Commun. Korean Math. Soc. **27** (2012), No. 3, pp. 497–503
http://dx.doi.org/10.4134/CKMS.2012.27.3.497

ON ELLIPTIC CURVES WHOSE 3-TORSION SUBGROUP SPLITS AS $\mu_3 \oplus \mathbb{Z}/3\mathbb{Z}$

Masaya Yasuda

Abstract. In this paper, we study elliptic curves E over $\mathbb{Q}$ such that the 3-torsion subgroup $E[3]$ is split as $\mu_3 \oplus \mathbb{Z}/3\mathbb{Z}$. For a non-zero integer m, let C_m denote the curve $x^3 + y^3 = m$. We consider the relation between the set of integral points of C_m and the elliptic curves E with $E[3] \simeq \mu_3 \oplus \mathbb{Z}/3\mathbb{Z}$.

1. Introduction

Let E be an elliptic curve over the field $\mathbb{Q}$ of rational numbers. For a prime p, the p-torsion points of E are the points of finite order p in the Mordell-Weil group $E(\mathbb{Q})$. Assume that E has a 3-torsion point P. By translating P to the point $(0,0)$, we get the Weierstrass equation of E as follows:

$$y^2 + axy + by = x^3,\ a, b \in \mathbb{Q} \tag{1}$$

with $\Delta(E) = b^3(a^3 - 27b) \neq 0$, where $\Delta(E)$ is the discriminant of E. For $m \in \mathbb{Z}$, let $E[m]$ denote the m-torsion subgroup of E. Using the Weil-pairing $e_3 : E[3] \times E[3] \to \mu_3$, we can define a map $E[3] \to \mu_3$ by $Q \mapsto e_3(P,Q)$. Since the point P is rational over $\mathbb{Q}$, this map gives an exact sequence

$$0 \to \mathbb{Z}/3\mathbb{Z} \to E[3] \to \mu_3 \to 0 \tag{2}$$

of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-modules. The purpose of this paper is to study elliptic curves E such that $E[3]$ is split as $\mu_3 \oplus \mathbb{Z}/3\mathbb{Z}$.

For an elliptic curve E with $E[3] \simeq \mu_3 \oplus \mathbb{Z}/3\mathbb{Z}$, there exists an isogeny $\phi : E \to E'$ with $\ker\phi = \mu_3$. Note that the image of a 3-torsion point of E gives a 3-torsion point of E'. In this paper, we determine the Weierstrass equation of E' of the form (1). In his paper [3], Miyawaki determined all the elliptic curves of prime power conductor which have a 3-torsion point. As an application, we determine all the isogeny relations among the elliptic curves of 3-power conductor which have a 3-torsion point.

Received July 20, 2011.
2010 *Mathematics Subject Classification.* Primary 14H52; Secondary 11G05.
Key words and phrases. elliptic curves, torsion points, Vélu's formula.

A classical question in number theory is to describe the positive integer m which can be written as the sum of two rational cubes. This leads one to study the curve $C_m : x^3 + y^3 = m$ for a non-zero integer m. We here consider the relation between the set of integral points of C_m and the elliptic curves E with $E[3] \simeq \mu_3 \oplus \mathbb{Z}/3\mathbb{Z}$.

2. Preliminaries

Let E be an elliptic curve over $\mathbb{Q}$ given by the equation (1) and $P = (0, 0)$. Note that the discriminant of E is given by $\Delta(E) = b^3(a^3 - 27b)$. Fix $Q = (x, y) \in E[3]$ with $x \neq 0$. Since $2Q = -Q$, we have

$$x^3 + \frac{a^2}{3}x^2 + abx + b^2 = 0. \tag{3}$$

Setting $x = z - \frac{a^2}{9}$, we get

$$z^3 + pz + q = 0,$$

where

$$p = -\frac{1}{27}a^4 + ab,\ q = \frac{2}{729}a^6 - \frac{1}{9}a^3b + b^2.$$

Set $f(z) = z^3 + pz + q$ and let $\Delta(f)$ denote its discriminant defined by $-4p^3 - 27q^2$. A computation shows the following result:

Lemma 2.1.

$$\Delta(f) = -\frac{\Delta(E)^2}{27b^4}.$$

Set

$$\begin{cases} u = \sqrt[3]{-\frac{q}{2} + \sqrt{-\frac{\Delta(f)}{4\cdot 27}}}, \\ v = \sqrt[3]{-\frac{q}{2} - \sqrt{-\frac{\Delta(f)}{4\cdot 27}}}. \end{cases}$$

Let ω be a primitive 3-th root of unity. By Caldano's formula, the solutions of the cubic equation (3) are

$$x = -\frac{a^2}{9} + u + v,\ -\frac{a^2}{9} + u\omega + v\omega^2,\ -\frac{a^2}{9} + u\omega^2 + v\omega. \tag{4}$$

By Lemma 2.1, we get

$$\begin{aligned} -\frac{q}{2} \pm \sqrt{-\frac{\Delta(f)}{4\cdot 27}} &= \frac{1}{2}\left(-q \pm \frac{|\Delta(E)|}{27b^2}\right) \\ &= \frac{1}{2}\left(-q \pm \frac{|b(a^3 - 27b)|}{27}\right) \\ &= -\frac{(a^3 - 27b)^2}{27^2},\ -\frac{a^3(a^3 - 27b)}{27^2}. \end{aligned}$$

Hence we have $u, v \in \mathbb{Q}(\sqrt[3]{a^3 - 27b})$. In particular, we have

$$u + v = -\frac{1}{9}\left(\sqrt[3]{(a^3 - 27b)^2} + a \cdot \sqrt[3]{a^3 - 27b}\right). \tag{5}$$

Let $\mathbb{Q}(E[3])$ denote the field generated by the points of $E[3]$. Taking $Q \in E[3]$ with $e_3(P, Q) = \omega$, we get a faithful representation $\rho : \mathrm{Gal}(\mathbb{Q}(E[3])/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_3)$ defined by

$$\begin{pmatrix} \sigma(P) \\ \sigma(Q) \end{pmatrix} = \rho(\sigma) \begin{pmatrix} P \\ Q \end{pmatrix}, \ \forall \sigma \in \mathrm{Gal}(\mathbb{Q}(E[3])/\mathbb{Q}).$$

By the exact sequence (2), we have $\rho = \left(\begin{smallmatrix} 1 & * \\ 0 & \chi \end{smallmatrix}\right)$ where χ is the cyclotomic character. We note that $\mathbb{Q}(\omega) \subseteq \mathbb{Q}(E[3])$ and the extension degree $[\mathbb{Q}(E[3]) : \mathbb{Q}]$ is divided by 3 (see [4] for details). Hence we have $\mathbb{Q}(E[3]) = \mathbb{Q}(\omega, \sqrt[3]{a^3 - 27b})$. Moreover, we have the following:

Proposition 2.2. *The exact sequence* (2) *of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$*-modules is split if and only if* $a^3 - 27b \in (\mathbb{Q}^\times)^3$.

3. The Weierstrass equation of E/μ_3 and isogeny relations

Let E be an elliptic curve with $E[3] \simeq \mu_3 \oplus \mathbb{Z}/3\mathbb{Z}$. In this section, we determine the Weierstrass equation of E/μ_3 of the form (1). As an application, we determine all the isogeny relations among the elliptic curves of 3-power conductor which have a 3-torsion point.

3.1. The Weierstrass equation of E/μ_3

Let C be a subgroup of an elliptic curve E. Vélu in [5] gives an explicit formula for determining the equation of the isogeny $E \to E/C$ and the Weierstrass equation of the curve E/C. We shall review here Vélu's formula. Let E be an elliptic curve given by a Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Let S be a set of representatives for $(C \setminus \{O\})/\{\pm 1\}$, where O is the point at infinity. We define two functions as follows: For a point $Q = (x, y)$ on $E \setminus \{O\}$,

$$\begin{cases} g^x(Q) &= 3x^2 + 2a_2x + a_4 - a_1y, \\ g^y(Q) &= -2y - a_1x - a_3. \end{cases}$$

Set

$$\begin{aligned} t(Q) &= \begin{cases} g^x(Q) & \text{if } Q = -Q \text{ on } E, \\ 2g^x(Q) - a_1g^y(Q) & \text{otherwise,} \end{cases} \\ u(Q) &= (g^y(Q))^2, \\ t &= \textstyle\sum_{Q \in S} t(Q), \\ w &= \textstyle\sum_{Q \in S} (u(Q) + x(Q)t(Q)). \end{aligned}$$

Then the Weierstrass equation of the elliptic curve E/C is given by

$$Y^2 + A_1XY + A_3Y = X^3 + A_2X^2 + A_4X + A_6,$$

where $A_1 = a_1,\ A_2 = a_2,\ A_3 = a_3,\ A_4 = a_4 - 5t,\ A_6 = a_6 - (a_1^2 + 4a_2)t - 7w$.

Let E be an elliptic curve $\mathbb{Q}$ given the equation (1) with $a^3 - 27b = -k^3 \in (\mathbb{Q}^\times)^3$. By Proposition 2.2, we have $E[3] \simeq \mu_3 \oplus \mathbb{Z}/3\mathbb{Z}$. Let $Q = (x, y) \in E[3]$ with $x = -\frac{a^2}{9} + u + v$ (see §2 for u and v). Then we can see $\mu_3 \simeq \langle Q \rangle \subseteq E[3]$. In the notation as above, we take $S = \{Q\}$ as a set of representatives for $(\mu_3 \setminus \{O\})/\{\pm 1\}$. By (5), we have

$$x = -\frac{1}{9}(a^2 + k^2 - ak) = -\frac{3b}{a+k}.$$

A computation shows that we have

$$t = -\frac{bk(a-2k)}{a+k},\ w = \frac{3b^2k(a-3k)}{(a+k)^2}.$$

Then the Weierstrass equation of the elliptic curve E/μ_3 is as follows:

$$Y^2 + aXY + bY = X^3 + A_4X + A_6,$$

where $A_4 = 5t,\ A_6 = -a^2t - 7w$. Let ϕ be the isogeny $E \to E/\mu_3$. We have

$$\phi(P) = \left(-\frac{t(a-t)}{3}, \frac{at(2a-t)}{9}\right),$$

where $P = (0, 0)$ is the 3-torsion point of E (see [5] for details). The change of variables $X \mapsto X - \frac{t(a-t)}{3},\ Y \mapsto Y + \frac{at(2a-t)}{9}$ gives the equation

$$Y^2 + aXY + \frac{(a+k)^3}{27}Y = X^3 - k(a-k)X^2 - \frac{k(a+k)^3}{27}.$$

After the change of variable $Y \mapsto Y - kX$, we obtain the equation of the form (1) as follows:

$$Y^2 + (a-2k)XY + \frac{(a+k)^3}{27}Y = X^3.$$

In summary, we have the following:

Proposition 3.1. *Let E be an elliptic curve over $\mathbb{Q}$ given by the equation* (1) *with $a^3 - 27b = -k^3 \in (\mathbb{Q}^\times)^3$. Then the Weierstrass equation of the elliptic curve E/μ_3 of the form* (1) *is as follows*:

$$E/\mu_3 : Y^2 + (a-2k)XY + \frac{(a+k)^3}{27}Y = X^3.$$

3.2. Application

By applying Proposition 3.1, we determine all the isogeny relations among the elliptic curves of 3-power conductor which have a 3-torsion point. In his paper [3], Miyawaki determined all such curves. In Table 1, we list all such curves. For each curve, the data given are Miyawaki's code E^i, coefficients $a,\ b$ of the equation (1), the discriminant Δ, the conductor N and the j-invariant j (see [3] for details).

TABLE 1. Elliptic curves of 3-power conductor which have a 3-torsion point

E^i	a	b	Δ	N	j
E^3	0	1	-3^3	3^3	0
E^4	-6	1	-3^5	3^3	$-2^{15}\cdot 3\cdot 5^3$
E^5	0	3	-3^7	3^5	0
E^8	6	9	-3^9	3^3	0
E^9	0	9	-3^{11}	3^5	0

Let E be one of elliptic curves E^3, E^8. Since $a^3 - 27b \in (\mathbb{Q}^\times)^3$, it follows from Proposition 2.2 that $E[3]$ is split as $\mu_3 \oplus \mathbb{Z}/3\mathbb{Z}$. We consider the Weierstrass equation of E/μ_3 as follows:

- In the case $E = E^3$, we have
$$E^3/\mu_3 : Y^2 - 6XY + Y = X^3$$
by Proposition 3.1. Therefore we have $E^4 = E^3/\mu_3$.
- In the case $E = E^8$, we have
$$E^8/\mu_3 : Y^2 + 27Y = X^3$$
by Proposition 3.1. The change of variables $X \mapsto 9X,\ Y \mapsto 27Y$ gives the equation $Y^2 + Y = X^3$. Therefore we have $E^3 = E^8/\mu_3$.

Therefore we have
$$E^8 \sim E^3 = E^8/\mu_3 \sim E^4 = E^3/\mu_3.$$
Since the conductor is an isogeny invariant, elliptic curves E^5, E^9 are not isogeneous to elliptic curves E^3, E^4, E^8. Since $\mathrm{rank}(E^5) = 0$ and $\mathrm{rank}(E^9) = 1$, we see that E^5 is not isogeneous to E^9.

Remark. We can determine all the elliptic curves E over $\mathbb{Q}$ with $E[3] \simeq \mu_3 \oplus \mathbb{Z}/3\mathbb{Z}$ and $j \in \mathbb{Z}$. In his paper [1], Frey determined all the elliptic curves having a 3-torsion point with $j \in \mathbb{Z}$. In Table 2, we list all such curves of the form (1).

TABLE 2. Elliptic curves having a 3-torsion point with $j \in \mathbb{Z}$

The Weierstrass equation of the form (1)	The j-invariant
$y^2 + 2ty = x^3\ (t \neq 0)$	0
$y^2 + 2xy + \frac{8}{27+3^n}y = x^3\ (0 \leq n \leq 6)$	$3^{6-n}(1+3^{n-1})^3(1+3^{n-3})$
$y^2 + 2xy + \frac{8}{27-3^n}y = x^3\ (0 \leq n \leq 6, n \neq 3)$	$3^{6-n}(1-3^{n-1})^3(3^{n-3}-1)$
$y^2 + 2xy - \frac{4}{27}y = x^3$	$2^4 3^3 5^3$

By Table 2 and Proposition 2.2, the Weierstrass equation of an elliptic curve E with $E[3] \simeq \mu_3 \oplus \mathbb{Z}/3\mathbb{Z}$ and $j \in \mathbb{Z}$ is either equal to

$$y^2 + k^3 y = x^3 \text{ for } k \in \mathbb{Q}^\times \tag{6}$$

or

$$y^2 + 2xy + \frac{1}{3}y = x^3. \tag{7}$$

We see that an elliptic curve given by the equation (6) is isomorphic to the elliptic curve E^3 defined in Table 1. Moreover, we see that an elliptic curve given by the equation (7) is isomorphic to the elliptic curve E^8 defined in Table 1. Therefore an elliptic curve E with $E[3] \simeq \mu_3 \oplus \mathbb{Z}/3\mathbb{Z}$ and $j \in \mathbb{Z}$ is either equal to E^3 or E^8.

4. Relation with the curve $x^3 + y^3 = m$

For a non-zero integer m, let C_m denote the curve defined by the equation $x^3 + y^3 = m$. In this section, we study the relation between the set $C_m(\mathbb{Z})$ of integral points of C_m and the elliptic curves E over $\mathbb{Q}$ with $E[3] \simeq \mu_3 \oplus \mathbb{Z}/3\mathbb{Z}$. For an elliptic curve E with a 3-torsion point, we get the Weierstrass equation of E of the form (1) with $a, b \in \mathbb{Z}$ by doing a change of variables. In this section, we denote by $E(a, b)$ an elliptic curve defined by the equation (1) with $a, b \in \mathbb{Z}$. By Proposition 2.2, we note that $E(a, b)[3] \simeq \mu_3 \oplus \mathbb{Z}/3\mathbb{Z}$ if and only if $a^3 - 27b = -k^3$ for some non-zero integer k. Therefore we have $(a, k) \in C_{27b}(\mathbb{Z})$ if $E(a, b)[3] \simeq \mu_3 \oplus \mathbb{Z}/3\mathbb{Z}$. For a non-zero integer b, we can give a map

$$\phi : C_{27b}(\mathbb{Z}) \to \{E(a, b) \mid a \in \mathbb{Z} \text{ and } E(a, b)[3] \simeq \mu_3 \oplus \mathbb{Z}/3\mathbb{Z}\}$$

defined by $\phi(\alpha, \beta) = E(\alpha, b)$ with $\alpha^3 + \beta^3 = 27b$. We note that the Weierstrass equation of $E(\alpha, b)$ given by the equation (1) is minimal if $(\alpha, \beta) \in C_{27b}(\mathbb{Z})$ with $\gcd(\alpha, \beta) = 1$ (see [2, Section 1]).

We consider the condition that $E(a, b)$ is isomorphic to $E(a', b')$ over $\mathbb{Q}$ with $a, b, a', b' \in \mathbb{Z}$. For an elliptic curve E over a field K given by a Weierstrass equation, we note that every isomorphism of E to another elliptic curve over K given by a Weierstrass equation can be given by a change of variables of the form $x \mapsto u^2x + r,\ y \mapsto u^3y + u^2sx + t$ with $r, s, t, u \in K$ (see [4]). Therefore we can see that

$$E(a, b) \simeq E(a', b') \Longleftrightarrow a = ua', b = u^3b' \text{ for some } u \in \mathbb{Q}^\times.$$

Let T denote the set of positive integers. We define an equivalence relation on the set $\coprod_{b \in T} C_{27b}(\mathbb{Z})$ as follows: For $(\alpha, \beta),\ (\alpha', \beta') \in \coprod_{b \in T} C_{27b}(\mathbb{Z})$, we define

$$(\alpha, \beta) \sim (\alpha', \beta') \Longleftrightarrow \alpha = u\alpha', \beta = u\beta' \text{ for some } u \in \mathbb{Q}^\times.$$

Then we have the following:

Theorem 4.1. *We have an isomorphism*

$$\Phi : \coprod_{b \in T} C_{27b}(\mathbb{Z})/\sim \longrightarrow \{\text{elliptic curves } E \text{ over } \mathbb{Q} \text{ with } E[3] \simeq \mu_3 \oplus \mathbb{Z}/3\mathbb{Z}\}$$

as sets defined by $(\alpha, \beta) \mapsto E(\alpha, b)$ *for* $(\alpha, \beta) \in C_{27b}(\mathbb{Z})$.

TABLE 3. P_n and nQ for some $n \geq 1$

Points of C_m	Points of E_m
$P_1 = (6, -3)$	$Q = (756, -20412)$
$P_2 = (5, 4)$	$2Q = (252, -756)$
$P_3 = \left(-\frac{51}{38}, \frac{219}{38}\right)$	$3Q = (513, 10935)$
$P_4 = \left(-\frac{1256}{61}, \frac{1265}{61}\right)$	$4Q = (15372, 1199996)$
$P_5 = \left(\frac{270813}{40049}, -\frac{197646}{40049}\right)$	$5Q = \left(\frac{104436}{841}, -\frac{1062465012}{24389}\right)$
$\vdots$	$\vdots$

For a non-zero integer m, we note that the curve C_m is isomorphic to an elliptic curve

$$E_m : Y^2 = X^3 - 432m^2,$$

where

$$X = \frac{12m}{y + x}, \quad Y = 36m\frac{y - x}{y + x}.$$

Take $b = 7$ and $m = 27b$. Then the curve C_m has a point $P_1 = (6, -3)$. Let $Q = (756, -20412)$ be a point of E_m corresponding to the point P_1. We denote by P_n a point of C_m corresponding to the point nQ of E_m for $n \geq 1$. In Table 3, we list P_n and nQ for some $n \geq 1$. As shown in Table 3, we see that the order of the point Q is infinite by [4, Ch. 8, Corollary 7.2]. Since P_1, $P_2 \in C_{27b}(\mathbb{Z})$, the map Φ gives elliptic curves $E(6, 7)$, $E(5, 7)$. Although $P_3 \notin C_{27b}(\mathbb{Z})$, we have $P_3' = (-51, 219) \in C_{27b'}(\mathbb{Z})$ with $b' = 38b$ and hence the map Φ gives an elliptic curve $E(-51, b')$. Similarly, points P_4 and P_5 give elliptic curves E with $E[3] \simeq \mu_3 \oplus \mathbb{Z}/3\mathbb{Z}$ using the map Φ. Therefore we can construct infinitely many elliptic curves E over $\mathbb{Q}$ with $E[3] \simeq \mu_3 \oplus \mathbb{Z}/3\mathbb{Z}$ in this way.

References

[1] G. Frey, *Some remarks concerning points of finite order on elliptic curves over global fields*, Ark. Mat. **15** (1977), no. 1, 1–19.

[2] T. Hadano, *Elliptic curves with a torsion point*, Nagoya Math. J. **66** (1977), 99–108.

[3] I. Miyawaki, *Elliptic curves of prime power conductor with $\mathbb{Q}$-rational points of finite order*, Osaka J. Math. **10** (1973), 309–323.

[4] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Math. **106**, Springer-Verlag, Berlin-Heidelberg New York, 1994.

[5] J. Vélu, *Isogénis entre courbs elliptiques*, C. R. Acad. Sci. Paris Sér. A-B (1971), 238–241.

FUJITSU LABORATORIES LTD.
4-1-1, KAMIKODANAKA, NAKAHARA-KU
KAWASAKI 211-8588, JAPAN
E-mail address: myasuda@labs.fujitsu.com