On the rank of elliptic curve $y^2 = x^3 + px$ and a recurrence formula

Keiichiro Nomoto

Kyushu University

2020/09/10

Introduction

Question

Which prime p can be written as the sum of two cubes of rational numbers?

The curve $A_p : x^3 + y^3 = p$ has the structure of an **elliptic curve** over $\mathbb{Q}$.

$$x^3 + y^3 = p \cong_{/\mathbb{Q}} y^2 = x^3 - 432p^2; (x, y) \mapsto \left(\frac{12p}{x+y}, \frac{36p(x-y)}{x+y} \right)$$

- $A_p(\mathbb{Q}) \cong \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{r} \oplus (\text{finite group})$ $(\because \text{Mordell} - \text{Weil Theorem})$
- $(\text{finite group}) = \begin{cases} \{O\} & (p \geq 3) \\ \{O, (1,1)\} & (p = 2) \end{cases}$ $(O = [1 : -1 : 0] : \text{infinity point})$

odd prime p is **cube sum** $\iff$ $r = \text{rank } A_p(\mathbb{Q}) \neq 0$

A 3-descent shows

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

If the Tate-Shafarevich group $Ш(A_p/\mathbb{Q})$ is **finite**, the **parity conjecture** of 3-Selmer group shows

- $\operatorname{rank} A_p(\mathbb{Q}) = 1$ $(p \equiv 4, 7, 8 \mod 9)$,
- $\operatorname{rank} A_p(\mathbb{Q}) = 0, 2$ $(p \equiv 1 \mod 9)$.

The remaining problem is essentially

For the case $p \equiv 1 \bmod 9$, whether the rank is 0 or 2 ?

For the case $p \equiv 1 \bmod 9$, the following theorem holds.

Theorem (Villegas, Zagier(1995))

Let p be a prime such that $p \equiv 1 \mod 9$. If $\operatorname{rank} A_p(\mathbb{Q}) = 2$, then $p | a_{(p-1)/3}(0)$, where the polynomial $a_n(t) \in \mathbb{Z}[t]$ is defined by the recurrence formula

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

The initial condition is $a_0(t) = 1, a_1(t) = -3t^2$. Moreover if we assume the Birch and Swinnerton-Dyer (BSD) conjecture, then the converse is true.

Villegas and Zagier did not give the details of the proof. So we have tried to recover it but we obtained main theorem 2. We talk about it later.

Theorem (Villegas, Zagier)

For $p \equiv 1 \bmod 9$ and $A_p : x^3 + y^3 = p$, there exists $a_n(t) \in \mathbb{Z}[t]$ s.t.

$$\operatorname{rank} A_p(\mathbb{Q}) = 2 \overset{\text{BSD}}{\iff} p | a_{(p-1)/3}(0).$$

Theorem (N.)

For $p \equiv 1, 9 \bmod 16$ and $E_p : y^2 = x^3 + px$, there exists $f_n(t) \in \mathbb{Z}[t]$ s.t.

$$\operatorname{rank} E_p(\mathbb{Q}) = 2 \overset{\text{BSD}}{\iff} p | f_{3(p-1)/8}(0).$$

Theorem (N.)

For $p \equiv 1 \bmod 9$ and $A_p : x^3 + y^3 = p$, there exists $x_n(t) \in \mathbb{Z}[t]$ s.t.

$$\operatorname{rank} A_p(\mathbb{Q}) = 2 \overset{\text{BSD}}{\iff} p | x_{(p-1)/3}(0).$$

Main Theorem 1

We consider the **elliptic curve** $E_p : y^2 = x^3 + px$. A 2-descent shows

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

If the Tate-Shafarevich group $Ш(E_p/\mathbb{Q})$ is **finite**, we have

- $\operatorname{rank} E_p(\mathbb{Q}) = 1$ $(p \equiv 3, 5, 13, 15 \mod 16)$,
- $\operatorname{rank} E_p(\mathbb{Q}) = 0, 2$ $(p \equiv 1, 9 \mod 16)$.

The remaining problem is essentially

For the case $p \equiv 1, 9 \bmod 16$, whether the rank is 0 or 2 ?

Theorem (N.)

Let p be a prime such that $p \equiv 1, 9 \bmod 16$. If $\operatorname{rank} E_p(\mathbb{Q}) = 2$, then $p | f_{3(p-1)/8}(0)$, where the polynomial $f_n(t) \in \mathbb{Z}[t]$ is defined by the recurrence formula

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

The initial condition is $f_0(t) = 1, f_1(t) = 2t+3$. Moreover if we assume the BSD conjecture, then the converse is true.

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	$-32283360t^9-435825360t^8-2479253184t^7-7727493312t^6-\cdots+1702205523$

Table: the recurrence formula for $f_n(t)$

p	$p\|f_{3(p-1)/8}(0)$	p	$p\|f_{3(p-1)/8}(0)$	p	$p\|f_{3(p-1)/8}(0)$
17		401		809	
41		409		857	
73	○	433		881	○
89	○	449		929	
97		457		937	○
113	○	521		953	
137		569		977	
193		577		1009	
233	○	593	○	1033	○
241		601	○	1049	○
257		617	○	1097	
281	○	641		1129	
313		673		1153	○
337	○	761		1193	○
353	○	769		1201	

Strategy

In the following, we suppose that a prime p satisfies $p \equiv 1, 9 \bmod 16$. The proof of the theorem is done in the following steps.

1. $\operatorname{rank} E_p(\mathbb{Q}) \neq 0 \overset{\text{BSD}}{\iff} L(E_p/\mathbb{Q}, 1) = 0$.
2. $L(E_p/\mathbb{Q}, 1) = 0 \iff S_p \equiv 0 \mod p$ (an **algebraic part** of $L(E_p/\mathbb{Q}, 1)$).
3. $S_p \equiv 0 \mod p \iff L_k \equiv 0 \mod p$ (an **algebraic part** of $L(\psi^{2k-1}, k)$) for some k.
4. Write $L(\psi^{2k-1}, k)$ in terms of a special value of "**derivative**" of some modular form.
5. Describe the special value of derivative of the modular form as a **recurrence formula**.

Conjecture (Birch and Swinnerton-Dyer conjecture)

Let $L(E/\mathbb{Q}, s)$ be the Hasse-Weil L-function of an elliptic curve E over $\mathbb{Q}$. Then the Taylor expansion of $L(E, s)$ at $s = 1$ has the form

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

where $c \neq 0$. Moreover, the constant c is equal to

$$\frac{\Omega_E \cdot \operatorname{Reg}(E) \cdot \#Ш(E/\mathbb{Q}) \cdot \prod_p c_p}{\#E(\mathbb{Q})_{\text{tors}}^2},$$

where

- Ω_E: real period,
- $\operatorname{Reg}(E)$: regulator,
- $Ш(E/\mathbb{Q})$: Tate-Shafarevich group,
- c_p: Tamagawa number at prime p.

Step 1. $\operatorname{rank} E_p(\mathbb{Q}) \neq 0 \overset{\text{BSD}}{\Longleftrightarrow} L(E_p/\mathbb{Q}, 1) = 0.$

- $L(E_p/\mathbb{Q}, s)$: Hasse-Weil L-function for $E_p : y^2 = x^3 + px$
- $\Omega = \Gamma(1/4)^2/2\pi^{1/2}$: real period of $E_1 : y^2 = x^3 + x$
- S_p: the constant such that

$$L(E_p/\mathbb{Q}, 1) = \frac{2\Omega}{p^{1/4}} S_p$$

Coates-Wiles Theorem implies

$$\operatorname{rank} E_p(\mathbb{Q}) \neq 0 \Longrightarrow S_p = 0.$$

Moreover, the BSD conjecture predicts **the converse is true** and $S_p = \#\text{Ш}(E_p/\mathbb{Q})$ if $\operatorname{rank} E_p(\mathbb{Q}) \neq 0$. In particular, $\underline{S_p \in \mathbb{Z}}$.

Step 2. $L(E_p/\mathbb{Q},1)=0 \iff S_p \equiv 0 \mod p$

Proposition (Zagier(1995))

Let $E/\mathbb{Q}$ be an elliptic curve of conductor N. Then

$$|L(E/\mathbb{Q},1)| < (4N)^{1/4}\left(\log\frac{\sqrt{N}}{8\pi}+\gamma\right)+c_0,$$

where $\gamma = 0.577\ldots$ is Euler's constant and $c_0=\zeta(1/2)^2=2.13263\ldots$.

This estimate leads to $\underline{S_p < p}$ and we have

$$L(E_p/\mathbb{Q},1)=\frac{2\Omega}{p^{1/4}}S_p=0 \iff S_p=0 \iff S_p\equiv 0 \mod p.$$

Step 3. $S_p \equiv 0 \mod p \iff L_k$ (an algebraic part of $L(\psi^{2k-1}, k)) \equiv 0 \mod p$

The elliptic curve $E_1 : y^2 = x^3 + x$ has **complex multiplication** by $\mathbb{Z}[\sqrt{-1}]$.

- ψ: **Hecke character** of $\mathbb{Q}(\sqrt{-1})$ associated to E_1.
- $L(E_p/\mathbb{Q}, s) = L(\psi\chi, s)$ for some **quartic character** χ over $\mathbb{Q}(\sqrt{-1})$.

Idea

A calculation of $L(\psi\chi, 1)$ which is **dependent** of prime p reduces to a calculation which is **independent** of p.

Set $k = (3p+1)/4 \in \mathbb{Z}$ (Note that $p \equiv 1, 9 \bmod 16$). Simple calculation gives

$$L(\psi\chi, 1) = \sum_{\mathfrak{a}} \chi(\mathfrak{a}) \frac{1}{\bar{\psi}(\mathfrak{a}) N\mathfrak{a}^s}\bigg|_{s=0},$$

$$L((\psi\chi)^{2k-1}, k) = L(\psi^{2k-1}, k) = \sum_{\mathfrak{a}} \left(\frac{\alpha}{\bar{\alpha}}\right)^{k-1} \frac{1}{\bar{\psi}(\mathfrak{a}) N\mathfrak{a}^s}\bigg|_{s=0},$$

where the sum runs over all non-zero ideals $\mathfrak{a} = (\alpha)$ of $\mathbb{Z}[\sqrt{-1}]$.

- $E_p : y^2 = x^3 + px$ is **ordinary** for $p \equiv 1 \bmod 4$.
- Then there exists a p-**adic** L-**function interpolating special values** above. (*cf.* Katz [1])

[1] N. M. Katz, *p-adic interpolation of real analytic Eisenstein series*, Ann. of Math. (2) 104 (1976), no. 3, 459-571. 14G10 (10D25)

We define the algebraic part of $L(\psi^{2k-1}, k)$ to be

$$L_k = \frac{2^{k+1}3^{k-1}\pi^{k-1}(k-1)!}{\Omega^{2k-1}} L(\psi^{2k-1}, k) \in \mathbb{Z}.$$

By an existsence a p-adic L-function, there exists a $\bmod p$ **congruence relation** between S_p and L_k. More precisely, the following holds.

$$S_p \equiv -2^{(p-13)/4} 3^{(p-1)/4} \left(\frac{p-1}{4}\right)!^2 L_k \mod p \quad (k = (3p+1)/4)$$

Therefore, we have

$$S_p \equiv 0 \mod p \iff L_k \equiv 0 \mod p.$$

Actually, L_k is a **square integer**. Thus we calculate the square root of L_k.

Step 4. Write $L(\psi^{2k-1}, k)$ in terms of a special value of "derivative" of some modular form.

Let ∂_k be the **Mass-Shimura operator**

$$\partial_k = D - \frac{k}{4\pi y} = \frac{1}{2\pi i}\frac{d}{dz} - \frac{k}{4\pi y} \ (z = x + iy),$$

and let the h-th derivative be

$$\partial_k^{(h)} := \partial_{k+2h-2} \circ \partial_{k+2h-4} \circ \cdots \circ \partial_{k+2} \circ \partial_k.$$

We set

$$\theta_2(z) = \sum_{n\in\mathbb{Z}+1/2} e^{\pi i n^2 z},\ \theta_4(z) = \sum_{n\in\mathbb{Z}} (-1)^n e^{\pi i n^2 z}.$$

By using the method of Villegas and Zagier [2], we calculate $L(\psi^{2k-1}, k)$.

Theorem (N.)

Let ψ be the Hecke character of $\mathbb{Q}(i)$ associated to $E_1 : y^2 = x^3 + x$. Then for $L(\psi^{2k-1}, s)$, we have

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

[2] Villegas, D. Zagier, *Square roots of central values of Hecke L-series.* Advances in number theory (Kingston, ON, 1991), 81-99, Oxford Sci. Publ., Oxford Univ. Press, New York, 1993. 11F67

Step 5. Describe the special value of "derivative" of the modular form as a recurrence formula.

- $E_2(z) = 1 - 24\sum_{n=1}^{\infty} \sigma_1(n)q^n$: **Eisenstein series** of weight 2
- $E_2^*(z) = E_2(z) - 3/\pi y$

For **holomorphic** modular form f, $\partial_k f$ is **not holomorphic** in general. But the **Ramanujan-Serre operator**

$$\vartheta_k = D - \frac{k}{12}E_2 = \partial_k - \frac{k}{12}E_2^*$$

maps a **holomorphic** modular form to a **holomorphic** modular form.

${}^\forall\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$, it follows that

$$E_2^*(\gamma z) = (cz+d)^2 E_2^*(z) \left(\iff E_2(\gamma z) = (cz+d)^2 E_2(z) + \frac{6}{\pi i}c(cz+d) \right)$$

and we have $\underline{E_2^*(i) = 0}$.

Villegas and Zagier have introduced the following series.

$$f_\partial(z,X) = \sum_{n=0}^{\infty} \frac{\partial_k^{(n)} f(z)}{k(k+1)\dots(k+n-1)} \frac{X^n}{n!} \ (z \in \mathbb{H}, X \in \mathbb{C}, f \in M_k(\Gamma))$$

$$f_\vartheta(z,X) = e^{-E_2^*(z)X/12} f_\partial(z,X) =: \sum_{n=0}^{\infty} \frac{F_n(z)}{k(k+1)\dots(k+n-1)} \frac{X^n}{n!}$$

Since $E_2^*(i) = 0$, we have

$$f_\partial(i,X) = f_\vartheta(i,X) \qquad \text{i.e.} \qquad \partial_{1/2}^{(N)} \theta_2(z)|_{z=i} = F_n(i).$$

How to behave the function $F_n(z)$?

Proposition (Villegas, Zagier(1993))

Let $f \in M_k(\Gamma)$. Then the series $f_\vartheta(z, X)$ has the expansion

$$f_\vartheta(z, X) = \sum_{n=0}^{\infty} \frac{F_n(z)}{k(k+1)\dots(k+n-1)} \frac{X^n}{n!}$$

where $F_n \in M_{k+2n}(\Gamma)$ is the modular form defined by the following recurrence formula

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

The initial condition is $F_0 = f, F_1 = \vartheta_k f$.

We have

- $\theta_2^4, \theta_4^4 \in M_2(\Gamma(2))$
- $\bigoplus_{k\in\frac{1}{2}\mathbb{Z}} M_k(\Gamma(2)) \cong \mathbb{C}[\theta_2, \theta_4]$.

The operator ϑ acts on $\mathbb{C}[\theta_2, \theta_4]$ as

$$\vartheta = \left(\frac{1}{12}\theta_2\theta_4^4 + \frac{1}{24}\theta_2^5\right)\frac{\partial}{\partial\theta_2} - \left(\frac{1}{12}\theta_2^4\theta_4 + \frac{1}{24}\theta_4^5\right)\frac{\partial}{\partial\theta_4}.$$

Therefore $F_n(z)$ is defiend by the recurrence formula

$$F_{n+1} = \left(\frac{1}{12}\theta_2\theta_4^4 + \frac{1}{24}\theta_2^5\right)\frac{\partial F_n}{\partial\theta_2} - \left(\frac{1}{12}\theta_2^4\theta_4 + \frac{1}{24}\theta_4^5\right)\frac{\partial F_n}{\partial\theta_4} - \frac{n(n-1/2)}{144}E_4F_{n-1}.$$

We divide both sides by $\theta_2^{4n+5}/24^{n+1}$.

$$\frac{24^{n+1}F_{n+1}}{\theta_2^{4n+5}} = 24^n\frac{2\theta_2\theta_4^4+\theta_2^5}{\theta_2^{4n+5}}\frac{\partial F_n}{\partial\theta_2} - 24^n\frac{2\theta_2^4\theta_4+\theta_4^5}{\theta_2^{4n+5}}\frac{\partial F_n}{\partial\theta_4} - 2n(2n-1)\frac{E_4}{\theta_2^8}\frac{24^{n-1}F_{n-1}}{\theta_2^{4n-3}}$$

We set

- $f_n = 24^n F_n/\theta_2^{4n+1}$ (<u>degree 0</u>),
- $t = (\theta_4^4-\theta_2^4)/\theta_2^4$ (which satisfies $\underline{t(i)=0}$).

Then the recurrence formula $F_n(z)$ transforms

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

and we have

$$F_N(i) = \frac{1}{24^N}\theta_2(i)^{4N+1}f_N(t(i)) = \frac{1}{24^N}\theta_2(i)^{4N+1}\underbrace{f_N(0)}_{=\sqrt{L_k}}.$$

Theorem (Villegas, Zagier)

For $p \equiv 1 \bmod 9$ and $A_p : x^3 + y^3 = p$, there exists $a_n(t) \in \mathbb{Z}[t]$ s.t.

$$\operatorname{rank} A_p(\mathbb{Q}) = 2 \overset{\text{BSD}}{\iff} p \mid a_{(p-1)/3}(0).$$

Theorem (N.)

For $p \equiv 1, 9 \bmod 16$ and $E_p : y^2 = x^3 + px$, there exists $f_n(t) \in \mathbb{Z}[t]$ s.t.

$$\operatorname{rank} E_p(\mathbb{Q}) = 2 \overset{\text{BSD}}{\iff} p \mid f_{3(p-1)/8}(0).$$

Theorem (N.)

For $p \equiv 1 \bmod 9$ and $A_p : x^3 + y^3 = p$, there exists $x_n(t) \in \mathbb{Z}[t]$ s.t.

$$\operatorname{rank} A_p(\mathbb{Q}) = 2 \overset{\text{BSD}}{\iff} p \mid x_{(p-1)/3}(0).$$

Main Theorem 2

Theorem (N.)

Let p be a prime such that $p \equiv 1 \bmod 9$. If $\operatorname{rank} A_p(\mathbb{Q}) = 2$, then $p | x_{(p-1)/3}(0)$, where the polynomial $x_n(t) \in \mathbb{Z}[t]$ is defined by the recurrence formula

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

The initial condition is $x_0(t) = 1, x_1(t) = 0$. Moreover if we assume the BSD conjecture, then the converse is true.

Villegas and Zagier have given the recurrence formula

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

by using a hypergeometric function and some identity of the Maass-Shimura operator.

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	$6561t^{16} + 40824t^{13} + \cdots - 99234720t^7 - 2974800t^4 + 6848t$
9	$-19683t^{18} - 157464t^{15} - \cdots + 359465040t^6 - 578304t^3 - 6848$

Table: the recurrence formula for $a_n(t)$ of Villegas and Zagier

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

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	$228168t^3 + 6848$

Perhaps we may make the recurrence formula simpler.

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

Summary

- Under the BSD conjecture, the problem of determine $\operatorname{rank} E_p(\mathbb{Q})$ is almost solved except for the case $p \equiv 1, 9 \bmod 16$.
- $\operatorname{rank} E_p(\mathbb{Q}) \neq 0\ (= 2) \iff p$ divides an algebraic part of $L(\psi^{2k-1}, k)$ via the theory of p-adic L-function.
- Write $L(\psi^{2k-1}, k)$ in terms of the special value of Maass-Shimura derivative of some modular form at $z = i$.
- By using the series $f_\partial(z, X)$, we describe the special value as the constant term of a polynomial that is defined by the recurrence formula.

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

$$\operatorname{rank} E_p(\mathbb{Q}) \neq 0 \overset{\text{BSD}}{\iff} p | f_{3(p-1)/8}(0)$$