# Which numbers are sums of two cubes?

Yukako Kezuka

## 1 はじめに

楕円曲線は数論において非常に興味深く重要な研究対象であり, 有理数体 $\mathbb{Q}$ 上の楕円曲線は 3 次方程式

$$E : y^2 = x^3 + Ax + B, \qquad A, B \in \mathbb{Q}$$

で表される曲線である. 楕円曲線 $E$ の有理点の集合 $E(\mathbb{Q})$ は群構造を持ち, モーデル-ヴェイユ群と呼ばれる有限生成アーベル群である. 楕円曲線の研究は少なくともフェルマー (1607–1665) にまで遡り, 1960 年代にバーチ-スウィンナートン・ダイアー予想 [1] が立てられたことにより活性化した. しかし, ある意味ではそのはるか前から楕円曲線の研究は始まっており, 数論における古くからの問題を楕円曲線の言語を用いて言い換えることにより, 問題の理解が深まるということが多々ある. たとえば $N \geq 1$ を任意の整数として, 「いかなる $N$ が全ての辺の長さが有理数である直角三角形の面積となるか」を問う合同数の問題は, 1000 年以上前から考えられていた数論上もっとも古い主要未解決問題のひとつである. つまり, $N$ が合同数であるとは

$$a^2 + b^2 = c^2, \qquad \frac{ab}{2} = N$$

を満たす有理数 $a, b, c$ が存在するということであるが, これは

$$E_N : y^2 = x^3 - N^2 x$$

という楕円曲線において $x, y \in \mathbb{Q}$, $y \neq 0$ となる解が存在するかを問うことと同値である. 楕円曲線 $E_N/\mathbb{Q}$ のねじれ部分群の非自明な元は $y = 0$ を満たすことから, 上記の条件は $E_N$ の階数が 1 以上であることと同値である. また,「2 つの 3 乗の和となる数はいかなる数か」という問題は, ディオファントスにまで遡る問題であるが, $X$ と $Y$ を変数とする方程式

$$C_N : X^3 + Y^3 = N$$

は $X = \frac{2^2 3^2 N + y}{2 \cdot 3x}$, $Y = \frac{2^2 3^2 N - y}{2 \cdot 3x}$ と変数変換することで $y^2 = x^3 - 2^4 3^3 N^2$ となり, $\mathbb{Q}$ 上の楕円曲線を定義する. 楕円曲線 $C_N/\mathbb{Q}$ のねじれ部分群が $N > 2$ のとき自明であることから, $N > 2$ が 2 つの有理数の 3 乗の和であることは, $C_N$ の階数が 1 以上であることと同値であることがわかる. しかし, この問題もまだ解決からは程遠い. 実際, $N$ が素数の場合においても, $N \equiv 1 \bmod 9$ の場合には階数 0（$N$ が 2 つの 3 乗の和ではない）と階数 2（$N$ が 2 つの 3 乗の和である）がどちらも起こり得る [10] ということがわかっているが, いつ階数 0 が起き, いつ階数 2 が起きるのかについては全くわかっていない. 本稿はこういった古典的な問題に直接貢献するものではないが, それに触発され古くから多くの数学者に研究されてきた楕円曲線 $C_N$ の演算の理解を深め, 特別な場合においてバーチ-スウィンナートン・ダイアー予想に貢献することを目的とする.

## 2 バーチ-スウィンナートン・ダイアー予想と 3 乗の和

整数 $N \geq 1$ が 2 つの有理数の 3 乗の和であるか否かを判別することの難しさを示すために, いくつか例を紹介したい. まず, $2 = 1^3 + 1^3$ が 2 つの有理数の 3 乗の和であることは容易に判別できるが, たとえば 13 と 17 もそうであり,

$$13 = \left(\frac{7}{3}\right)^3 + \left(\frac{2}{3}\right)^3$$
$$17 = \left(\frac{18}{7}\right)^3 + \left(\frac{-1}{7}\right)^3$$

を満たす. そして 157 も 2 つの有理数の 3 乗の和であり,

$$157 = \left(\frac{19964887}{1142148}\right)^3 + \left(\frac{-19767319}{1142148}\right)^3$$

を満たす [13] が, この時点でやみくもに解を探すだけでは不十分であることは明らかだ. ちなみに, 157 は合同数でもあり, $a$, $b$, $c$ を

$$a = \frac{411340519227716149383203}{21666555693714761309610}$$
$$b = \frac{6803298487826435051217540}{411340519227716149383203}$$
$$c = \frac{22440351770433696992455751309067486316094847204 1}{8912332268928859588025535178967163570016480830}$$

とする直角三角形の面積であることがザギエ [15] によって証明された. このように, $N$ が素数の場合ですら上記の古典的な問題が簡単ではないことは明らかであり, より

現代的な視点が必要となる．バーチ-スウィンナートン・ダイアー予想は全ての楕円曲線を扱う予想であるが, これを述べるために, $E$ を $\mathbb{Q}$ 上に定義された楕円曲線とする．また, $L(E,s)$ を $s$ を複素変数とする $E/\mathbb{Q}$ の ハッセ-ヴェイユの $L$-関数とし, $Ш(E)$ を $E/\mathbb{Q}$ のテイト-シャファレヴィッチ群とする．複素関数 $L(E,s)$ は $\mathrm{Re}(s) > \frac{3}{2}$ のときにしか収束しないが, $E$ が虚数乗法を持つとき, あるいは $\mathbb{Q}$ 上で定義されているときは解析接続によって複素平面全体に拡張できることが、それぞれドイリングの定理, そしてモジュラー性定理からわかっている．テイト-シャファレヴィッチ群は有限群であることが予想されており, その位数は $E$ の演算の複雑さ (局所大域原理の成立に対する障害) を測る．テイト-シャファレヴィッチ群について知られていることはまだ少ないが, 有限である場合にその位数は完全平方数であることがキャッセルズの定理 [2] からわかっている．バーチ-スウィンナートン・ダイアー予想は, 楕円曲線 $E$ に伴う複素解析的な構造物である $L(E,s)$ の $s=1$ における振る舞いを, 演算的な構造物である $E(\mathbb{Q})$ や $Ш(E)$ に以下のように関連づけるものである．

**予想 2.1** (Birch–Swinnerton-Dyer)**.** 楕円曲線 $E/\mathbb{Q}$ の複素級数 $L(E,s)$ の $s=1$ における零点の位数を $\mathrm{ord}_{s=1} L(E,s) = r_{\mathrm{a}}$ とし, $E(\mathbb{Q})$ の階数を $\mathrm{rank}(E(\mathbb{Q})) = r$ とすると

$$r_{\mathrm{a}} = r$$

が成り立つ．さらに, $L(E,s)$ を $s=1$ においてテイラー展開したとき

$$L(E,s) \sim \lambda(s-1)^r \qquad (s \to 1)$$

となる先頭項 $\lambda$ は公式

$$\lambda = \frac{cR\Omega \#(Ш(E))}{\left(\#(E(\mathbb{Q})_{\mathrm{tor}})\right)^2}$$

によって表される．ここで $c = \prod_q c_q$ は素数 $q$ における玉河数の積であり, $R$ は $E/\mathbb{Q}$ の単数基準, $\Omega$ は実周期, $E(\mathbb{Q})_{\mathrm{tor}}$ は $E(\mathbb{Q})$ のねじれ部分群である．

楕円曲線 $E/\mathbb{Q}$ が $r_a \leq 1$ を満たすとき, $r_a = r$ が成り立ち $Ш(E)$ が有限であることは, グロス-ザギエ [5], コリヴァギン [8] の定理によって証明されている．なお, 楕円曲線 $E$ が虚数乗法を持ち, $L(E,1) \neq 0$ のとき, ルービン [11] は岩澤理論を用いて バーチ-スウィンナートン・ダイアーの $p$-部分がほとんど全ての素数 $p$ おいて成り立つことを証明した．

**定理 2.2** (Rubin)**.** 楕円曲線 $E/\mathbb{Q}$ が虚 2 次体 $K$ の整数環 $\mathcal{O}_K$ により虚数乗法を持ち, $L(E,1) \neq 0$ のとき, $p \nmid \#(\mathcal{O}_K^\times)$ を満たす全ての素数 $p$ においてバーチ-スウィンナートン・ダイアーの $p$-部分

$$\mathrm{ord}_p\left(L^{(\mathrm{alg})}(E,1)\right) = \mathrm{ord}_p\left(\frac{\prod_q c_q \#(Ш(E))}{\left(\#(E(\mathbb{Q})_{\mathrm{tor}})\right)^2}\right)$$

が成り立つ.

ここで $\mathrm{ord}_p$ は $\mathrm{ord}_p(p) = 1$ と正規化された $p$ 進付値であり, $L^{(\mathrm{alg})}(E,1) = \frac{L(E,1)}{\Omega}$ は有理数であることがよく知られている [4]. また, $r = 0$ のときは $R = 1$ と定義されている. 虚 2 次体 $K$ の整数環の単元群は $K$ における 1 の冪根の群であるため, $K = \mathbb{Q}(\sqrt{-3})$ の場合は $\#(\mathcal{O}_K^\times) = 6$ であり, $p = 2$ と $p = 3$ のみが残る. その他 $K$ の場合は $\#(\mathcal{O}_K^\times) = 2$ あるいは 4 であるため, $p = 2$ のみが残される. 本稿では, $K = \mathbb{Q}(\sqrt{-3})$ で虚数乗法を持つ楕円曲線として $C_N$ を取り上げる. バーチ-スウィンナートン・ダイアー予想を仮定すると, 整数 $N > 2$ が 2 つの有理数の 3 乗の和であるということは, 楕円曲線 $C_N : X^3 + Y^3 = N$ の $L$-関数 $L(C_N, s)$ が $s = 1$ の点において 0 の値を取ることと同値である.

## 3 玉河数の可分性

楕円曲線 $C_N : X^3 + Y^3 = N$ は虚 2 次体 $K = \mathbb{Q}(\sqrt{-3})$ の整数環 $\mathcal{O}_K$ により虚数乗法を持つため, 定理 2.2 より, $L(C_N, 1) \neq 0$ の場合は残るは バーチ-スウィンナートン・ダイアー予想の 2-部分と 3-部分を考える必要がある. バーチ-スウィンナートン・ダイアー予想 2.1 に登場する玉河数 $c_q = [E(\mathbb{Q}_q) : E^0(\mathbb{Q}_q)]$ はテイトのアルゴリズム [14] によって計算できる局所指数であるが, $E$ が素数 $q$ において悪い還元を持つときのみ $c_q > 1$ が起こり得る. ここで $E^0(\mathbb{Q}_q)$ とは $q$ を法にして非特異な還元を持つ $\mathbb{Q}_q$-有理点の群である. さらに, $E$ が虚数乗法を持つとき, $c_q \leq 4$ であることがわかっているため, 玉河数の積 $\prod_q c_q$ は素数 2 と 3 のみで割り切れる. なお, $Ш(E)$ は多くの場合は自明であるか, その位数は小さな素数の積であることが多い様子が数値実験から観察できることからも, バーチ-スウィンナートン・ダイアー予想の $p$-部分が $p$ が小さいときに特に難しく, そして非常に興味深いことが窺える. 本節と第 4 節においては楕円曲線 $C_N$ の バーチ-スウィンナートン・ダイアー予想の 3-部分に焦点を当て, 第 5 節では 2-部分についても言及する. まずは $L^{(\mathrm{alg})}(C_N, 1)$ の 3 進付値に関する結果を紹介する.

**定理 3.1.** 無立方な整数 $N > 1$ に対し, $k(N)$ を相異なる $N$ の素因数の個数とする. このとき, 楕円曲線 $C_N : X^3 + Y^3 = N$ において, 不等号

$$\mathrm{ord}_3\left(L^{(\mathrm{alg})}(C_N, 1)\right) \geq \begin{cases} k(N) & N \text{ の素因数が全て } K \text{ で分解する場合} \\ k(N) - 1 & \text{その他の場合} \end{cases}$$

が成り立つ.

詳しい証明は [6] を参照していただくことにして, ここでは定理 3.1 と バーチ-スウィンナートン・ダイアー予想の整合性について言及する. まず, 定理 3.1 は特別な場合において, 不等号ではなく等号を示すことができ, この場合に バーチ-スウィンナートン・ダイアー予想の 3-部分が証明できる (定理 4.1 参照). 次に, $s(N)$, $i(N)$, $r(N)$ をそれぞれ相異なる $N$ の素因数で $K$ で分解するもの, 惰性が残るもの, 分岐するものの個数とする. すると,

$$k(N) = s(N) + i(N) + r(N)$$

と書けるが, 勿論 $N$ が 3 で割り切れる場合には $r(N) = 1$ であり, その他の場合には $r(N) = 0$ である. また, テイトのアルゴリズムから $C_N$ の玉河数の積が

$$\mathrm{ord}_3\left(\prod_{q\mathrm{bad}} c_q\right) = \begin{cases} s(N) + 1 & N \equiv 1, 8 \bmod 9 \text{ の場合} \\ s(N) & \text{その他の場合} \end{cases}$$

を満たすことが計算できる. よって, $r(N)$ と $\mathrm{ord}_3\left(Ш(C_N)\right)$ に関係があることが バーチ-スウィンナートン・ダイアー予想されるが, 次の定理は 3-降下法から得られる.

**定理 3.2.** 無立方な整数 $N > 1$ に対し, $C_N : X^3 + Y^3 = N$ とする. このとき, $C_N/\mathbb{Q}$ のテイト-シャファレヴィッチ群の 3-ねじれ部分群 $Ш(C_N)[3]$ の位数は, 不等号

$$\mathrm{ord}_3\left(\#\left(Ш(C_N)[3]\right)\right) \geq i(N) - t(N) - 1 - \mathrm{rank}(C_N)$$

を満たす. ここで $i(N)$ は相異なる $N$ の素因数で $K$ で惰性が残るものの個数であり, $t(N)$ は $N \equiv \pm 1 \bmod 9$ のとき $t(N) = 1$, $\mathrm{ord}_3(N) = 1$ のとき $t(N) = -1$, その他の場合には $t(N) = 0$ と定義する.

さらに, 定理 3.1 から得られる $L^{(\mathrm{alg})}(C_N, 1)$ の玉河数の積による可分性と $L(C_N, 1)$ の値をテータ関数の CM 点における値で表す公式を組み合わせることによって, 次の系を得る.

**系 3.3.** 無立方な整数 $N > 2$ の素因数が全て $K$ で分解する（$k(N) = s(N)$ を満たす）とき, バーチ-スウィンナートン・ダイアー予想の公式によって予言される $Ш(C_N)$ の位数は完全平方数である.

無立方な整数 $N > 2$ に対して $C_N/\mathbb{Q}$ のねじれ部分群は自明であるため, バーチ-スウィンナートン・ダイアー予想の公式によって予言される $Ш(C_N)$ の位数とは

$$\mathcal{S}_N = \frac{L^{(\mathrm{alg})}(C_N, 1)}{\prod_q c_q}$$

を意味する. また, 系 3.3 は前述したキャッセルズの定理から予言されることに整合する.

# 4 バーチ-スウィンナートン・ダイアー予想の 3-部分

本節より, 素数 $p$ を

$$p \equiv 2 \bmod 9 \quad \text{あるいは} \quad p \equiv 5 \bmod 9$$

を満たす奇素数とする. さらに $p^*$, $p_*$ の表記を

$$p^* = \begin{cases} p & p \equiv 2 \bmod 9 \text{ の場合} \\ p^2 & p \equiv 5 \bmod 9 \text{ の場合}, \end{cases} \quad p_* = \begin{cases} p^2 & p \equiv 2 \bmod 9 \text{ の場合} \\ p & p \equiv 5 \bmod 9 \text{ の場合} \end{cases} \tag{4.1}$$

と定める. これまで $N$ の相異なる素因数の個数を制限することをしなかったが, 李永雄との共同研究 [7] において, $N$ の素因数を 2 と $p$ に限定することにより, 次の定理 4.1 を得た.

**定理 4.1.** 奇素数 $p$ を $p \equiv 2 \bmod 9$ あるいは $p \equiv 5 \bmod 9$ を満たすものとし、 $N = 2p^*$, $2p_*$ あるいは $2^2p^*$ とする. このとき, $Ш(C_N)$ は有限であり, バーチ-スウィンナートン・ダイアー予想の 3-部分が $C_N/\mathbb{Q}$ において成り立つ.

このとき, $\mathrm{rank}(C_{2p^*}) = 1$ であることがサッジェの定理 [12] からわかっている. なお, 3-降下法を用いて, $\mathrm{rank}(C_{2p_*}) = \mathrm{rank}(C_{2^2p_*}) = 0$ を示すことができる. 定理 4.1 では, 階数が 0 である $N = 2p_*$, $2^2p^*$ の場合に定理 3.1 における不等号が等号になることを示すことにより, $L(C_N, 1) \neq 0$ であり バーチ-スウィンナートン・ダイアー予想の 3-部分が成り立つことを証明する. さらに, 階数が 1 である $N = 2p^*$ の場合においては, サッジェの構成した非自明なヒーグナー点と $L$-関数の特殊値をグロス-ザギエ公式を用いて関連づけることにより得られた, $\#\left(Ш(C_{2p^*})\right) \times \#\left(Ш(C_{2p_*})\right)$ が バーチ-スウィンナートン・ダイアー予想の 3-部分に予想されるものと一致する, という蔡-舒-田の定理 [3] を組み合わせることにより, 証明を得る.

# 5　テイト-シャファレヴィッチ群の 2-部分の非自明性

最後に, テイト-シャファレヴィッチ群の 2-部分についての結果を述べる. 本節でも $p$ を $p \equiv 2 \bmod 9$ あるいは $p \equiv 5 \bmod 9$ を満たす奇素数とし, $N = 2p$ あるいは $N = 2p^2$ とする. また, $L = \mathbb{Q}(\sqrt[3]{p})$ と置き, $\mathrm{Cl}(L)$ を $L$ のイデアル類群とする. このとき, $L$ のイデアル類群 $\mathrm{Cl}(L)$ の 2-ねじれ部分群と $C_N/\mathbb{Q}$ の 2-セルマー群 $\mathrm{Sel}_2(C_N)$ を 2-降下法で関係付ける李との共同研究 [7] により, 次の定理が示される.

**定理 5.1.** 奇素数 $p \equiv 2, 5 \bmod 9$ に対し, $p^*$, $p_*$ を (4.1) で定義し, $N = 2p^*$ あるいは $N = 2p_*$ と定める. このとき, $r = \mathrm{rank}(C_N)$ は $N = 2p^*$ の場合は $r = 1$, $N = 2p_*$ の場合は $r = 0$ であり, 以下は同値である.

1. $\mathrm{rank}_2(\mathrm{Cl}(L)) \geq r + 1$.
2. $Ш(C_N)[2]$ が非自明である.

特に $\mathrm{rank}_2(\mathrm{Cl}(L)) \geq 2$ を満たすとき, $C_{2p^*}$ は階級 1 で非自明な $Ш(C_{2p^*})[2]$ を持つ楕円曲線である.

**証明.** イデアル類群の 2-階数 $\mathrm{rank}_2(\mathrm{Cl}(L)) = \dim_{\mathbb{F}_2}(\mathrm{Cl}(L)/2\mathrm{Cl}(L))$ を $\ell$ と置き,

$$N_1 = \{\alpha \in L^\times/(L^\times)^2 : L(\sqrt{\alpha})/L \text{ は分岐する }\}$$
$$N_2 = \{\alpha \in L^\times/(L^\times)^2 : \alpha > 0, (\alpha) = I^2, I \text{ は } L \text{ の分数イデアル }\}$$

と定義する. このとき, 局所・大域クンマー写像を用いて, $\mathrm{Sel}_2(C_N)$ が

$$N_1 \subset \mathrm{Sel}_2(C_N) \subset N_2$$

の包含関係を満たすことが示される. 数体 $H_2$ を $L$ の冪数 2 の最大アーベル不分岐拡大とすると, クンマー理論により

$$N_1 \simeq \mathrm{Hom}(\mathrm{Gal}(H_2/L), \mu_2)$$

が得られる. また, 類体論により $\mathrm{Gal}(H_2/L) \simeq \mathrm{Cl}(L)[2]$ であるため, $\#(N_1) = 2^\ell$ であることがわかる. その一方で

$$N_2 \to \mathrm{Cl}(L)[2] \quad \alpha \mapsto [I]$$

は核が $\mathbb{Z}/2\mathbb{Z}$ に同型である全射であることを示すことができる. よって, $\epsilon(C_N/\mathbb{Q})$ を

$C_N/\mathbb{Q}$ の関数等式の符号とすると, モンスキーに証明された 2-偶奇予想 [9] により

$$\dim_{\mathbb{F}_2} \mathrm{Sel}_2(C_N) = \begin{cases} \ell & \text{if } \epsilon(C_N/\mathbb{Q}) = (-1)^{\ell} \\ \ell+1 & \text{if } \epsilon(C_N/\mathbb{Q}) = (-1)^{\ell+1} \end{cases}$$

が得られる. この事実と $\mathrm{Sel}_2(C_N)$ と $Ш(C_N)[2]$ の関係を組み合わせることにより, 定理が従う. □

階級 0 の楕円曲線で非自明なテイト-シャファレヴィッチ群の 2-ねじれ部分を持つ例は多く知られているが, 階級 1 の場合このような例は数値計算でしか知られていない. 定理 5.1 において注目すべき点は, 階級 1 を持つ楕円曲線 $C_{2p^*}$ が非自明なテイト-シャファレヴィッチ群の 2-ねじれ部分を持つか否かの理論的な判定法が得られるということである.

## 6 謝辞

早稲田整数論研究集会で講演をする機会を与えていただいた緒先生方に感謝の意を表する. 本研究の一部は Marie Skłodowska-Curie grant agreement No. 101026826 の下で European Union's Horizon 2020 research and innovation プログラムに支援を受けたものである.

## 参考文献

[1] B. Birch, P. Swinnerton-Dyer, *Notes on elliptic curves. II*, J. Reine Angew. Math. 218 (1965) 79–108.

[2] J.W.S. Cassels, *Arithmetic on curves of genus 1. IV. Proof of the Hauptvermutung*, J. Reine Angew. Math. 211 (1962) 95–112.

[3] L. Cai, J. Shu, Y. Tian, *Cube sum problem and an explicit Gross–Zagier formula*, Amer. J. Math. 139, no. 3 (2017) 785–816.

[4] C. Goldstein and N. Schappacher, *Séries d'Eisenstein et fonctions L de courbes elliptiques à multiplication complexe*, J. Reine Angew. Math. 327 (1981) 184–218.

[5] B. Gross, D. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. 84 (2) (1986) 225–320.

[6] Y. Kezuka, *Tamagawa number divisibility of central L-values of twists of the Fermat elliptic curve*, J. Théor. Nombres Bordeaux, Tome 33, No. 3.2 (2021) 945–970.

Iwasawa 2019 special issue.

[7] Y. Kezuka, Y-X. Li, *A classical family of elliptic curves having rank one and the 2-primary part of their Tate-Shafarevich group non-trivial*, Doc. Math. Vol. 25 (2020) 2115–2147.

[8] V. A. Kolyvagin, *Finiteness of $E(\mathbb{Q})$ and $Ш(E, \mathbb{Q})$ for a subclass of Weil curves*, Math. USSR Izvestiya, 32 (3) (1989).

[9] P. Monsky, *Generalizing the Birch-Stephens theorem. I. Modular curves*, Math. Z. 221, no. 3 (1996) 415–420.

[10] F. Rodriguez Villegas, D. Zagier *Which primes are sums of two cubes?* CMS Conf. Proc. 15, Amer. Math. Soc. Providence, RI (1995).

[11] K. Rubin, *The "main conjectures" of Iwasawa theory for imaginary quadratic fields*, Invent. Math. 103, no. 1 (1991) 25–68.

[12] P. Satgé, *Un analogue du calcul de Heegner*, Invent. Math. 87, no. 2 (1987) 425–439.

[13] E. S. Selmer, *The diophantine equation $ax^3+by^3+cz^3 = 0$*, Acta Math. 85 (1951), 203–362.

[14] J. Tate, *Algorithm for determining the type of a singular fiber in an elliptic pencil*, Modular Functions of One Variable IV, Lecture Notes in Math. Springer 476 (1975) 33–52.

[15] D. Zagier, *Elliptische Kurven: Fortschritte und Anwendungen*, Jahresber. Deutsch. Math.-Verein. 92 (2) (1990) 58–76.

Yukako Kezuka
Institut de Mathématiques de Jussieu
4 Pl. Jussieu
75005 Paris, France
*y*ukako.kezuka@imj-prg.fr