値と Zhao's method

- 楕円曲線の二次ツイストに対する代数的部分の 2 進付値の下界を与えた. 特にいくつかの場合には等号成立条件を与えた. 結果として, 階数が 0 となる二次ツイストの無限族を構成した.
- その証明は, Zhao's method(約数の個数に関する帰納法による評価手法) によって達成される.