BULL. AUSTRAL. MATH. SOC. 11G05, 14H52
VOL. 73 (2006) [245–254]

CONSTRUCTION OF ELLIPTIC CURVES WITH CYCLIC GROUPS OVER PRIME FIELDS

NAOYA NAKAZAWA

The purpose of this article is to construct families of elliptic curves E over finite fields F so that the groups of F-rational points of E are cyclic, by using a representation of the modular invariant function by a generator of a modular function field associated with the modular group $\Gamma_0(N)$, where $N = 5$, 7 or 13.

1. INTRODUCTION

The purpose of this article is to give some families of elliptic curves E defined over finite fields F so that the groups $E(F)$ of F-rational points of E are cyclic. An approach to construct families of such elliptic curves is to use the representation of the modular invariant function J by a generator of a modular function field of genus 0. Let N be a positive integer. Denote by $\Gamma(N)$ the principal congruence subgroup of $SL_2(\mathbb{Z})$ of level N and by $A(N)$ the modular function field over $\mathbb{C}$ associated with the group $\Gamma(N)$. In [6], to this purpose, the author used the representation of J given by $J = X^5 + 5X^4 + 40X^3$, where X is a generator of a subfield of $A(5)$ of degree 5 over $\mathbb{C}(J)$(see [4]).

In this article, we construct such families of elliptic curves by using the modular function field $A_0(N)$ associated with the modular group $\Gamma_0(N)$. Let N be one of 2, 3, 5, 7 and 13. Then $A_0(N)$ is of genus 0 and it is well known that $A_0(N)$ is generated over $\mathbb{C}$ by a modular function $h = \big(\eta(\tau)/\eta(N\tau)\big)^{24/(N-1)}$, where $\eta(\tau) = e^{2\pi i\tau/24}\prod_{n\geqslant 1}(1 - e^{2n\pi i\tau})$. This result is easily obtained from Theorem 21 of [7, p. 153]. We remark in the case N is prime, $A_0(N)$ is of genus 0 if and only if $N = 2, 3, 5, 7, 13$. Since $J \in A_0(N)$, J is a rational function $j_N(h)$ of h. See [2, Section 4] for the explicit forms of $j_N(h)$. By putting $g = N^{12/(N-1)}/h$, $j_N(h)$ is transformed into $\widetilde{j}_N(g)$ as follows:

$$\begin{aligned}
(N=2)\quad & \widetilde{j}_2(g) = (g+16)^3/g,\\
(N=3)\quad & \widetilde{j}_3(g) = (g+27)(g+3)^3/g,\\
(N=5)\quad & \widetilde{j}_5(g) = (g^2+10g+5)^3/g,\\
(N=7)\quad & \widetilde{j}_7(g) = (g^2+13g+49)(g^2+5g+1)^3/g,\\
(N=13)\quad & \widetilde{j}_{13}(g) = (g^2+5g+13)(g^4+7g^3+20g^2+19g+1)^3/g.
\end{aligned}$$

Received 8th November, 2005
The author would like to express his heartly gratitude to Professor N.Ishii for the encouragement to consider this problem and also for the very helpful advice.

Now, for non-zero $s \in \overline{\mathbb{Q}}$, such that $\tilde{j}_N(s) \neq 0, 1728$, define an elliptic curve $E_N(s)$ by

$$E_N(s) : y^2 = f_N(s,x) = x^3 - 3\frac{\tilde{j}_N(s)}{\tilde{j}_N(s) - 1728}x - 2\frac{\tilde{j}_N(s)}{\tilde{j}_N(s) - 1728}. \tag{1}$$

It is well known that the j-invariant of $E_N(s)$ is $\tilde{j}_N(s)$ and $E_N(s)(\overline{\mathbb{Q}})$ has a $\mathbb{Q}(s)$-rational cyclic group of order N. For example, see [**1**, Section 3]. This implies that if N is odd, then the N-division polynomial $\psi_N(x)$ of $E_N(s)$ has a $\mathbb{Q}(s)$-rational factor $D_N(s,x)$ of degree $(N-1)/2$ as a polynomial of x.

The following Proposition 1.1, obtained easily from a result of Gupta and Murty ([**3**, Lemma 1]), is essential for our argument. For an elliptic curve E defined over a field L and a prime number l, we denote by $K_l(E)$ the field generated over L by the coordinates of all l-division points of E.

Proposition 1.1. *Assume that a prime number p is of the form $p = q_1^{m_1} \dots q_n^{m_n} + 1$, where $q_1, \dots, q_{n-1}$ and q_n are distinct primes. For an elliptic curve E defined over $\mathbb{Q}$ such that E has good reduction at p, let $\overline{E}$ be the reduction of E modulo p. Then the group $\overline{E}(\mathbb{F}_p)$ of $\mathbb{F}_p$-rational points is cyclic if and only if p does not split completely in $K_{q_1}(E), \dots, K_{q_{n-1}}(E)$, and $K_{q_n}(E)$.*

Proposition 1.2. *Let E be an elliptic curve over a field L, and l be a prime number distinct from the characteristic of L. If the l-division polynomial $\psi_l(x)$ of E does not split over L, then not all elements of order l of $E(\overline{L})$ are rational over L.*

Proof: The splitting field in $\overline{L}$ of ψ_l over L is the subfield generated by the x-coordinates of the elements of order l of $E(\overline{L})$. ∎

By Propositions 1.1 and 1.2, we have the following assertion.

Theorem 1.3. *Let $s \in \mathbb{Q}$, N be one of 3, 5, 7 and 13, and p be a prime number of the form $p = 2^{m_2}N^{m_N} + 1$. Assume that an elliptic curve $E_N(s)$ defined by (1) has good reduction at p. If $D_N(s,x)$ and $f_N(s,x)$ do not split completely modulo p, then the group $\overline{E_N(s)}(\mathbb{F}_p)$ is cyclic.*

Proof: By Proposition 1.2, p splits completely neither in $K_N\big(E_N(s)\big)$ nor $K_2\big(E_N(s)\big)$. Therefore, by Proposition 1.1, the assertion holds true. ∎

By using Theorem 1.3, we construct families of elliptic curves with the desired properties for every $N = 3, 5, 7, 13$. However, here, we shall give our results only for $N = 5, 7$ or 13.

Notation. In the following, for $\alpha = a/b \in \mathbb{Q}$, $(a,b) = 1$, and a prime number p, we put $(\alpha/p)^* = (ab/p)$.

2. The case $N = 5$

For a non-zero number $s \in \mathbb{Q}$, such that $\tilde{j}_5(s) \neq 0, 1728$, we shall consider an elliptic curve $E_5(s)$ defined by (1). The 5-division polynomial $\psi_5(x)$ of $E_5(s)$ has a quadratic factor

$$D_5(s,x) = A(s)(s^2+4s-1)^2x^2 + 2A(s)(s^2+10s+5)(s^2+4s-1)x + (s^2+10s+5)^2(s^2+22s+89),$$

where $A(s) = s^2+22s+125$. The discriminant of $D_5(s,x)$ is

$$2^4 3^2 A(s)(s^2+10s+5)^2(s^2+4s-1)^2.$$

Let p be a prime number of the form $p = 2^{m_2}5^{m_5}+1$. If $\left(A(s)/p\right)^* = -1$, then $D_5(s,x)$ does not split completely modulo p. By the way, the discriminant of $f_5(s,x)$ is

$$\frac{2^8 3^6 (s^2+10s+5)^6 s}{(s^2+4s-1)^6 A(s)^3}.$$

Thus if $\left(A(s)/p\right)^* = -1$ and $(s/p)^* = 1$, then by Theorem 1.3, the group $\overline{E_5(s)}(\mathbb{F}_p)$ is cyclic. If we take a non-square integer ε and a pair of rational numbers (S,T) such that

$$A(S^2) = S^4 + 22S^2 + 125 = \varepsilon T^2, \tag{2}$$

then for a prime number of the form $p = 2^{m_2}5^{m_5}+1$ satisfying $(\varepsilon/p) = -1$ and $s = S^2$, we know $\overline{E_5(s)}(\mathbb{F}_p)$ is a cyclic group. For instance, by taking $\varepsilon = 13$, we have the following theorem.

THEOREM 2.1. *Let p be a prime number of the form $p = 2^{m_2}5^{m_5}+1$ satisfying $\left(13/p\right) = -1$. Consider the elliptic curve $\mathcal{E}_1$ defined by*

$$\mathcal{E}_1 : V^2 = U^3 - 565812U - 163779759.$$

Then we have the following assertions.

(i) *$\mathcal{E}_1$ is transformed into the curve defined by $S^4+22S^2+125 = 13T^2$, by the transformation*

$$S = S(U,V) = \frac{5(V+24U+10647)}{(V-54U-23517)}$$

and

$$T = T(U,V) = \frac{10(V^2-270V+1314U^2+1131624U+243513621)}{(V-54U-23517)^2}.$$

(ii) *The point $Q = (1092, 22815)$ is a rational point of $\mathcal{E}_1$ of infinite order.*

(iii) *Let $[m]Q = \overbrace{Q+\cdots+Q}^{m} = (U_m, V_m)$ and $S_m = S(U_m,V_m)$. If the elliptic curve $E_5(S_m^2)$ has good reduction at p, then the group $\overline{E_5(S_m^2)}(\mathbb{F}_p)$ is cyclic.*

https://doi.org/10.1017/S000497270003882X Published online by Cambridge University Press

Proof: Since $[m]Q \neq O$, for integers $1 \leqslant m \leqslant 12$, by Mazur's theorem ([**9**, p. 223]), we see the order of Q is infinity. This shows (ii). Putting $S = S(U, V)$ and $T = T(U, V)$ in the equation (2), for $\varepsilon = 13$, we see that $S(U, V)^4 + 22S(U, V)^2 + 125 - 13T(U, V)^2$ is a multiple of $V^2 - U^3 + 565812U + 163779759$. This shows (i). The assertion (iii) is obvious by the above argument. ∎

We shall list some examples of prime numbers of the form $p = 2^{m_2}5^{m_5} + 1$ satisfying $(13/p) = -1$ and the orders of $\overline{E_5(S_m^2)}(\mathbb{F}_p)$ in Table 1.

m	1	2	3	4	5	6	7
$p = 2^3 5 + 1$	32	52	52	32	32	52	52
$2^4 5^2 + 1$	392	432	372	382	402	432	392
$2^6 5^2 + 1$	1642	1572	1632	1562	1622	1582	1632
$2^7 5^3 + 1$	15862	15852	15932	16072	16152	15972	15832
$2^{13} 5 + 1$	40962	40612	41152	41202	40822	40742	41182
$2^{15} 5 + 1$	163422	163832	164022	163812	164062	163462	164472

Table 1: Orders of $\overline{E_5(S_m^2)}(\mathbb{F}_p)$ in Theorem 2.1.

3. The case $N = 7$

Let $\omega = (-1 + \sqrt{-3})/2$. For a non-zero number $s \in \mathbb{Q}(\omega)$, such that $\widetilde{j}_7(s) \neq 0, 1728$, we consider an elliptic curves $E_7(s)$ defined by (1). The 7-division polynomial $\psi_7(x)$ of $E_7(s)$ has a cubic factor

$$
\begin{aligned}
(3)\quad D_7(s, x) = A(s)^3x^3 &+ 3A(s)^2B(s)C(s)x^2 \\
&+ 3A(s)B(s)^2C(s)(s^2 + 13s + 33)x \\
&+ B(s)^3C(s)(s^4 + 26s^3 + 219s^2 + 778s + 881),
\end{aligned}
$$

where $A(s) = s^4 + 14s^3 + 63s^2 + 70s - 7$, $B(s) = s^2 + 5s + 1$ and $C(s) = s^2 + 13s + 49$. By replacing $A(s)x/B(s)$ by x, (3) is transformed into

$$
(4)\quad x^3 + 3C(s)x^2 + 3C(s)(s^2 + 13s + 33)x + C(s)(s^4 + 26s^3 + 219s^2 + 778s + 881).
$$

Further by replacing x by $x - C(s)$, (4) is transformed into

$$
(5)\qquad d_7(s, x) = x^3 - 48C(s)x + 64(2s + 13)C(s).
$$

Since the discriminant of $d_7(s, x)$ is $2^{12}3^6C(s)^2$, the Galois group of the splitting field over $\mathbb{Q}(\omega)$ of $d_7(s, x)$ is isomorphic to a subgroup of $\mathbb{Z}/3\mathbb{Z}$. Further we know that the roots of the equation $d_7(s, x) = 0$ are given by

$$
x = \frac{\theta_1 + \theta_2}{3}, \frac{\omega\theta_1 + \omega^2\theta_2}{3}, \frac{\omega^2\theta_1 + \omega\theta_2}{3},
$$

where

$$\theta_1 = -6\sqrt[3]{\left((2s+13)+3\sqrt{-3}\right)\left((2s+13)-3\sqrt{-3}\right)^2},$$
$$\theta_2 = -6\sqrt[3]{\left((2s+13)+3\sqrt{-3}\right)^2\left((2s+13)-3\sqrt{-3}\right)}.$$

Let $\mathfrak{p}$ be a prime ideal of $\mathbb{Q}(\omega)$ over p. We remark that if $\theta_1+\theta_2 \in \mathbb{F}_\mathfrak{p}$, then $\theta_1, \theta_2 \in \mathbb{F}_\mathfrak{p}$. By the way, the discriminant of $f_7(s,x)$ is

$$\frac{2^8 3^6 B(s)^6 C(s)^2 s}{A(s)^6}.$$

Therefore, we have

Proposition 3.1. *Let p be a prime number and $\mathfrak{p}$ a prime ideal of $\mathbb{Q}(\omega)$ over p. Then, for $s \in \mathbb{Q}(\omega)$, we have the following assertions.*

(i) *If $\left((2s+13)+3\sqrt{-3}\right)/\left((2s+13)-3\sqrt{-3}\right)$ is non-cubic modulo $\mathfrak{p}$, then $D_7(s,x)$ does not split completely modulo $\mathfrak{p}$.*

(ii) *If s is non-square modulo $\mathfrak{p}$, then $f_7(s,x)$ does not split completely modulo $\mathfrak{p}$.*

Let p be a prime number of the form $p = 2^{m_2}7^{m_7}+1$ and put $S = 2s+13$. Suppose that $p+1 \not\equiv 0 \bmod 9$. Then we have $\left(\omega/(p)\right)_3 = \omega^{(p^2-1)/3} \neq 1$. Let us consider a pair (S,T) of elements of $\mathbb{Q}(\omega)$ such that

$$\frac{S+3\sqrt{-3}}{S-3\sqrt{-3}} = \omega T^3, \text{ where } T \in \mathbb{Q}(\omega).$$

Then we have

$$S = S(T) = \frac{(\sqrt{-3})^3(1+\omega T^3)}{1-\omega T^3}. \tag{6}$$

Since $(\omega/(p))_3 \neq 1$, by Proposition 3.1, $D_7\left(\left(S(T)-13\right)/2, x\right)$ does not split completely modulo (p).

In the following, we restrict ourselves to the case $S(T)$ is a rational number. First, we shall show the following lemma.

Lemma 3.2. *For $T \in \mathbb{Q}(\omega)$, put*

$$S(T) = \frac{(\sqrt{-3})^3(1+\omega T^3)}{1-\omega T^3}.$$

Then $S(T) \in \mathbb{Q}$ if and only if $T = a+\sqrt{-3}b$ for some $a, b \in \mathbb{Q}$ such that $a^2+3b^2 = 1$.

Proof: Assume that

$$S(T) = \frac{(\sqrt{-3})^3(1+\omega T^3)}{1-\omega T^3} \in \mathbb{Q}.$$

https://doi.org/10.1017/S000497270003882X Published online by Cambridge University Press

Then we know

$$\frac{(\sqrt{-3})^3(1+\omega T^3)}{1-\omega T^3}=\frac{(-\sqrt{-3})^3(1+\omega^2\overline{T}^3)}{1-\omega^2\overline{T}^3},$$

where $\overline{T}$ is the complex conjugate of T. By a simple calculation, we know $T^3\overline{T}^3 = 1$. Since $T\overline{T} \in \mathbb{R}$, we see that $T\overline{T} = 1$. Put $T = a + \sqrt{-3}b(a, b \in \mathbb{Q})$. Then we have $T\overline{T} = a^2 + 3b^2 = 1$. Conversely, if $T = a + \sqrt{-3}b$, where a, b are rational numbers such that $a^2 + 3b^2 = 1$, then by a simple calculation, we see

$$S(T)=\frac{(\sqrt{-3})^3(1+\omega T^3)}{1-\omega T^3}=\frac{9(12ab^2-12b^3-a+3b)}{12ab^2+36b^3-a-9b-2}\in\mathbb{Q}.$$

∎

By Lemma 3.2 and the above argument, if we take a pair of rational numbers (a, b) such that $a^2 + 3b^2 = 1$ and put $T = a + \sqrt{-3}b$, then we see $D_7\Big(\big(S(T) - 13\big)/2, x\Big)$ does not split completely modulo p.

We know there exist infinity many pairs of rational numbers (a, b) such that $a^2 + 3b^2 = 1$. For instance,

$$(a,b)=\left(\frac{-3\alpha^2+\beta^2}{3\alpha^2+\beta^2},\frac{2\alpha\beta}{3\alpha^2+\beta^2}\right)$$

is a $\mathbb{Q}$-rational solution of $a^2 + 3b^2 = 1$, for $\alpha, \beta \in \mathbb{Z}$. Hence we have

Theorem 3.3. *Let p be a prime number of the form $p = 2^{m_2}7^{m_7} + 1$ satisfying $p + 1 \not\equiv 0 \bmod 9$. For $\alpha, \beta \in \mathbb{Z}$, $(\alpha, \beta) \neq (0, 0)$, let*

$$s(\alpha,\beta)=-\frac{33\alpha^3+45\alpha^2\beta-33\alpha\beta^2-5\beta^3}{3\alpha^3+9\alpha^2\beta-3\alpha\beta^2-\beta^3}.$$

If $E_7\big(s(\alpha, \beta)\big)$ has good reduction at p, and $\big(s(\alpha, \beta)/p\big)^* = -1$, then the group $\overline{E_7\big(s(\alpha, \beta)\big)}(\mathbb{F}_p)$ is cyclic.

Proof: Put $a = (-3\alpha^2 + \beta^2)/(3\alpha^2 + \beta^2)$, $b = (2\alpha\beta)/(3\alpha^2 + \beta^2)$ and

$$T=\frac{-3\alpha^2+\beta^2}{3\alpha^2+\beta^2}+\sqrt{-3}\frac{2\alpha\beta}{3\alpha^2+\beta^2}.$$

By (6), we have $(S(T) - 13)/2 = s(\alpha, \beta)$. Therefore, by Proposition 3.1, the polynomials $D_7(s(\alpha, \beta), x)$ and $f_7(s(\alpha, \beta), x)$ do not split completely modulo p. By Theorem 1.3, we have our assertion. ∎

We remark that $2^{m_2}7^{m_7} + 2 \equiv 0 \bmod 9$ if and only if $m_2 + 4m_7 \equiv 4 \bmod 6$. For instance, we have $m_2 + 4m_7 \not\equiv 4 \bmod 6$ for prime numbers

$$p = 2^27+1, 2^27^3+1, 2^27^6+1, 2^47+1, 2^47^5+1, 2^47^{19}+1, 2^67^2+1, 2^67^5+1, 2^67^{11}+1.$$

For $p = 2^67^2 + 1$, we shall give some examples of (α, β) such that $\big(s(\alpha, \beta)/p\big)^* = -1$ and the orders of $\overline{E_7\big(s(\alpha, \beta)\big)}(\mathbb{F}_p)$ in Table 2.

(α,β)	$(1,1)$	$(2,9)$	$(3,2)$	$(3,8)$	$(4,1)$	$(4,5)$	$(5,2)$
$\lvert\overline{E_7(s(\alpha,\beta))}(\mathbb{F}_p)\rvert$	3200	3102	3146	3202	3186	3076	3060

Table 2: Orders of $\overline{E_7(s(\alpha,\beta))}(\mathbb{F}_p)(p = 2^6 7^2 + 1)$.

4. The case $N = 13$

For a non-zero rational number s, such that $\widetilde{j}_{13}(s) \neq 0, 1728$, we consider an elliptic curve $E_{13}(s)$ defined by (1).

4.1. Computation of $D_{13}(s,x)$. We shall determine a factor $D_{13}(s,x)$ of degree 6 of the 13-division polynomial $\psi_{13}(x)$ of $E_{13}(s)$. By Schoof's method, $D_{13}(s,x)$ can be computed by coefficients of $E_{13}(s)$ and of a 13-isogenous curve $\widehat{E_{13}}(s)$. The equation

$$J = \widetilde{j}_{13}(g) = \frac{(g^2+5g+13)(g^4+7g^3+20g^2+19g+1)^3}{g}$$

can be transformed into the modular equation $\Phi(g, J) = 0$ given in [5, Section 3.2.1]. Therefore, by Morain [5, Section 3.2], the curve $\widehat{E_{13}}(s)$ can be obtained as follows:

$$\widehat{E_{13}}(s) : y^2 = x^3 - 3\cdot 13^4 \overline{E_4}^{(13)} x - 2\cdot 13^6 \overline{E_6}^{(13)},$$

where

$$\begin{aligned}
\overline{E_4}^{(13)} &= (s^4+247s^3+3380s^2+15379s+28561)H_1(s)H_2(s)^2/28561,\\
\overline{E_6}^{(13)} &= (s^6-494s^5-20618s^4-237276s^3-1313806s^2-3712930s^2-4826809)\\
&\qquad\qquad \times H_1(s)H_2(s)^3/4826809,\\
H_1(s) &= (s^2+5s+13)/(s^2+6s+13),\\
H_2(s) &= (s^4+7s^3+20s^2+19s+1)/(s^6+10s^5+46s^4+108s^3+122s^2+38s-1).
\end{aligned}$$

Let $D_{13}(s,x) = x^6+e_5x^5+e_4x^4+e_3x^3+e_2x^2+e_1x+e_0$. Then by Schoof [8, Section 8], we have

$$\begin{aligned}
e_0 &= H_1(s)^2H_2(s)^6(s^{14}+38s^{13}+649s^{12}+6844s^{11}+50216s^{10}+271612s^9\\
&\qquad +1115174s^8+3520132s^7+8549270s^6+15812476s^5+21764840s^4\\
&\qquad +21384124s^3+13952929s^2+5282630s+854569)/(s^2+6s+13),\\
e_1 &= 6H_1(s)^2H_2(s)^5(s^{10}+27s^9+316s^8+2225s^7+10463s^6+34232s^5\\
&\qquad +78299s^4+122305s^3+122892s^2+69427s+16005),\\
e_2 &= 3H_1(s)^2H_2(s)^4(5s^8+110s^7+1045s^6+5798s^5+20508s^4+47134s^3\\
&\qquad +67685s^2+54406s+17581),\\
e_3 &= 4H_1(s)H_2(s)^3(5s^6+80s^5+560s^4+2214s^3+5128s^2+6568s+3373),\\
e_4 &= 3H_1(s)H_2(s)^2(5s^4+55s^3+260s^2+583s+537),\\
e_5 &= 6H_2(s)(s^2+5s+13).
\end{aligned}$$

https://doi.org/10.1017/S000497270003882X Published online by Cambridge University Press

4.2. Construction of cyclic groups $\overline{E_{13}(s)}(\mathbb{F}_p)$. Let p be a prime number of the form $p = 2^{m_2}13^{m_{13}} + 1$. By a simple computation using Mathematica 5.0, we know the discriminant of $D_{13}(s,x)$ is

$$\frac{2^{60}3^{30}(s^2+5s+13)^{10}H_2(s)^{30}}{(s^2+6s+13)^{15}},$$

and the discriminant of $f_{13}(s,x)$ defined in (1) is

$$\frac{2^8 3^6 s(s^2+5s+13)^2 H_2(s)^6}{(s^2+6s+13)^3}.$$

Thus if $\left((s^2+6s+13)/p\right)^* = -1$ and $(s/p)^* = 1$, then $D_{13}(s,x)$ and $f_{13}(s,x)$ do not split completely modulo p. Therefore, by Theorem 1.3, the group $\overline{E_{13}(s)}(\mathbb{F}_p)$ is cyclic. In particular, if we take a rational number ε and a pair of rational numbers (S,T) so that

$$S^4 + 6S^2 + 13 = \varepsilon T^2, \quad \left(\frac{\varepsilon}{p}\right)^* = -1, \tag{7}$$

then the group $\overline{E_{13}(S^2)}(\mathbb{F}_p)$ is cyclic. For $\lambda \in \mathbb{Z}$, if we take $\varepsilon = (\lambda^4+6\lambda^2+13)/\lambda^2$, then we have the following theorem.

Theorem 4.1. *Let λ be an integer such that $\lambda \not\equiv 0 \bmod 13$. Let p be a prime number of the form $p = 2^{m_2}13^{m_{13}} + 1$ satisfying $\left((\lambda^4+6\lambda^2+13)/p\right) = -1$. Consider the elliptic curve $\mathcal{E}_2(\lambda)$ defined by*

$$\mathcal{E}_2(\lambda): V^2 = U^3 - 4\lambda^4(\lambda^4+6\lambda^2+13)^2 U - 3\lambda^6(\lambda^4+6\lambda^2+13)^3,$$

and put $\varepsilon(\lambda) = (\lambda^4+6\lambda^2+13)/\lambda^2$. Then we have the following assertions.

(i) *$\mathcal{E}_2(\lambda)$ is transformed into the curve defined by $S^4+6S^2+13 = \varepsilon(\lambda)T^2$, by the transformation*

$$S = S(U,V) = -\frac{\lambda\left((3\lambda^2+13)U + V + \lambda^2(5\lambda^2+13)(\lambda^4+6\lambda^2+13)\right)}{\lambda^2(\lambda^2+3)U - V + \lambda^4(\lambda^2+5)(\lambda^4+6\lambda^2+13)},$$

and

$$T = T(U,V) = \frac{\lambda(U^3 + A_1U^2 + A_2U + BV + C)}{\left(\lambda^2(\lambda^2+3)U - V + \lambda^4(\lambda^2+5)(\lambda^4+6\lambda^2+13)\right)^2},$$

where

$$\begin{aligned} A_1 &= 3\lambda^2(\lambda^4+10\lambda^2+13),\\ A_2 &= 4\lambda^4(\lambda^4+6\lambda^2+13)^2,\\ B &= -4\lambda^4(\lambda^4-13),\\ C &= 2\lambda^6(\lambda^4-2\lambda^2+13)(\lambda^4+6\lambda^2+13)^2. \end{aligned}$$

(ii) *The point* $Q(\lambda) = \big((\lambda^4+2\lambda^2+13)(\lambda^4+6\lambda^2+13)/4, (\lambda^4-13)(\lambda^4+6\lambda^2+13)^2/8\big)$ *is a rational point of* $\mathcal{E}_2(\lambda)$ *of infinite order.*

(iii) *Let*

$$[m]Q(\lambda) = \overbrace{Q(\lambda) + \cdots + Q(\lambda)}^{m} = \big(U_m(\lambda), V_m(\lambda)\big)$$

and

$$S_m(\lambda) = S\big(U_m(\lambda), V_m(\lambda)\big).$$

If the elliptic curve $E_{13}(S_m(\lambda)^2)$ *has good reduction at* p*, then the group* $\overline{E_{13}(S_m(\lambda)^2)}(\mathbb{F}_p)$ *is cyclic.*

PROOF: First, we shall show the assertion (ii). Assume that $Q(\lambda)$ is a torsion point. Then by the Nagell–Lutz Theorem ([**9**, p. 221]), the y-coordinate y of $Q(\lambda)$ is an integer, $y = 0$, or the square of y-coordinate y of $Q(\lambda)$ divides the discriminant Δ of $\mathcal{E}_2(\lambda)$. If $\lambda \equiv 0 \bmod 2$, then $(\lambda^4-13)(\lambda^4+6\lambda^2+13)^2/8$ is not an integer. We consider the case $\lambda \equiv 1 \bmod 2$. Obviously, $[2]Q(\lambda) \neq O$. Suppose that y^2 divides Δ. Since $\Delta = -13\lambda^{12}(\lambda^4+6\lambda^2+13)^6$, and λ is prime to 13, we have λ^4-13 divides $8(\lambda^4+6\lambda^2+13)$. Since $8(\lambda^4+6\lambda^2+13) = 8\big(\lambda^4-13+2(3\lambda^2+13)\big)$ and $(\lambda^4-13)/4$ is odd, we have $(\lambda^4-13)/4$ divides $3\lambda^2+13$. Let p_0 be an odd prime number dividing $(\lambda^4-13)/4$. Then we have $\lambda^4-13 \equiv 0 \bmod p_0$ and $3\lambda^2+13 \equiv 0 \bmod p_0$. These congruences imply $p_0 = 13$ and 13 divides λ. This shows a contradiction. Therefore the assertion (ii) holds true. Next, putting $S = S(U,V)$ and $T = T(U,V)$ in the equation (7), for $\varepsilon = \varepsilon(\lambda)$, we see that $S(U,V)^4 + 6S(U,V)^2 + 13 - \varepsilon(\lambda)T(U,V)^2$ is a multiple of a polynomial $U^3 - 4\lambda^4(\lambda^4+6\lambda^2+13)^2U - 3\lambda^6(\lambda^4+6\lambda^2+13)^3 - V^2$. This shows the assertion (i). The assertion (iii) is obvious. $\square$

EXAMPLE 1. In Theorem 4.1, take $\lambda = 1$ or 2. For $\lambda = 1$, we have $\big((\lambda^4+6\lambda^2+13)/p\big) = (5/p)$, and for $\lambda = 2$, we have $\big((\lambda^4+6\lambda^2+13)/p\big) = \big(53/p\big)$. In Tables 3 and 4, we shall list some examples of prime numbers of the form $p = 2^{m_2}13^{m_{13}}+1$ satisfying $\big((\lambda^4+6\lambda^2+13)/p\big) = -1$, and the orders of $\overline{E_{13}(S_m(\lambda)^2)}(\mathbb{F}_p)$ for $\lambda = 1$ and 2 respectively.

m	1	2	3	4	5	6
$p = 2^2 13 + 1$	58	58	50	54	58	singular
$2^2 13^2 + 1$	678	singular	678	652	singular	652
$2^{10} 13 + 1$	13336	13314	13266	13180	13266	13310
$2^4 13^3 + 1$	35028	34998	35080	35180	35418	35306
$2^{14} 13^2 + 1$	2771264	2769288	2770956	2767386	2771728	2769860

Table 3: Orders of $\overline{E_{13}(S_m(1)^2)}(\mathbb{F}_p)$.

REMARK. At present we do not know the order and generators of the cyclic group $\overline{E_N(s)}(\mathbb{F}_p)$. We think it is an interesting problem to determine them but this problem is beyond the scope of this article.

m	1	2	3	4	5	6
$p = 2^2 13^2 + 1$	682	678	708	652	700	674
$2^4 13^3 + 1$	35414	34868	35184	34994	34998	35340
$2^{14} 13^2 + 1$	2768842	2770714	2770870	2769444	2771706	2766068
$2^{20} 13 + 1$	13631026	13634034	13625124	13632192	13636114	13628166

Table 4: Orders of $\overline{E_{13}(S_m(2)^2)}(\mathbb{F}_p)$.

References

[1] P. Deligne and M. Rapoport, 'Les schemes de modulus de courbes elliptiques', in *Modular functions of one variable, II*, Lecture Notes in Math. **349** (Springer–Verlag, Berlin, 1973), pp. 143–316.

[2] N.D. Elkies, 'Elliptic and modular curves over finite fields and related computational issues', *AMS/IP Studies in Advanced Math.* **7** (1998), 21–76.

[3] R. Gupta and M.R. Murty, 'Cyclicity and generation of points mod p on elliptic curves', *Invent. Math.* **101** (1990), 225–235.

[4] N. Ishii, 'Defining equations of modular function fields', *Math. Japon.* **38** (1993), 941–951.

[5] F. Morain, 'Calcul du nombre de points sur une courbe elliptique dans un corps fini : aspects algorithmiques', *J. Théor. Nombres Bordeaux* **7** (1995), 255– 282.

[6] N. Nakazawa, 'Parametric families of elliptic curves with cyclic $\mathbb{F}_p$-rational points groups', *Tokyo J. Math.* **28** (2005), 381–392.

[7] B. Schoeneberg, *Elliptic modular functions* (Springer–Verlag, Berlin, Heildelberg, New York, 1974).

[8] R. Schoof, 'Counting points on elliptic curves over finite fields', *J. Théor. Nombres Bordeaux* **7** (1995), 219–254.

[9] J.H. Silverman, *The arithmetic of elliptic curves*, Graduate Text in Mathematics **106** (Springer–Verlag, Berlin, Heidelberg, New York 1986.).

Graduate school of Science
Osaka Prefecture University
1-1 Gakuen-cho, Sakai
Osaka 599-8531
Japan
e-mail: nao-nkzw@smail.plala.or.jp