漸化式を用いた楕円曲線の階数の判定法について

九州大学 大学院 数理学府 博士後期課程2年 **野本 慶一郎**

E-mail: nomoto.keiichiro.635@s.kyushu-u.ac.jp

異分野・異業種研究交流会2021

2021年11月13日(土)

【研究の動機】 楕円曲線とは, $y^2 = x^3 + ax + b$という方程式で定義される曲線の一種で, 暗号理論への応用等, 様々な分野で用いられる対象である. 楕円曲線に対して, 階数という整数論的に重要な量が定まる. これは楕円曲線の有理点の個数を記述する量であるが, 一般に階数が2以上であることを示す方法はほとんど知られていない. Rodriguez Villegas, Zagierは, 古典的な整数問題に関係する楕円曲線の階数が2であることの必要十分条件を, ある簡単な漸化式を用いて与えた.* 発表者はこの簡明な判定法に興味をもち, 他の楕円曲線に対しても同様の必要十分条件を与えることができないか考え, 本研究を行った.

【研究の位置付け】 リーマン予想と並んで難問とされているミレニアム問題の一つに, Birch and Swinnerton-Dyer(BSD)予想がある. BSD予想は, 楕円曲線の階数とL関数の特殊値の関係を主張するが, 未解決な部分が大多数である. したがって具体的な楕円曲線に対してBSD予想が成り立つ例を挙げることは整数論的に大きな結果とされている.

*** しかし詳細な証明は与えられておらず, その行間を埋めようと試みたところ, より計算効率のよい結果が得られた.**

Reference

[1] F. Rodriguez Villegas, D. Zagier, Which primes are sums of two cubes?, Number theory (Halifax, NS, 1994), 295-306, CMS Conf. Proc., 15, Amer. Math. Soc., Providence, RI, 1995. 11F67 (11D85 11G40)

[2] K. Nomoto, The rank of a CM elliptic curve and a recurrence formula, J. Number Theory (2021)

問. 素数pは有理数の3乗の和で表せるか？

例えば$p = 31$のとき, 知られている最も単純な式は以下である.

$$31 = \left(\frac{277028111}{119531076}\right)^3 + \left(\frac{316425265}{119531076}\right)^3$$

- 見た目よりも難しい問題である.
- 具体的に解を探すのではなく,
  存在性に着目する.

答. 以下の漸化式での$(p-1)/3$番目の多項式の定数項が素数pの倍数のとき表せる.

ただし, $p \equiv 1 \bmod 9$と仮定する.

Rodriguez Villegas, Zagier

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

Nomoto

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

表1: Rodriguez Villegas, Zagierが与えた漸化式の振る舞い

n	$a_n(t)$
0	1
1	$-3t^2$
2	$9t^4 + 2t$
3	$-27t^6 - 18t^3 - 2$
4	$81t^8 + 108t^5 + 36t^2$
5	$-243t^{10} - 540t^7 - 360t^4 + 152t$
6	$729t^{12} + 2430t^9 + 2700t^6 - 16440t^3 - 152$
7	$-2187t^{14} + 10206t^{11} - 17010t^8 + 1311840t^5 + 24240t^2$
8	$6561t^{16} + 40824t^{13} + 95256t^{10} - 99234720t^7 - 2974800t^4 + 6848t$
9	$-19683t^{18} - 157464t^{15} - 489888t^{12} + 7449816240t^9 + 359465040t^6 - 578304t^3 - 6848$

表2: Nomotoが与えた漸化式の振る舞い(1)

n	$x_n(t)$
0	1
1	0
2	$-t$
3	2
4	$-33t^2$
5	$76t$
6	$-339t^3$
7	$4314t^2$
8	$-72687t^4 - 3424t$
9	$228168t^3 + 6848$

整数問題から楕円曲線の理論へ

楕円曲線$A_p : x^3 + y^3 = p$は以下の方程式(Weierstrass標準形)に書き換えられる.

$$x^3 + y^3 = p \simeq y^2 = x^3 - 432p^2 \qquad (x, y) \mapsto \left(\frac{12p}{x+y}, \frac{36p(x-y)}{x+y} \right)$$

Mordell-Weilの定理と簡単な計算により, 楕円曲線A_pの$\mathbb{Q}$-有理点は以下の構造をもつ. $(p \neq 2)$

$$A_p(\mathbb{Q}) \simeq \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{r := \mathrm{rank} A_p(\mathbb{Q})}$$

$P \in A_p(\mathbb{Q})$が存在

$\iff \mathrm{rank} A_p(\mathbb{Q}) \neq 0$

3-降下法を用いると, 以下の階数の評価が得られる.

$$\mathrm{rank} A_p(\mathbb{Q}) \leq \begin{cases} 0 & (p \equiv 2,5 \bmod 9) \\ 1 & (p \equiv 4,7,8 \bmod 9) \\ 2 & (p \equiv 1 \bmod 9) \end{cases}$$

- 適切な仮定
- L関数の関数等式の符号
- Parity予想の帰結

$$\mathrm{rank} A_p(\mathbb{Q}) = \begin{cases} 0 & (p \equiv 2,5 \bmod 9) \\ 1 & (p \equiv 4,7,8 \bmod 9) \\ 0,\ 2 & (p \equiv 1 \bmod 9) \end{cases}$$

素数$p \equiv 1 \bmod 9$が有理数の3乗の和で表せる $\iff$ $\mathrm{rank} A_p(\mathbb{Q}) = 2 (\neq 0)$

----------▶ 階数が0でないことを漸化式の言葉で記述 (証明の詳細はスライド5枚目へ)

異なる楕円曲線へ

楕円曲線$E_p : y^2 = x^3 + px$ を考える. (p: 素数)

楕円曲線$A_p : x^3 + y^3 = p$の場合と同様にして, 右の等式を得る.

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

Theorem(N.)

$p \equiv 1,9 \bmod 16$を素数とする. BSD予想の下, 以下が成り立つ.

$$\mathrm{rank}E_p(\mathbb{Q}) = 2(\neq 0) \iff p \mid f_{3(p-1)/8}(0)$$

ここで, $f_n(t) \in \mathbb{Z}[t]$とは以下の漸化式で定まる多項式である.

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

表3: Nomotoが与えた漸化式の振る舞い(2)

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	$-1512t^5-11340t^4-\cdots-34992t^2-13122t+2187$
6	$21816t^6+196344t^5+\cdots+1027890t^2+433026t+80919$
7	$-280368t^7-2943864t^6-\cdots-46517490t^2-24074496t-5189751$
8	$3319056t^8+39828672t^7+\cdots+1016482608t^2+423420696t+82097793$
9	$-32283360t^9-435825360t^8-\cdots+2060573904t^2+4373050842t+1702205523$

表4: 定数項が素数pの倍数か

p	$p\mid(\frac{3(p-1)}{8}$ 番目の定数項)	p	$p\mid(\frac{3(p-1)}{8}$ 番目の定数項)
17		257	
41		281	○
73	○	313	
89	○	337	○
97		353	○
113	○	401	
137		409	
193		433	
233	○	449	
241		457	

証明の全体像

$\mathrm{rank} E_p(\mathbb{Q}) \neq 0$

p進L関数の補完公式による
代数的部分の間の合同

$L_k :=$ ($L(\psi^{2k-1}, k)$の代数的部分)

ψ : あるHecke指標, $k = \dfrac{3(p-1)}{4} + 1$

BSD予想

$\mathrm{rank} E_p(\mathbb{Q}) = \mathrm{ord}_{s=1} L(E_p/\mathbb{Q}, 1)$

$S_p = 0$ $\Longleftrightarrow$ $S_p \equiv 0 \bmod p$ $\Longleftrightarrow$ $L_k \equiv 0 \bmod p$

$|S_p| < p$

$S_p :=$ ($L(E_p/\mathbb{Q}, 1)$の代数的部分)

ある保型形式の$(k-1)$階
非正則微分の振る舞い

$L_k = |f_{(k-1)/2}(0)|^2$

$f_{3(p-1)/8}(0) \equiv 0 \bmod p$