Functiones et Approximatio
56.1 (2017), 61–65
doi: 10.7169/facm/1591

FAMILY OF ELLIPTIC CURVES WITH GOOD REDUCTION EVERYWHERE OVER NUMBER FIELDS OF GIVEN DEGREE

Nao Takeshi

Abstract: We give families of elliptic curves having good reduction everywhere over number fields which are generated by their j-invariants of given degree.

Keywords: elliptic curves, everywhere good reduction, j-invariants.

It is known that the j-invariant $j(E)$ of an elliptic curve E defined over a number field K is an algebraic integer if and only if there exists a finite extension F/K such that E attains good reduction everywhere over F (cf. [3, Proposition VII.5.5]). It follows that every algebraic integer α belongs to $j(\mathcal{E}_F^0)$ for some extension field F of $\mathbb{Q}(\alpha)$. Here, $\mathcal{E}_F$ is the set of isomorphism classes of elliptic curves defined over F, $\mathcal{E}_F^0$ is the subset of $\mathcal{E}_F$ defined by

$$\mathcal{E}_F^0 = \{E \in \mathcal{E}_F : \ E \text{ has good reduction everywhere over } F\}$$

and $j(\mathcal{E}_F^0) = \{j(E) : \ E \in \mathcal{E}_F^0\}$. However, we have $\alpha \notin j(\mathcal{E}_{\mathbb{Q}(\alpha)}^0)$ for many algebraic integers α, because it is known that $\mathcal{E}_K^0$ is a finite set for any K. For example, we have $\alpha \notin j(\mathcal{E}_{\mathbb{Q}(\alpha)}^0)$ for any rational integer α, because there exist no elliptic curves having good reduction everywhere over $\mathbb{Q}$, that is, $\mathcal{E}_{\mathbb{Q}}^0 = \emptyset$. We consider the following problem.

Problem. *Find algebraic integers α such that $\alpha \in j(\mathcal{E}_{\mathbb{Q}(\alpha)}^0)$, i.e., $\alpha = j(E)$ for some elliptic curve E defined over $\mathbb{Q}(\alpha)$ and having good reduction everywhere over $\mathbb{Q}(\alpha)$.*

In [2], Rohrlich considered a specific case of the problem. He gave a necessary and sufficient condition for an algebraic integer α to be the j-invariant of an elliptic curve $E \in \mathcal{E}_{\mathbb{Q}(\alpha)}^0$ with complex multiplication by the ring of integers of an imaginary

2010 Mathematics Subject Classification: primary: 11G05, 14H52; secondary: 11R04

quadratic field. By his result, it is immediately shown that there exist infinitely many algebraic integers α satisfying $\alpha \in j(\mathcal{E}^0_{\mathbb{Q}(\alpha)})$. However, since there exist only finitely many imaginary quadratic fields with given class number, his result gives a finite number of algebraic integers $\alpha \in j(\mathcal{E}^0_{\mathbb{Q}(\alpha)})$ of given degree. In this paper, we prove the following theorem.

Theorem 1. *For any $n \geqslant 2$, there exist infinitely many algebraic integers α of degree n such that $\alpha \in j(\mathcal{E}^0_{\mathbb{Q}(\alpha)})$.*

Theorem 1 is known to be true for the case $n \leqslant 3$. Tate showed that a root α of the polynomial $x^2 - 1728x + a^{12}$ with $a \in \mathbb{Z}$ prime to 6 satisfies $\alpha \in j(\mathcal{E}^0_{\mathbb{Q}(\alpha)})$. Actually, the elliptic curve defined by the equation

$$y^2 + xy = x^3 - \frac{36}{\alpha - 1728}x - \frac{1}{\alpha - 1728} \tag{1}$$

has the j-invariant equal to α and has good reduction everywhere over the quadratic field $\mathbb{Q}(\alpha)$ (see the remark following the proof of Proposition 2). The author gave a family of elliptic curves having good reduction everywhere over cubic fields with cubic j-invariants ([4, Theorem 1.2]).

We give two families of elliptic curves having good reduction everywhere in Propositions 2 and 3. The elliptic curves in Proposition 2 are inspired by the example of Tate, and Proposition 3 is a straightforward generalization of the result of the author.

Proposition 2. *Let $n, a \in \mathbb{Z}$ with $n \geqslant 2$. Assume that a satisfies $a^4 \equiv 1 \pmod{1728}$ and $\gcd\big(a, 1728^n(n-1) - 1\big) = 1$. The polynomial*

$$f_{n,a}(x) = x^n + \left(\frac{a^4 - 1}{1728} - 1728^{n-1}\right)x + 1$$

is irreducible over $\mathbb{Q}$. For a root α of $f_{n,a}(x)$, let E be the elliptic curve defined by (1). Then $j(E) = \alpha$ and E has good reduction everywhere over $\mathbb{Q}(\alpha)$.

Proposition 3. *Let $n, a \in \mathbb{Z}$ with $n \geqslant 2$. The polynomial*

$$g_{n,a}(x) = x^n - 16^{n-2}(a - 16)x^{n-1} + ax - 1$$

is irreducible over $\mathbb{Q}$. For a root ϵ of $g_{n,a}(x)$, let E_1 and E_2 be the elliptic curves defined by the equations

$$E_1 :\ y^2 + xy = x^3 + 16\epsilon x^2 + 8\epsilon x + \epsilon \tag{2}$$

and

$$E_2 :\ y^2 + xy = x^3 - 8\epsilon x^2 + 2\epsilon(8\epsilon - 3)x + \epsilon(4\epsilon - 1). \tag{3}$$

Then E_1 and E_2 have good reduction everywhere over $\mathbb{Q}(\epsilon)$. Moreover, their j-invariants, given by

$$j_1 = \frac{\big(4096\epsilon^2 - 256\epsilon + 1\big)^3}{\epsilon(16\epsilon - 1)} \qquad \text{and} \qquad j_2 = \frac{\big(256\epsilon^2 + 224\epsilon + 1\big)^3}{\epsilon(1 - 16\epsilon)^4} \tag{4}$$

respectively, satisfy $\mathbb{Q}(\epsilon) = \mathbb{Q}(j_1) = \mathbb{Q}(j_2)$.

Theorem 1 follows immediately from Proposition 2 since there exist infinitely many $a \in \mathbb{Z}$ satisfying the conditions. In the case $n \geqslant 3$, Theorem 1 also follows from Proposition 3 since the number of the roots ϵ defining the same j-invariant is only finite by (4). When $n = 2$, the polynomial $g_{2,a}(x) = x^2 + 16x - 1$ does not depend on $a \in \mathbb{Z}$, so Proposition 3 only gives elliptic curves defined over the quadratic field $\mathbb{Q}(\epsilon) = \mathbb{Q}(\sqrt{65})$. The two propositions give almost distinct algebraic integers α satisfying $\alpha \in j(\mathcal{E}^0_{\mathbb{Q}(\alpha)})$ (see Proposition 5).

In order to prove the irreducibility of $f_{n,a}(x)$ and $g_{n,a}(x)$ in Propositions 2 and 3, we use the following lemma which follows immediately from the irreducibility criterion of Perron ([1, Theorem 2]).

Lemma 4. *Let $n \in \mathbb{Z}$ with $n \geqslant 2$ and*

$$F(x) = x^n + sx^{n-1} + tx \pm 1,$$

where $s, t \in \mathbb{Z}$. If $|s| > |t| + 2$ or $|t| > |s| + 2$, then $F(x)$ is irreducible over $\mathbb{Q}$.

We begin the proofs of the propositions.

Proof of Proposition 2. Set $b = \frac{a^4-1}{1728} - 1728^{n-1}$. We have $|b| > 2$. Indeed, $(x, y) = (12^n, a^2)$ is on the elliptic curve $y^2 = x^3 + 1728b + 1$, but this curve has no integral point of such a form if $|b| \leqslant 2$. Therefore $f_{n,a}(x) = x^n + bx + 1$ is irreducible by Lemma 4.

The discriminant of (1) is given by

$$\Delta = \frac{\alpha^2}{(\alpha - 1728)^3}.$$

We denote by $\mathrm{ord}_\mathfrak{p}$ the normalized additive valuation on $\mathbb{Q}(\alpha)$ at $\mathfrak{p}$. Assume that a prime ideal $\mathfrak{p}$ of $\mathbb{Q}(\alpha)$ satisfies $\mathrm{ord}_\mathfrak{p}(\alpha - 1728) = 0$. The coefficients of (1) are $\mathfrak{p}$-integral. Moreover, we have $\mathrm{ord}_\mathfrak{p}(\Delta) = 0$ since α is a unit by the definition. Thus E has good reduction at $\mathfrak{p}$. Assume that $\mathfrak{p}$ satisfies $\mathrm{ord}_\mathfrak{p}(\alpha - 1728) > 0$. Then we have $\mathrm{ord}_\mathfrak{p}(\alpha) = \mathrm{ord}_\mathfrak{p}(6) = 0$. To prove that E has good reduction at $\mathfrak{p}$, we have only to show that $\mathrm{ord}_\mathfrak{p}(\Delta) \equiv 0 \pmod{12}$ (cf. [3, Exercise 7.2]). Since α is a root of $f_{n,a}(x)$, we have

$$\begin{aligned} a^4\alpha &= -1728\alpha^n + 1728^n\alpha + \alpha - 1728 \\ &= (\alpha - 1728)\left(1 - 1728\alpha \sum_{i=0}^{n-2} 1728^i \alpha^{n-2-i}\right). \end{aligned}$$

Hence $\mathrm{ord}_\mathfrak{p}(a) > 0$, which implies $\mathrm{ord}_\mathfrak{p}(1728^n(n-1) - 1) = 0$ by the assumption on a. On the other hand, we have

$$1 - 1728\alpha \left(\sum_{i=0}^{n-2} 1728^i \alpha^{n-2-i}\right) \equiv 1 - 1728^n(n-1) \pmod{\mathfrak{p}}$$

since $\alpha \equiv 1728 \pmod{\mathfrak{p}}$. Thus $\mathrm{ord}_{\mathfrak{p}}(\alpha - 1728) = \mathrm{ord}_{\mathfrak{p}}(a^4) = 4\,\mathrm{ord}_{\mathfrak{p}}(a)$. This shows that $\mathrm{ord}_{\mathfrak{p}}(\Delta) = 2\,\mathrm{ord}_{\mathfrak{p}}(\alpha) - 3\,\mathrm{ord}_{\mathfrak{p}}(\alpha - 1728) = -12\,\mathrm{ord}_{\mathfrak{p}}(a) \equiv 0 \pmod{12}$ as desired. ■

Remark. As in the proof above, E with discriminant $\Delta = \frac{\alpha^2}{(\alpha-1728)^3}$ has good reduction at a prime $\mathfrak{p}$ with $\mathrm{ord}_{\mathfrak{p}}(6) = 0$ if $\mathrm{ord}_{\mathfrak{p}}(\alpha) \geqslant 0$ and $2\,\mathrm{ord}_{\mathfrak{p}}(\alpha) \equiv 3\,\mathrm{ord}_{\mathfrak{p}}(\alpha - 1728) \pmod{12}$. For the example of Tate, this condition is verified by $\alpha(\alpha-1728) = a^{12}$. Our curves are constructed so that α is a unit and $\mathrm{ord}_{\mathfrak{p}}(\alpha-1728) \equiv 0 \pmod 4$.

Proof of Proposition 3. When $n = 2$ and 3, the polynomial $g_{n,a}(x)$ is irreducible over $\mathbb{Q}$ since $g_{n,a}(\pm 1) \neq 0$. When $n \geqslant 4$, if $a \neq 16$, we have $16^{n-2}|a-16| > |a| + 2$. So $g_{n,a}(x)$ is irreducible by Lemma 4. The irreducibility of $g_{n,16}(x) = x^n + 16x - 1$ also follows by Lemma 4.

Let ϵ be a root of $g_{n,a}(x)$. The discriminants of E_1 and E_2 are given by $-\epsilon(1-16\epsilon)$ and $\epsilon(1-16\epsilon)^4$ respectively. Clearly ϵ is a unit by the definition, and $1-16\epsilon$ is also a unit since $1-16\epsilon$ is a root of $(-16)^n g_{n,a}\left(\frac{1-x}{16}\right) \in \mathbb{Z}[x]$ which is a monic polynomial with constant term $1 - 16^{n-1}(a-16) + 16^{n-1}a - 16^n = 1$. Therefore E_1 and E_2 have unit discriminants, that is, E_1 and E_2 have good reduction everywhere over $\mathbb{Q}(\epsilon)$. By (4), ϵ^{-1} is a root of the polynomial

$$x^6 + (j_1 - 768)x^5 - 2^4(j_1 - 13056)x^4 - 2^{21}11x^3 + 2^{24}51x^2 - 2^{32}3x + 2^{36}. \quad (5)$$

Every conjugate of ϵ^{-1} over $\mathbb{Q}(j_1)$ is a unit and a root of (5). On the other hand, (5) have only one 2-adic unit root since j_1 is a 2-adic unit by (4). Therefore $\epsilon^{-1} \in \mathbb{Q}(j_1)$. This means $\mathbb{Q}(\epsilon) = \mathbb{Q}(j_1)$. We can show that j_2 satisfies $\mathbb{Q}(j_2) = \mathbb{Q}(\epsilon)$ by using the same argument, because ϵ^{-1} is a root of the polynomial of the form

$$\begin{aligned} x^6 - (j_2 - 672)x^5 + 2^6(j_2 + 2364)x^4 - 2^9(3j_2 - 22624)x^3 \\ + 2^{14}(2364 + j_2)x^2 - 2^{16}(j_2 - 672)x + 2^{24} \end{aligned}$$

over $\mathbb{Q}(j_2)$ by (4). ■

Remark (cf. [4, Remark 4.1 (A2)]). E_1 and E_2 are isogenous to the elliptic curve

$$E_3 :\ y^2 + xy = x^3 - 8\epsilon x^2 + \epsilon(16\epsilon - 1)x \qquad \text{with } j_3 = \frac{\left(256\epsilon^2 - 16\epsilon + 1\right)^3}{\epsilon^2(1-16\epsilon)^2}$$

which has three $\mathbb{Q}(\epsilon)$-rational points of order 2. Therefore, we have the four curves E_1, E_2, E_3 and

$$E_4 :\ y^2 + xy = x^3 - 2\epsilon x^2 + \epsilon^2 x \qquad \text{with } j_4 = \frac{\left(16\epsilon^2 - 16\epsilon + 1\right)^3}{\epsilon^4(1-16\epsilon)}$$

isogenous to each other. So E_3 and E_4 also belong to $\mathcal{E}^0_{\mathbb{Q}(\epsilon)}$. It is shown that the degree of j_3 (resp. j_4) is greater than or equal to $\frac{n}{2}$ (resp. $\frac{n}{4}$) by applying the same argument as in the proof of Proposition 3. Actually, there is a case that the degrees of j_3 and j_4 are $\frac{n}{2}$. For example, when $(n, a) = (4, 32)$, we have $\mathbb{Q}(j_3) = \mathbb{Q}(j_4) = \mathbb{Q}(\sqrt{16385})$.

We end this paper by remarking that the number fields given in Propositions 2 and 3 have different number of real places in general.

Proposition 5.

(i) *Assume n is odd and $|a| > \sqrt[4]{1728^n + 1}$. Then the number of real places of the field defined by $f_{n,a}(x)$ is* 1.

(ii) *Assume n is even. Then the number of real places of the field defined by $f_{n,a}(x)$ is less than or equal to* 2.

(iii) *Assume $a \neq 16$ (resp. $a \leqslant -48$ or $a > 16$) if n is odd (resp. even). Then the number of real places of the field defined by $g_{n,a}(x)$ is 3 (resp. 4).*

Proof. Count the number of the real roots of $f_{n,a}(x)$ and $g_{n,a}(x)$. ■

Acknowledgment. The author would like to thank Kazuo Matsuno for many helpful suggestions and comments. This work was partially supported by Grant-in-Aid for JSPS Fellows Grant Number 2611708.

References

[1] O. Perron, *Neue Kriterien für die Irreduzibilität algebraischer Gleichungen*, J. Reine Angew. Math. **132** (1907), 288–307.

[2] D.E. Rohrlich, *Elliptic curves with good reduction everywhere*, J. London Math. Soc. **25** (1982), 216–222.

[3] J.H. Silverman, *The Arithmetic of Elliptic Curves* (2nd edition), Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 2009.

[4] N. Takeshi, *Elliptic curves with good reduction everywhere over cubic fields*, Int. J. Number Theory **11** (2015), no. 4, 1149–1164.

Address: Nao Takeshi: Department of Mathematics, Gakushuin University, 1-5-1, Mejiro, Toshima-ku, Tokyo, 171-8588, Japan.

E-mail: m10ntakeshi@gmail.com

Received: 26 November 2015; **revised:** 16 March 2016