

## CONSTRUCTION OF HIGH-RANK ELLIPTIC CURVES WITH A NONTRIVIAL TORSION POINT

KOH-ICHI NAGAO

ABSTRACT. We construct a family of infinitely many elliptic curves over  $\mathbb{Q}$  with a nontrivial rational 2-torsion point and with rank  $\geq 6$ , which is parametrized by the rational points of an elliptic curve of rank  $\geq 1$ .

### 1. INTRODUCTION

The problem of constructing high-rank elliptic curves over  $\mathbb{Q}$  with a nontrivial torsion point has been studied by several people. Among them, Kretschmer [1] found an example of rank  $\geq 10$  and Zimmer and Schneiders [6] found two examples of rank  $\geq 11$ . Regarding the problem of constructing infinitely many such curves, Mestre [3] found elliptic curves of the form  $y^2 = x^3 + kx$  (where  $(0,0)$  is a 2-torsion point) with rank  $\geq 4$ . In this note, we show the following.

**Theorem 1.** *There are infinitely many elliptic curves over  $\mathbb{Q}$  with a nontrivial 2-torsion point and with rank  $\geq 6$ .*

### 2. THE CURVE $Y^2 = aX^4 + bX^2 + c$

In this note, high-rank elliptic curves of the form  $Y^2 = aX^4 + bX^2 + c$  are treated. First, we show that curves of this form have nontrivial 2-torsion points.

**Lemma 2.1.** *Let  $E : Y^2 = aX^4 + bX^2 + c$  be a curve of genus one over a field  $K$ . Assume that  $E$  has a  $K$ -rational point  $(x, y)$  and regard  $E$  as an elliptic curve whose group structure is given by  $(x, y)$  as origin. Then one has  $2(-x, -y) = 0$ .*

*Sketch of the proof.* We denote the two points at infinity on  $E$  by  $\infty$  and  $\infty'$ . More precisely,  $\infty$  and  $\infty'$  are written as  $(0, \sqrt{a})$ ,  $(0, -\sqrt{a})$ , respectively, on the dual model of  $E$  given by the equation  $Y^2 = cX^4 + bX^2 + a$ . Then we have

$$(1) \quad 2\infty - 2\infty' = \operatorname{div}(-Y + \sqrt{a}X^2 + \frac{b}{2\sqrt{a}}) \sim 0,$$

$$(2) \quad (x, y) + (x, -y) - \infty - \infty' = \operatorname{div}(X - x) \sim 0,$$

$$(3) \quad (x, -y) + (-x, -y) - 2\infty = \operatorname{div}(Y + \sqrt{a}X^2 - y + \sqrt{a}x^2) \sim 0,$$

where the symbol  $\sim$  means the relation of rational equivalence class of divisors. By eliminating  $(x, -y)$  from (2) and (3), we have

$$(-x, -y) - (x, y) \sim \infty - \infty',$$

---

Received by the editor June 16, 1994 and, in revised form, November 1, 1994 and November 13, 1995.

1991 *Mathematics Subject Classification.* Primary 11G05, 11D25; Secondary 11Y50.

*Key words and phrases.* Elliptic curve.

©1997 American Mathematical Society

and hence we obtain

$$2(-x, -y) - 2(x, y) \sim 2\infty - 2\infty' \sim 0,$$

which completes the proof.  $\square$

In §3, we will construct an elliptic curve over  $\mathbb{Q}(T)$  of the form  $\mathcal{E} : Y^2 = a(T)X^4 + b(T)X^2 + c(T)$ , which contains at least six  $\mathbb{Q}(T)$ -rational points  $P_1, \dots, P_6$ . Further, we consider  $\mathcal{E}$  as a curve defined over the function field  $\mathbb{Q}(C)$ , where  $C$  is the curve defined by the equation  $S^2 = a(T)$ . So the two points  $\infty$  and  $\infty'$  at infinity of  $\mathcal{E}$  become  $\mathbb{Q}(C)$ -rational points and we can choose the point  $\infty$  as the origin. We know the point  $\infty'$  is a nontrivial 2-division point, and we can use all six points  $P_1, \dots, P_6$  to obtain independent points. It is remarked that a rational point  $p = (t, s)$  on the curve  $C$  gives rise to an elliptic curve over  $\mathbb{Q}$ , which is obtained from  $\mathcal{E}$  by the specialization  $(T, S) \rightarrow (t, s)$ . Thus, if  $C$  has infinitely many rational points, we can obtain infinitely many elliptic curves over  $\mathbb{Q}$  with a nontrivial 2-torsion point and rank  $\geq 6$ .

### 3. CONSTRUCTION

For any 6-tuple  $A = (a_1, a_2, a_3, a_4, a_5, a_6) \in \mathbb{A}^6(\mathbb{Q}(T))$ , let

$$p_A(X) = (X^2 - a_1^2)(X^2 - a_2^2)(X^2 - a_3^2)(X^2 - a_4^2)(X^2 - a_5^2)(X^2 - a_6^2) \in \mathbb{Q}(T)[X].$$

Then we see easily that there are uniquely determined (up to the signature of  $r_A$ ) polynomials  $g_A(X), r_A(X) \in \mathbb{Q}(T)[X]$  satisfying  $\deg g_A(X) = 6$ ,  $\deg r_A(X) \leq 4$  and  $p_A(X) = g_A(X)^2 - r_A(X)$ . (We note that  $g_A(X)$  and  $r_A(X)$  are contained in  $\mathbb{Q}(T)[X^2]$ .) In this note, we only treat the case when  $\deg r_A(X)$  is 4 and the equation  $r_A(X) = 0$  has no double root. Then the curve  $Y^2 = r_A(X)$  is an elliptic curve over  $\mathbb{Q}(T)$ , which is denoted by  $\mathcal{E}_A$ , and contains the six  $\mathbb{Q}(T)$ -rational points  $P_i = (a_i, g_A(a_i))$  ( $i = 1, \dots, 6$ ).

By Lemma 2.1, we see that  $\mathcal{E}_A$  is an elliptic curve over  $\mathbb{Q}(T)$  with nontrivial 2-torsion points since  $r_A(X)$  is an element of  $\mathbb{Q}(T)[X^2]$ . When  $A$  is of the form  $(\pm T + \alpha_1, \dots, \pm T + \alpha_6)$  ( $\alpha_i \in \mathbb{Q}$ ), the coefficient of  $X^4$  in  $r_A(X)$  seems to be (however we cannot prove it) a quartic polynomial of  $T$ , which will be important for our purpose.

Thus we consider the case  $A = (T + 1, T + 2, T + 3, -T + 5, -T + 6, -T + 9)$ . Then the equation of  $\mathcal{E} = \mathcal{E}_A$  is written as

$$\begin{aligned} Y^2 = & 4((-311T^4 - 2814T^3 + 58104T^2 - 239744T + 297024)X^4 \\ & + (622T^6 - 1848T^5 + 2380T^4 - 90410T^3 - 6696T^2 + 2080960T - 3928704)X^2 \\ & - 311T^8 + 4662T^7 - 4288T^6 - 171446T^5 + 410752T^4 \\ & + 2203272T^3 - 5965776T^2 - 10364480T + 28872256) \end{aligned}$$

and  $P_i$  are as follows:

$$\begin{aligned} P_1 &= (T + 1, 2(-200T^3 + 711T^2 + 1512T - 5024)), \\ P_2 &= (T + 2, 4(-73T^3 + 192T^2 + 714T - 2116)), \\ P_3 &= (T + 3, 2(12T^3 + 323T^2 + 304T - 4192)), \\ P_4 &= (-T + 5, 2(316T^3 - 3165T^2 + 10080T - 10784)), \\ P_5 &= (-T + 6, 4(159T^3 - 1832T^2 + 6902T - 8252)), \\ P_6 &= (-T + 9, 2(-300T^3 + 5411T^2 - 27128T + 40736)). \end{aligned}$$

Let us consider the elliptic curve

$$C : S^2 = -311T^4 - 2814T^3 + 58104T^2 - 239744T + 297024$$

in the  $(T, S)$ -plane.

**Lemma 3.1.** *The curve  $C$  contains infinitely many rational points.*

*Proof.* By a direct calculation, we see that  $C$  has rational points whose  $T$ -coordinates are  $-4, -8/3, -13/4, 16/5, 24/5, 20/7, 37/8, 29/12, 43/12, 32/13, 232/47, 272/79, -230/113$ . By the theorem of Mazur [2], stating that the number of torsion points of an elliptic curve over  $\mathbb{Q}$  is  $\leq 16$ , we see that  $C$  has infinitely many rational points since  $C$  has more than 26 rational points.  $\square$

**Proposition 3.1.** *The points  $P_1, P_2, \dots, P_6$  are independent  $\mathbb{Q}(C)$ -rational points when the group structure is given by  $\infty$  as origin.*

We give the proof of Proposition 3.1 in the next section. Now, by a theorem of Silvermann [5, Theorem 20.3], which says the specialization map is injective for all but finitely many points  $p \in C$ , and by Proposition 3.1, we obtain easily that the rank of curves which are obtained by the specialization from  $\mathcal{E}$  by a rational point  $p \in C(\mathbb{Q})$  is  $\geq 6$  for all but finitely many cases. Hence we get Theorem 1.

#### 4. INDEPENDENCE OF RATIONAL POINTS

To prove Proposition 3.1, since the specialization map is always a homomorphism, we have only to show that there exists a rational point  $p$  on  $C$  such that  $P_1, \dots, P_6$  are specialized to six independent rational points on the elliptic curve obtained by the specialization from  $\mathcal{E}$  by  $p$ . We claim this is the case for  $p = (272/79, 11067/26)$ . Now, we consider the case that  $E^*$  is the elliptic curve obtained by the specialization  $(T, S) \rightarrow (272/79, 11067/26)$  from  $\mathcal{E}$ . Let the  $p_i^*$ 's be the rational points on  $E^*$  obtained by the above specialization from  $P_i$ . The equation of  $E^*$  and the rational points  $p_i^*$ 's are written as follows (for simplicity, we change the coordinate  $(1008/38950081) \cdot Y$  to  $Y$ ):

$$\begin{aligned} E^* : Y^2 &= 10817567046049X^4 - 339753752030234X^2 + 3686523169893001, \\ p_1^* &= (351/79, 34570084), \\ p_2^* &= (430/79, -55818951), \\ p_3^* &= (509/79, 90688524), \\ p_4^* &= (123/79, -54096988), \\ p_5^* &= (202/79, 43904487), \\ p_6^* &= (439/79, -59247156). \end{aligned}$$

**Lemma 4.1.** *Let  $E^* : Y^2 = a^2X^4 + bX^2 + c$  ( $a, b, c \in K$ ) be an elliptic curve over a field  $K$ . Then  $E^*$  is  $K$ -isomorphic to the curve  $E : Y^2 = X(X^2 - 2bX + b^2 - 4a^2c)$ , which has a nontrivial rational 2-torsion  $(0, 0)$ , by the map  $\phi : E^* \rightarrow E$ ,*

$$\phi(X, Y) = (-2aY + 2a^2X^2 + b, 4a^2XY - 4a^3X^3 - 2abX).$$

(We note that the two points at infinity of  $E^*$  map respectively to the unique point at infinity and the point of coordinate  $(0, 0)$  of  $E$ .)

*Proof.* See Mordell [4, p.77].  $\square$

We remark that this lemma gives another proof of the fact that  $\mathcal{E}_A$  has a non-trivial  $\mathbb{Q}(C)$ -rational 2-torsion point.

Using Lemma 4.1, we see easily that a Weierstrass model of  $E^*$ , which is denoted by  $E$ , and the rational points  $p_i = \phi(p_i^*)$  can be written as follows:

$$\begin{aligned}
 E : Y^2 &= X(X^2 + 679507504060468X - 44084234209900772519029117440), \\
 p_1 &= (-140066013780432, 4093620582907949270112), \\
 p_2 &= (668400902705280, -23931679912802873126400), \\
 p_3 &= (-38170471955952, 1617755981603108309088), \\
 p_4 &= (68543386187360, -702002032096036284480), \\
 p_5 &= (-487106389903140, 8192998933658320758480), \\
 p_6 &= (718064066419488, -26247951601418953547712).
 \end{aligned}$$

Now, in order to show the independence of  $p_1, \dots, p_6$  on  $E$ , we need notation and two lemmas. Let  $E : Y^2 = X^3 + aX^2 + bX$  be an elliptic curve over  $\mathbb{Q}$ . Then  $E$  is 2-isogenous to  $E' : Y^2 = X^3 - 2aX^2 + (a^2 - 4b)X$  by the map  $\psi : E' \rightarrow E$ ,  $\psi(x, y) = (y^2/4x^2, y(a^2 - 4b - x^2)/8x^2)$ . Let  $\alpha : E(\mathbb{Q}) \rightarrow \mathbb{Q}^*/\mathbb{Q}^{*2}$  be the map defined by

$$\alpha(P) = \begin{cases} 1 \cdot \mathbb{Q}^{*2}/\mathbb{Q}^{*2} & \text{if } P = \infty, \\ b \cdot \mathbb{Q}^{*2}/\mathbb{Q}^{*2} & \text{if } P = (0, 0), \\ x \cdot \mathbb{Q}^{*2}/\mathbb{Q}^{*2} & \text{if } P = (x, y), P \neq \infty, (0, 0), \end{cases}$$

and  $\alpha' : E'(\mathbb{Q}) \rightarrow \mathbb{Q}^*/\mathbb{Q}^{*2}$  the map defined by

$$\alpha'(P) = \begin{cases} 1 \cdot \mathbb{Q}^{*2}/\mathbb{Q}^{*2} & \text{if } P = \infty, \\ (a^2 - 4b) \cdot \mathbb{Q}^{*2}/\mathbb{Q}^{*2} & \text{if } P = (0, 0), \\ x \cdot \mathbb{Q}^{*2}/\mathbb{Q}^{*2} & \text{if } P = (x, y), P \neq \infty, (0, 0). \end{cases}$$

(We consider  $\mathbb{Q}^*/\mathbb{Q}^{*2}$  as a vector space over  $\mathbb{Z}/2\mathbb{Z}$ .)

In the following, we assume that  $E(\mathbb{Q})_{\text{tor}} = E'(\mathbb{Q})_{\text{tor}} = \{\infty, (0, 0)\}$ .

**Lemma 4.2.** *The  $\mathbb{Q}$ -rank of  $E$  is equal to*

$$\text{rank}_{\mathbb{Z}/2\mathbb{Z}}(\alpha(E(\mathbb{Q}))) + \text{rank}_{\mathbb{Z}/2\mathbb{Z}}(\alpha'(E'(\mathbb{Q}))) - 2.$$

*Proof.* See Zimmer [7, Theorem 8.1]. □

More precisely, we easily obtain the following lemma.

**Lemma 4.3.** *Let  $G$  be a subgroup of  $E(\mathbb{Q})$ . Then the  $\mathbb{Q}$ -rank of  $G$  is greater than, or equal to,  $\text{rank}_{\mathbb{Z}/2\mathbb{Z}}(\alpha(G)) + \text{rank}_{\mathbb{Z}/2\mathbb{Z}}(\alpha'(\psi^{-1}(G))) - 2$ .*

We apply Lemma 4.3 to our curve  $E$  and the subgroup  $G = \langle (0, 0), p_1, p_2, \dots, p_6 \rangle$ . In this case, the equation of  $E'$  is written as

$$Y^2 = X(X^2 - 1359015008120936X + 638067384914090025583516848784).$$

We see easily that  $E(\mathbb{Q})_{\text{tor}} = E'(\mathbb{Q})_{\text{tor}} = \{\infty, (0, 0)\}$  by Zimmer [7, Theorem 7.3]. Thus, the assumption of Lemma 4.3 holds.

By a direct calculation we have

$$\begin{aligned}\alpha((0, 0)) &= -2 \cdot 5 \cdot 7 \cdot 19 \cdot 47 \cdot 67 \cdot 83 \cdot 139 \cdot 181 \cdot \mathbb{Q}^{*2}/\mathbb{Q}^{*2}, \\ \alpha(p_1) &= -19 \cdot 79 \cdot 83 \cdot 139 \cdot \mathbb{Q}^{*2}/\mathbb{Q}^{*2}, \\ \alpha(p_2) &= 2 \cdot 3 \cdot 5 \cdot 47 \cdot 79 \cdot 83 \cdot 181 \cdot \mathbb{Q}^{*2}/\mathbb{Q}^{*2}, \\ \alpha(p_3) &= -3 \cdot 7 \cdot 19 \cdot 67 \cdot 79 \cdot 181 \cdot \mathbb{Q}^{*2}/\mathbb{Q}^{*2}, \\ \alpha(p_4) &= 2 \cdot 5 \cdot 7 \cdot 19 \cdot 47 \cdot 79 \cdot 139 \cdot \mathbb{Q}^{*2}/\mathbb{Q}^{*2}, \\ \alpha(p_5) &= -3 \cdot 5 \cdot 7 \cdot 47 \cdot 67 \cdot 79 \cdot 83 \cdot \mathbb{Q}^{*2}/\mathbb{Q}^{*2}.\end{aligned}$$

So they are independent elements in the  $\mathbb{Z}/2\mathbb{Z}$ -vector space  $\mathbb{Q}^*/\mathbb{Q}^{*2}$ . On the other hand, let

$$p' = (32608658554556738404/169, 185553135139334125323174897696/2197)$$

be the rational point on  $E'$  such that  $\psi(p') = p_1 + p_2 + p_3 + p_4 + p_5 + p_6$ . Then we have

$$\begin{aligned}\alpha'(p') &= 627169 \cdot \mathbb{Q}^{*2}/\mathbb{Q}^{*2}, \\ \alpha'((0, 0)) &= 17 \cdot 7103 \cdot 48679 \cdot 627169 \cdot \mathbb{Q}^{*2}/\mathbb{Q}^{*2}.\end{aligned}$$

So they are independent in  $\mathbb{Q}^*/\mathbb{Q}^{*2}$ . Using Lemma 4.3, we can now conclude that  $p_1, \dots, p_6$  are independent points on  $E$ , and the proof is complete.

*Remark.* Using the computer system PARI, we can compute the determinant of the matrix of height pairings  $\langle p_i, p_j \rangle$  ( $1 \leq i, j \leq 6$ ). Since this determinant is 48107.7640..., the points  $p_1, \dots, p_6$  are independent on  $E$ , which gives another proof of Proposition 3.1.

#### ACKNOWLEDGMENT

I should like to express my thanks to Professor Yoshio Mimura at the Osaka Electro and Communication University and Professor Noburo Ishii at the Osaka Prefecture University for their useful advice.

#### REFERENCES

1. T. J. Kretschmer, *Construction of elliptic curves with large rank*, Math. Comp. **46** (1986), 627–635. MR **87g**:11069
2. B. Mazur, *Rational points on modular curves*, Lecture Notes in Math. **601** (1977), 107–148. MR **56**:8579
3. J. -F. Mestre, *Rang de courbes elliptiques d'invariant donné*, C. R. Acad. Sci. **314** (1992), 919–922. MR **93e**:11075
4. L. J. Mordell, *Diophantine equations*, Academic Press, London, 1969. MR **40**:2600
5. J. H. Silverman, *The arithmetic theory of elliptic curves*, Graduate Texts in Math. **106**, Springer-Verlag, New-York, 1986. MR **87g**:11070
6. H. G. Zimmer and U. Schneiders, *The rank of elliptic curves upon quadratic extension*, in *Computational Number Theory* (eds. A. Pethö, M. E. Pohst, H. C. Williams, H. G. Zimmer), Walter de Gruyter, Berlin, 1991, pp.239–260. MR **92m**:11053
7. H. G. Zimmer, *Computational aspects of the theory of elliptic curves*, in *Number theory and applications* (ed. R. A. Mollin), Kluwer Academic Publishers, Dordrecht, 1989, pp.279–324. MR **92g**:11057

SHIGA POLYTECHNIC COLLEGE, 1414 FURUKAWA CHO, OH-MIHACHIMAN SHIGA 523, JAPAN  
E-mail address: nagao@shiga-pc.ac.jp