TOKYO J. MATH.
VOL. 28, NO. 2, 2005

Parametric Families of Elliptic Curves with Cyclic $\mathbf{F}_p$-Rational Points Groups

Naoya NAKAZAWA

Osaka Prefecture University

(Communicated by H. Tsuji)

1. Introduction

In elliptic cryptography, it is needed for a given finite field F, to construct an elliptic curve whose group of F-rational points is cyclic of a large order. An approach to construct such elliptic curves is, for a given elliptic curve E defined over an algebraic number field K, to determine a set $S_{E,K}$ of prime ideals $\mathfrak{p}$ of K such that group $\bar{E}(\mathbf{F}_\mathfrak{p})$ of rational points of the reduction $\bar{E}$ of E modulo $\mathfrak{p}$ is cyclic. R. Gupta and M. R. Murty [3] obtained a result for this problem in probabilistic point of view. However, in general, the problem to determine the set $S_{E,K}$ is not easy. In the case E has complex multiplication and an ordinary good reduction at $\mathfrak{p}$, it is noted the group structure of $\bar{E}(\mathbf{F}_\mathfrak{p})$ is determined by the trace of Frobenius endomorphism (cf. [9]). In this case, the trace can be computed easily from the quadratic norm representation of a prime number (cf. [4], [5], [6], [7]). Therefore, in this case, we can give a family of prime ideals contained in $S_{E,K}$. For example see [2].

The purpose of this article is, without the properties of complex multiplication, to construct a family of elliptic curves E defined over $\mathbf{Q}$ such that for prime numbers of the form $p = 2^\alpha 3^\beta 5^\gamma q^\delta + 1$($q$:an odd prime) $\bar{E}(\mathbf{F}_p)$ are cyclic. The key for considering this problem is the next theorem.

THEOREM 1 (cf. [3]). *For an elliptic curve $E/\mathbf{Q}$ and a positive integer n, let $E[n]$ be the set of n-division points and $K_n(E)$ be the field generated over $\mathbf{Q}$ by all points of $E[n]$. Let p be a prime number such that E has good reduction at p and $\bar{E}(\mathbf{F}_p)$ the group of rational points on the reduction of E modulo p. Then we have*

(a) *$\bar{E}(\mathbf{F}_p)$ is cyclic if and only if p does not split completely in $K_l(E)$ for any prime l.*

(b) *The cyclotomic field $\mathbf{Q}(\zeta_n)$ is contained in $K_n(E)$ for any n.*

COROLLARY 2. *If a prime p of the form $p = 2^\alpha q_1^{\beta_1} \cdots q_m^{\beta_m} + 1$ ($q_1, \cdots, q_m$:odd primes) does not split completely in $K_2(E)$, $K_{q_1}(E), \cdots, K_{q_m}(E)$, then $\bar{E}(\mathbf{F}_p)$ is cyclic.*

Received January 15, 2004; revised May 27, 2004

PROOF. For an odd prime $q \neq q_i (i = 1, \cdots m)$, we have $p \not\equiv 1 \pmod{q}$. Thus p does not split completely in the cyclotomic field $\mathbf{Q}(\zeta_q)$. By Theorem 1(b) p does not split completely in $K_q(E)$, either. Therefore by (a), we have our assertions. □

EXAMPLE 3. (i) If a prime of the form $p = 2^{2^n} + 1$(Fermat prime) does not split completely in $K_2(E)$, then it is clear that $\bar{E}(\mathbf{F}_p)$ is cyclic.

(ii) For a prime of the form $p = 2^s q + 1 (q$: an odd prime such that $2^{s+2} < q)$, if p does not split completely in $K_2(E)$, then we can show easily that $q^2 \not| |\bar{E}(\mathbf{F}_p)|$ and therefore $\bar{E}(\mathbf{F}_p)$ is cyclic. We see there exist no integers $k \neq 0$ such that $|kq^2 - p - 1| \leq 2\sqrt{p}$ as follows. If this inequality holds, then

$$\frac{2^s q + 2 - \sqrt{2^s q + 1}}{q^2} \leq k \leq \frac{2^s q + 2 + \sqrt{2^s q + 1}}{q^2} .$$

However, since

$$\frac{2^s q + 2 + \sqrt{2^s q + 1}}{q^2} < \frac{2^s}{2^{s+2}} + \frac{2}{2^{s+2}} + \frac{2\sqrt{2^s q + 1}}{q^2} < \frac{1}{2} + \frac{1}{2^{s+1}} < 1$$

and

$$\left| \frac{2^s q + 2 - \sqrt{2^s q + 1}}{q^2} \right| \leq \left| \frac{2^s q + 2}{q^2} \right| + \left| \frac{2\sqrt{2^s q + 1}}{q^2} \right| < \frac{2^s}{q} + \frac{2}{q^2} + \frac{2\sqrt{2^s + 1}}{q^2} < 1 ,$$

k is not a non-zero integer. Thus $q^2 \not| |\bar{E}(\mathbf{F}_p)|$ by Hasse's inequality $||\bar{E}(\mathbf{F}_p)| - p - 1| \leq 2\sqrt{p}$.

2. Primes of the form $p = 2^\alpha 3^\beta + 1$

Let p be a prime number of the form $p = 2^\alpha 3^\beta + 1$. In this section, we construct a family of elliptic curves E over $\mathbf{Q}$ such that $\bar{E}(\mathbf{F}_p)$ are cyclic groups. By Corollary 2, if p does not split completely in $K_2(E)$ and $K_3(E)$, then $\bar{E}(\mathbf{F}_p)$ is cyclic. First, we note there exist many prime numbers of the form $2^\alpha 3^\beta + 1$, for example,

$$\begin{array}{rl}
\alpha = 1 & \beta = \cdots, 132, 180, 320, 696, 782, 822, 897, \cdots \\
\alpha = 2 & \beta = \cdots, 201, 249, 805, \cdots \\
\alpha = 3 & \beta = \cdots, 130, 143, 331, 332, 980, \cdots \\
\alpha = 4 & \beta = \cdots, 195, 296, 297, 533, 545, 644, 884, 932, \cdots \\
\cdots & \\
\alpha = 1000 & \beta = \cdots, 544, 807, \cdots \\
\cdots & .
\end{array}$$

THEOREM 4. *For given integers c and u, let $E_{c,u}/\mathbf{Q}$ be an elliptic curve defined as follows:*

$$E_{c,u}/\mathbf{Q} : y^2 = x^3 - (c^2 - 3)ux^2 + (2c + 3)u^2 x .$$

For a prime number of the form $p = 2^\alpha 3^\beta + 1$, *if* $c \not\equiv -1, -3/2, 3 \pmod{p}$ *and*

$$\left(\frac{-u}{p}\right) = \left(\frac{(c+1)(c-3)}{p}\right) = -1\,,$$

then $\overline{E_{c,u}}(\mathbf{F}_p)$ *is cyclic.*

PROOF. Put $A = -(c^2-3)u$, $B = (2c+3)u^2$ and $f(x) = x^2 + Ax + B$. Then $E_{c,u}[2] = \{O, (0,0), (\eta_1, 0), (\eta_2, 0)\}$ where η_1, η_2 are the roots of $f(x) = 0$. Since the discriminant of $f(x)$ is

$$D_2 = A^2 - 4B = (c+1)^3(c-3)u^2\,,$$

we have $\mathbf{Q}(\sqrt{(c+1)(c-3)}) \subset K_2(E_{c,u})$. Therefore, if

$$\left(\frac{(c+1)(c-3)}{p}\right) = -1\,,$$

then p does not split completely in $K_2(E_{c,u})$. Next we consider the decomposition of p in $K_3(E_{c,u})$. In this case, the 3-division polynomial $\phi_3(x)$ of $E_{c,u}$ factors over $\mathbf{Q}[x]$ as follows:

$$\phi_3(x) = 3x^4 + 4Ax^3 + 6Bx^2 - B^2 = (x+u)(3x^3 + r_2x^2 + r_1x + r_0)\,.$$

Thus we see $P_3 = (-u, \pm\sqrt{f(-u)})$ are 3-division points of $E_{c,u}$. Since $f(-u) = -(c+1)^2u^3$, we have $\mathbf{Q}(\sqrt{-u}) \subset K_3(E_{c,u})$. Therefore, the assumption shows that p does not split completely in $K_3(E_{c,u})$. □

REMARK. The discriminant of $E_{c,u}$ is $\delta_{E_{c,u}} = (c+1)^3(2c+3)^2(c-3)$, and j-invariant $j(E_{c,u}) = \frac{256c^3(c^3-6c-6)^3}{\delta_{E_{c,u}}}$.

COROLLARY 5. *Let* w *be an integer such that*

$$\left(\frac{w}{p}\right) = -1$$

and

$$(7w+9)(w+1)(9w+7) \not\equiv 0 \pmod{p}\,.$$

Then for

$$c = \frac{-(5w+3)}{w-1} \text{ or } \frac{3w+5}{w-1}\,,$$

$(\frac{(c+1)(c-3)}{p}) = -1$, *and therefore* $\overline{E_{c,u}}(\mathbf{F}_p)$ *is cyclic.*

PROOF. Put

$$c = \frac{-(5w+3)}{w-1}\,.$$

Since

$$c+1=\frac{-4(w+1)}{w-1} \quad \text{and} \quad c-3=\frac{-8w}{w-1},$$

$$\left(\frac{(c+1)(c-3)}{p}\right)=\left(\frac{32w(w+1)}{p}\right). \tag{1}$$

By assumptions,

$$\delta_{E_{c,u}}=\frac{512(7w+9)^2(w+1)^3w}{(w-1)^6}\not\equiv 0 \pmod{p}.$$

On the other hands, for

$$c'=\frac{3w+5}{w-1},$$

it satisfies that

$$\left(\frac{(c'+1)(c'-3)}{p}\right)=\left(\frac{32(w+1)}{p}\right), \tag{2}$$

and we have

$$\delta_{E_{c',u}}=\frac{512(9w+2)^2(w+1)^3}{(w-1)^6}\not\equiv 0 \pmod{p}.$$

By (1) and (2),

$$\left(\frac{(c+1)(c-3)}{p}\right)\left(\frac{(c'+1)(c'-3)}{p}\right)=\left(\frac{w}{p}\right)=-1.$$

Therefore by Theorem 4, we have our assertions. □

In the next example, by using Corollary 5, we shall give families of elliptic curves $E_{c,u}$ in Theorem 4 such that $\overline{E_{c,u}}(\mathbf{F}_p)$ are cyclic. Hereafter, the notion C_N denotes the cyclic group of order N.

EXAMPLE 6. In the following tables, let

$$c_1(w)=\frac{-(5w+3)}{w-1} \quad \text{and} \quad c_2(w)=\frac{3w+5}{w-1}.$$

1) $p=2^7 3^3+1=3457$. $(\frac{5}{p})=(\frac{-5}{p})=-1$. Put $u=5$.

w	5	7	10	14	15	17	19	20	21	23
c	$c_1(w)$	$c_1(w)$	$c_1(w)$	$c_2(w)$	$c_1(w)$	$c_1(w)$	$c_2(w)$	$c_2(w)$	$c_1(w)$	$c_1(w)$
$\overline{E_{c,5}}(\mathbf{F}_p)$	C_{3388}	C_{3412}	C_{3406}	C_{3448}	C_{3460}	C_{3544}	C_{3454}	C_{3448}	C_{3514}	C_{3400}

2) $p=2^4 3^5+1=3889$. $(\frac{11}{p})=(\frac{-11}{p})=-1$. Put $u=11$.

w	11	13	19	26	29	33	38	39	41	43
c	$c_1(w)$	$c_1(w)$	$c_1(w)$	$c_1(w)$	$c_1(w)$	$c_1(w)$	$c_2(w)$	$c_1(w)$	$c_1(w)$	$c_2(w)$
$\overline{E_{c,11}}(\mathbf{F}_p)$	C_{3850}	C_{3940}	C_{3994}	C_{3844}	C_{3874}	C_{3880}	C_{3838}	C_{3856}	C_{3928}	C_{3928}

3. Primes of the form $p = 2^\alpha 5^\beta + 1$ and $2^\alpha 5^\beta q^\gamma + 1$

In this section we consider the case that a prime p is given by the form $2^\alpha 5^\beta + 1$ or $2^\alpha 5^\beta q^\alpha + 1$.

3.1. $p = 2^\alpha 5^\beta + 1$**.** The following (α, β)'s are examples such that $p = 2^\alpha 5^\beta + 1$ are primes:

$$\begin{aligned}
\alpha &= 1 \ \ \beta = \cdots, 105, 159, 297, \cdots \\
\alpha &= 4 \ \ \beta = \cdots, 116, 166, 394, \cdots \\
\alpha &= 5 \ \ \beta = \cdots, 159, 483, 891, 897, \cdots \\
\alpha &= 6 \ \ \beta = \cdots, 194, 854, \cdots \\
&\cdots \\
\alpha &= 100 \ \ \beta = 36, 324, 418, 428, 436, 596, 804, \cdots \\
&\cdots \cdots .
\end{aligned}$$

Let $E/\mathbf{Q}$ be an elliptic curve and j the j-invariant of E. Then we know $K_5(E)$ contains the splitting field over $\mathbf{Q}$ of the polynomial

$$g(X, j) = X^5 + 5X^4 + 40X^3 - j \tag{3}$$

(cf. §3 of [1]). Therefore if $g(X, j)$ is not decomposed into linear factors modulo p, p does not split completely in $K_5(E)$. Furthermore if p does not split completely in $K_2(E)$, we see $\bar{E}(\mathbf{F}_p)$ is cyclic. Hereafter, we consider the case that $g(X, j)$ factors in $\mathbf{Q}[X]$ as follows:

$$g(X, j) = (X^2 + aX + b)(X^3 + rX^2 + sX + t)\,. \tag{4}$$

Comparing the coefficients (3) with (4), we obtain the quadratic equation of s:

$$s^2 + (a^2 - 40)s - a(a^2 - 5a + 40)(a - 5) = 0\,. \tag{5}$$

Take

$$s = \frac{1}{2}\{-(a^2 - 40) - \sqrt{5}(a - 4)\sqrt{a^2 + 20}\}\,.$$

Then we have

$$b = \frac{1}{2}\{3a^2 - 10(a - 4) + \sqrt{5}(a - 4)\sqrt{a^2 + 20}\}\,, \tag{6}$$

$$t = \frac{1}{2}\{a^2(4a - 25) + 50(a - 4) + \sqrt{5}(2a - 5)(a - 4)\sqrt{a^2 + 20}\} \tag{7}$$

and

$$j = -bt\,. \tag{8}$$

The discriminant of $X^2 + aX + b$ is

$$D_5(E) = a^2 - 4b = -5(a^2 - 4a + 16) - 2\sqrt{5}(a-4)\sqrt{a^2+20}\,.$$

If

$$\left(\frac{D_5(E)}{p}\right) = -1\,,$$

then p does not split completely in $K_5(E)$. Further if there exists a positive rational number u such that $\sqrt{a^2+20} = \sqrt{5}u$, then

$$D_5(E) = -5(u-2)(5u+2a+2)\,. \tag{9}$$

Thus by a simple calculation, we have the next theorem.

THEOREM 7. *For a rational number λ such that $5\lambda^2 - 1 > 0$, let E_λ be an elliptic curve defined by*

$$E_\lambda : y^2 = x^3 + 3375T(\lambda)x - 6750T(\lambda)\,,$$

where $T(\lambda) = \frac{R(\lambda)}{S(\lambda)}$ and

$$R(\lambda) = (\lambda-1)(10\lambda^2+5\lambda+1)^3\,,$$
$$S(\lambda) = (15\lambda^2+10\lambda+2)(5\lambda^2-5\lambda-1)^2(15\lambda^2+10\lambda+7)^2\,.$$

Then we have

(a) *The j-invariant $j(E_\lambda)$ and discriminant δ_{E_λ} of E_λ are*

$$j(E_\lambda) = \frac{8000(\lambda-1)(10\lambda^2+5\lambda+1)^3}{(5\lambda^2-1)^5}\,, \quad \delta_{E_\lambda} = \frac{-15625R(\lambda)^2(5\lambda^2-1)^5}{64S(\lambda)^3}\,.$$

(b) *For a prime number p such that*

$$\left(\frac{-(15\lambda^2+10\lambda+2)}{p}\right) = -1 \quad \textit{and} \quad \left(\frac{5\lambda^2-1}{p}\right) = 1\,,$$

p splits completely neither in $K_2(E_\lambda)$ nor in $K_5(E_\lambda)$. Furthermore, if p is of the form $p = 2^\alpha 5^\beta + 1$, then $\overline{E_\lambda}(\mathbf{F}_p)$ is cyclic.

PROOF. In the above argument, put

$$a = \frac{20\lambda}{5\lambda^2-1}\,.$$

Then

$$u = \frac{2(5\lambda^2+1)}{5\lambda^2-1} > 0\,.$$

By (6)$\sim$(8), we know the j-invariant $j(E_\lambda)$ of E_λ is

$$j(E_\lambda) = \frac{8000(\lambda-1)(10\lambda^2+5\lambda+1)^3}{(5\lambda^2-1)^5}\,.$$

By (9), we have

$$D_5(E_\lambda) = \frac{-5\cdot 4^2(15\lambda^2+10\lambda+2)}{(5\lambda^2-1)^2}\,.$$

Since $(\frac{5}{p}) = 1$,

$$\left(\frac{D_5(E_\lambda)}{p}\right) = \left(\frac{-(15\lambda^2+10\lambda+2)}{p}\right).$$

The discriminant of $x^3 + 3375T(\lambda)x - 6750T(\lambda) = 0$ is

$$D_2(E_\lambda) = -\frac{2^2 3^{12} 5^6 R(\lambda)^2(5\lambda^2-1)^5}{S(\lambda)^3}\,.$$

Therefore

$$\left(\frac{D_2(E_\lambda)}{p}\right) = \left(\frac{-(15\lambda^2+10\lambda+2)(5\lambda^2-1)}{p}\right).$$

The assumption in (b) implies

$$\left(\frac{D_5(E_\lambda)}{p}\right) = \left(\frac{D_2(E_\lambda)}{p}\right) = -1\,.$$

Hence the prime p splits completely neither in $K_2(E_\lambda)$ nor in $K_5(E_\lambda)$. □

In the above theorem, if we take λ such that $15\lambda^2 + 10\lambda + 2 = 3w^2$ for some $w \in \mathbf{Q}$, then

$$\left(\frac{D_5(E_\lambda)}{p}\right) = \left(\frac{-3}{p}\right) = -1\,.$$

Therefore we obtain the next theorem.

THEOREM 8. *Let $\varepsilon = 9 + 4\sqrt{5}$ and $\varepsilon^n = c_n + \sqrt{5}d_n (n \in \mathbf{Z})$. Put*

$$\lambda = \frac{-1-d_n}{3}\,.$$

For a prime number $p = 2^\alpha 5^\beta + 1$, if $(\frac{5d_n^2+10d_n-4}{p}) = 1$, then $\overline{E_\lambda}(\mathbf{F}_p)$ is cyclic.

PROOF. Consider the quadratic equation of λ:

$$15\lambda^2 + 10\lambda + 2 - 3w^2 = 0\,. \tag{10}$$

Its discriminant is $D' = 20(9w^2-1)$. Therefore if there exists $w \in \mathbf{Q}$ such that $9w^2-1 = 5L^2$ for $L \in \mathbf{Q}$, the equation (10) has $\mathbf{Q}$-rational roots. Set $\varepsilon = 9+4\sqrt{5}$, which is a unit of $\mathbf{Q}(\sqrt{5})$, and $\varepsilon^n = c_n + \sqrt{5}d_n (c_n, d_n \in \mathbf{Z})$. Then $c_n^2 - 5d_n^2 = 1$. Therefore if we put $w = \pm c_n/3$ and $L = \pm d_n$, then one of the roots of (10) is

$$\lambda = \frac{-1-d_n}{3}\,.$$

Thus

$$\left(\frac{-(15\lambda^2+10\lambda+2)}{p}\right) = \left(\frac{-3c_n^2}{p}\right) = \left(\frac{-3}{p}\right) = -1\,,$$

and since

$$\left(\frac{5\lambda^2-1}{p}\right) = \left(\frac{5d_n^2+10d_n-4}{p}\right),$$

by Theorem 7, we have our assertions. □

We shall give some examples of cyclic groups obtained from the elliptic curves in Theorem 8.

EXAMPLE 9. Put $\lambda = \frac{-1-d_n}{3}$.

1) $p = 2^7 5 + 1 = 641$.

n	2	3	5	6	7	8	15	16	28	79
$\lambda \bmod p$	403	210	637	397	318	418	303	164	566	101
$\overline{E_\lambda}(\mathbf{F}_p)$	C_{692}	C_{642}	C_{602}	C_{612}	C_{672}	C_{652}	C_{632}	C_{682}	C_{662}	C_{622}

2) $p = 2^5 5^3 + 1 = 4001$.

n	1	5	9	11	12	13	17	22	24	76
$\lambda \bmod p$	1332	2695	3590	2353	93	196	1458	1329	1147	443
$\overline{E_\lambda}(\mathbf{F}_p)$	C_{4032}	C_{4002}	C_{3972}	C_{3962}	C_{4052}	C_{4062}	C_{4042}	C_{4102}	C_{4122}	C_{4012}

EXAMPLE 10. 1) $p = 2^{30}5^{58} + 1$. Put $\lambda = \frac{-1-d_2}{3}$. Then

$$E_\lambda : y^2 = x^3 + Ax + B\,,$$

$$A = 659383519356383944211233770181584624749790589534 2$$

$$B = 240652325974914617407753245963683075050041882093 17$$

and

$$\overline{E_\lambda}(\mathbf{F}_p) \simeq C_{372529029846191406250000062494855718121648703732 32}\,.$$

2) $p = 2^{100}5^{36} + 1$. Put $\lambda = \frac{-1-d_4}{3}$. Then

$$E_\lambda : y^2 = x^3 + Ax + B\,,$$

$$A = 64524827801115519668308741908266115459762428289863677 67$$

$$B = 55417785134864476823382516183467769080475143420272644 67$$

and

$$\overline{E_\lambda}(\mathbf{F}_p) \simeq C_{184467440737095516160000000033348012232588127294099076 92}.$$

3.2. $p = 2^\alpha 5^\beta q^\gamma + 1$

3.2.1. $p = 2^\alpha 5^\beta q^\gamma + 1 (q \geq 7$:an odd prime). Next we consider primes p of the form $p = 2^\alpha 5^\beta q^\gamma + 1 (q \geq 7$:an odd prime). If q^2 does not divide $|\overline{E_\lambda}(\mathbf{F}_p)|$, then clearly $\overline{E_\lambda}(\mathbf{F}_p)$ is cyclic. Thus we have the following theorem.

THEOREM 11. *For primes p of the form $2^\alpha 5^\beta q^\gamma + 1 (q \geq 7$:an odd prime), let us consider the rational number*

$$\lambda = \frac{-1 - d_n}{3}$$

and the elliptic curve E_λ given in Theorems 7 and 8. Let E_λ^v be the twist of E_λ defined by

$$E_\lambda^v : y^2 = x^3 + 3375v^2T(\lambda)x - 6750v^3T(\lambda),\ v \in \mathbf{Z}\,.$$

If

$$\left(\frac{v}{p}\right) = -1 \ \textit{and}\ \left(\frac{5d_n^2 + 10d_n - 4}{p}\right) = 1\,,$$

then either $\overline{E_\lambda}(\mathbf{F}_p)$ or $\overline{E_\lambda^v}(\mathbf{F}_p)$ is cyclic.

PROOF. Since $q \not\equiv 0 \pmod 3$, $p = 2^\alpha 5^\beta q^\gamma + 1 \equiv 2 \pmod 3$. Thus similarly in Theorem 8,

$$\left(\frac{-(15\lambda^2 + 10\lambda + 2)}{p}\right) = \left(\frac{-3}{p}\right) = -1\,.$$

If

$$\left(\frac{5d_n^2 + 10d_n - 4}{p}\right) = 1\,,$$

then p splits completely neither in $K_5(E_\lambda)$ nor $K_2(E_\lambda)$. Further, if p splits completely in $K_q(E_\lambda)$, then we have $q^2 || \overline{E_\lambda}(\mathbf{F}_p)|$.

On the other hands, since

$$|\overline{E_\lambda}(\mathbf{F}_p)| + |\overline{E_\lambda^v}(\mathbf{F}_p)| = 2p + 2 \not\equiv 0 \pmod{q}$$

and $|\overline{E_\lambda}(\mathbf{F}_p)| \equiv 0 \pmod{q}$, we see $|\overline{E_\lambda^v}(\mathbf{F}_p)| \not\equiv 0 \pmod{q}$.

Now since $j(E_\lambda^v) = j(E_\lambda)$, $D_5(E_\lambda^v) = D_5(E_\lambda)$. Thus p does not split completely in $K_5(E_\lambda^v)$. Since the discriminant $D_2(E_\lambda^v)$ of $x^3 + 3375v^2T(\lambda)x - 6750v^3T(\lambda) = 0$ satisfies $D_2(E_\lambda) = v^6 D_2(E_\lambda^v)$, p does not split completely in $K_2(E^v)$, either.

Hence $\overline{E_\lambda^v}(\mathbf{F}_p)$ is cyclic. □

3.2.2. $p = 2^\alpha 3^\beta 5^\gamma + 1 (\alpha = 1, 2)$. Let p be a prime number of the form $p = 2^\alpha 3^\beta 5^\gamma + 1$. Since $p \equiv 1 \pmod 3$, for a parameter λ and the elliptic curve E_λ defined in Theorems 7 and 11, p may split completely in $K_5(E_\lambda)$. However, for these p, if $p \equiv 5, 7 \pmod 8$, thus $\alpha = 1, 2$, we can give another type of λ such that $\overline{E_\lambda}(\mathbf{F}_p)$ is cyclic.

THEOREM 12. *Let p be a prime number of the form $2^\alpha 3^\beta 5^\gamma + 1 (\alpha = 1, 2, \beta, \gamma > 0)$. Further if $\alpha = 1$, then we assume that $p \equiv 7 \pmod 8$. Put*

$$\varepsilon = \sqrt{6} - \sqrt{5}$$

and

$$\varepsilon^{2k-1} = m_{2k-1}\sqrt{6} + n_{2k-1}\sqrt{5} \ \ (k = 1, 2, 3, \cdots, m_{2k-1}, n_{2k-1} \in \mathbf{Z}) .$$

Let

$$\lambda = \frac{-1 - n_{2k-1}}{3}$$

and E_λ, E_λ^v be elliptic curves defined in Theorems 7 and 11. If

$$\left(\frac{5n_{2k-1}^2 + 10n_{2k-1} - 4}{p}\right) = 1 ,$$

then either $\overline{E_\lambda}(\mathbf{F}_p)$ or $\overline{E_\lambda^v}(\mathbf{F}_p)$ is cyclic.

PROOF. Consider the quadratic equation

$$15\lambda^2 + 10\lambda + 2 - 2w^2 = 0 . \tag{11}$$

Its discriminant is $D' = 20(6w^2 - 1)$. We shall give integers L and w such that $6w^2 - 1 = 5L^2$. Let $\varepsilon = \sqrt{6} - \sqrt{5}$. Then $\varepsilon^{2k-1} = m_{2k-1}\sqrt{6} + n_{2k-1}\sqrt{5}$ $(m_{2k-1}, n_{2k-1} \in \mathbf{Z})$. This shows that $6m_{2k-1}^2 - 5n_{2k-1}^2 = 1$. Therefore $(w, L) = (\pm m_{2k-1}, \pm n_{2k-1})$ are solutions of $6w^2 - 1 = 5L^2$. Put

$$\lambda = \frac{-1 - n_{2k-1}}{3} .$$

Then $15\lambda^2+10\lambda+2=2m_{2k-1}^2$. Thus

$$\left(\frac{-(15\lambda^2+10\lambda+2)}{p}\right)=\left(\frac{-2}{p}\right)=-1 \quad \text{and} \quad \left(\frac{5\lambda^2-1}{p}\right)=\left(\frac{5n_{2k-1}^2+10n_{2k-1}-4}{p}\right).$$

Therefore by the first part of (b) of Theorem 11 and the similar argument in its theorem, we have our assertions. □

3.2.3. Examples. The following two examples are groups of rational points of elliptic curves given in Theorems 11 and 12 respectively.

EXAMPLE 13. Put $\lambda=\frac{-1-d_n}{3}$ and $p=2^4 5^2 7+1=2801$.

n	4	6	7	8	15	18	23	25	26
$\lambda \bmod p$	2542	763	1159	1431	2760	66	2469	997	1783
$\overline{E_\lambda}(\mathbf{F}_p)$	C_{2712}	C_{2812}	C_{2892}	$C_{58}\times(C_7)^2$	C_{2722}	C_{2862}	C_{2842}	C_{2822}	C_{2742}
$\overline{E_\lambda^v}(\mathbf{F}_p)$	C_{2892}	C_{2792}	C_{2712}	C_{2762}	C_{2882}	C_{2742}	C_{2762}	C_{2782}	C_{2862}

EXAMPLE 14. Put $\lambda=\frac{-1-n_{2k-1}}{3}$.

1) $p=2\cdot 3\cdot 5^3+1=751$.

k	4	5	8	10	11	17	21	25
$\lambda \bmod p$	168	441	721	692	545	484	376	110
$\overline{E_\lambda}(\mathbf{F}_p)$	$C_{78}\times(C_3)^2$	C_{792}	C_{762}	C_{772}	C_{742}	C_{712}	C_{752}	C_{802}
$\overline{E_\lambda^v}(\mathbf{F}_p)$	C_{802}	C_{712}	C_{742}	C_{732}	C_{762}	$C_{88}\times(C_3)^2$	C_{752}	C_{702}

2) $p=2^2 3^4 5^2+1=8101$.

k	1	2	3	7	12	14	18	22	26
$\lambda \bmod p$	5400	0	5408	4484	6637	7311	6318	3628	1985
$\overline{E_\lambda}(\mathbf{F}_p)$	C_{8172}	C_{8102}	C_{8002}	C_{8052}	C_{8042}	C_{8122}	$C_{888}\times(C_3)^2$	C_{8032}	C_{7982}
$\overline{E_\lambda^v}(\mathbf{F}_p)$	C_{8032}	C_{8102}	C_{8202}	C_{8152}	C_{8162}	C_{8082}	C_{8212}	C_{8172}	C_{8222}

References

[1] N. ISHII, Defining equations of modular function fields, Math. Japon. **38**, No. 5 (1993), 941–951.

[2] N. ISHII, Families of cyclic groups of order obtained from the elliptic curves with CM-8, DMIS-RR-01-1 (2001).

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

[4] F. LEPRÉVOST and F. MORAIN, Revêtements de courbes elliptiques à multiplication complexe par des courbes hyperelliptiques et sommes de caractères, J. Number Theory **64** (1997), 165–182.

[5] A. R. RAJWADE, A note on the number of solutions N_p of congruence $y^2 \equiv x^3 - Dx \pmod p$, Proc. Cambridge Phil. Soc. **67** (1970), 603–605.

[6] A. R. RAJWADE, Certain classical congruences via elliptic curves, J. London Math. Soc. (2) **8** (1974), 60–62.

[7] A. R. RAJWADE, The Diophantine equation $y^2=x(x^2+21D+112D^2)$ and the conjectures of Birch and Swinnerton-Dyer, J. Austral. Math. Soc. **24** (1977), 286–295.

[8] J. H. SILVERMAN, *The Arithmetic of Elliptic Curves*, GTM106, Springer-Verlag (1986).
[9] C. WITTMAN, Group structure of elliptic curves over finite fields, J. Number Theory **88** (2001), 335–344.

Present Address:
GRADUATE SCHOOL OF SCIENCE, OSAKA PREFECTURE UNIVERSITY,
SAKAI, OSAKA, 599–8531 JAPAN.