J. KSIAM **Vol.4**, No.1, 29-38, 2000

A CRITERION ON PRIMITIVE ROOTS MODULO p

HWASIN PARK, JOONGSOO PARK AND DAEYEOUL KIM

ABSTRACT. In this paper, we consider a criterion on primitive roots modulo p where p is the prime of the form $p = 2^k q + 1$, q odd prime. For such p we also consider the least primitive root modulo p. Also, we deal with certain isomorphism classes of elliptic curves over finite fields.

§0. Introduction

In the famous book Disquisitiones Arithmeticae, C. F. Gauss had proved that the multiplicative group $\mathbb{Z}_p^*$ is cyclic and he had conjectured that 10 is a generator of $\mathbb{Z}_p^*$ for infinitely many p. We call a is a primitive root modulo p if a is a generator of $\mathbb{Z}_p^*$. In 1927, E. Artin generalized Gauss' conjecture as: For a not equal to 1, -1, or a perfect square, do there exist infinitely many primes p having a as a primitive root. In 1986, Artin's conjecture was proved for almost all primes but at most two primes by assuming the generalized Riemann hypothesis ([2]).

We note that Gauss' proof is not constructive, so that we have difficulties to get primitive roots modulo p. In this paper, we restrict ourselves p to be the prime of the form $p = 2q + 1$, $4q + 1$, $8q + 1 \cdots$ where q is an odd prime. We consider criterions that for which prime p , $a = 2, 3, 5, 7, \cdots$ can be primitive roots modulo p.

Also, we deal with isomorphism classes of elliptic curves over finite fields. These results are similar with the results of [8].

§1. Primitive roots

Let p and q be odd primes.

1991 AMS Subject Classification: 11A07, 11A15, 11A41, 14H52.
Key words and phrases: primitive roots, elliptic curves over finite fields.

Lemma 1.1. *Let* $p = 2^k q + 1$, $k \in \mathbb{Z}^+$. *Then the set of primitive roots modulo* p *is the set of quadratic non-residues modulo* p *except for* a *such that*

$$a^s \equiv -1 \pmod{p}, \quad s = 2^{k-1}.$$

Proof. Let S be the set of primitive roots modulo p and let T be the subset of $\mathbb{Z}_p^*$ which are quadratic non-residues modulo p. If $a \in S$, then $(a,p) = 1$ and $a^{p-1} \equiv 1 \pmod{p}$. Since $p-1$ is the smallest, $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. Then $a \in T$. Thus $S \subset T$. Also, $\mid S \mid = \phi(\phi(p)) = \phi(2^k q) = 2^{k-1}(q-1)$ and $\mid T \mid = \frac{p-1}{2} = 2^{k-1}q$. Thus $\mid T \mid - \mid S \mid = 2^{k-1}$.
Case I. $k = 1$. We know that $-1 \in T$ and $-1 \notin S$, since $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}} = (-1)^q = -1$ and $(-1)^2 \equiv 1 \pmod{p}$. In this case, $\mid T \mid - \mid S \mid = 1$, and $a = -1$ satisfies Lemma.
Case II. $k > 1$. Then $a \in T$, since $(\frac{a}{p}) \equiv a^{\frac{p-1}{2}} \pmod{p} = a^{2^{k-1}q} \equiv (-1)^q \pmod{p} = -1$. But $a \notin S$, since a is a perfect square modulo p if $k > 1$. In this case, $\mid T \mid - \mid S \mid = 2^{k-1}$ and $a^{2^{k-1}} \equiv -1 \pmod{p}$ has 2^{k-1} incongruent solutions. Thus Lemma holds.

By Lemma 1.1, we can show the following:

Theorem 1.2. *Let* $p = 2q + 1$.

(1) 2 *is a primitive root modulo* p *if and only if* $q \equiv 1 \pmod{4}$.
In this case, 2 *is the least primitive root modulo* p.
(2) 3 *is a primitive root modulo* p *if and only if* $q = 3$.
In this case, 3 *is the least primitive root modulo* p.
(3) 5 *is a primitive root modulo* p *if and only if* $q \equiv 1, 3 \pmod{5}$.
In particular, 5 *is the least primitive root modulo* p *if and only if* $q \equiv 3, 11 \pmod{20}$.
(4) 6 *is a primitive root modulo* p *if and only if* $q \equiv 5 \pmod{12}$.
(5) 7 *is a primitive root modulo* p *if and only if* $q \equiv 5, 11 \pmod{14}$.
In particular, 7 *is the least primitive root modulo* p *if and only if* $q \equiv 19, 39 \pmod{140}$.
(6) 8 *is a primitive root modulo* p *if and only if* $q \equiv 1 \pmod{4}$.
(7) 10 *is a primitive root modulo* p *if and only if* $q \equiv 3, 9, 11 \pmod{20}$.
(8) 11 *is a primitive root modulo* p *if and only if* $q \equiv 1, 7, 13, 15 \pmod{22}$, *or* $q = 11$.
In particular, 11 *is the least primitive root modulo* p *if and only if* $q \equiv$ 79, 139, 279, 359, 419, 499, 519, 639, 799, 939, 1079, 1399 (mod 1540).
(9) 12 *is not a primitive root for all* p.
(10) 13 *is a primitive root modulo* p *if and only if* $q \equiv 2, 3, 5, 7, 9, 10 \pmod{13}$.
In particular, 13 *is the least primitive rot modulo* p *if and only if* $q \equiv$ 659, 699, 839, 919, 1219, 1359, 1539, 2239, 2319, 2459, 2759, 3039, 3299, 3779, 4139, 4299, 4579, 4839, 5179, 5319, 6119, 6159, 6379, 6819, 6939, 6999, 7079, 7519, 7699, 7919, 8479, 8759, 9239, 9799, 9939, 10019, 10299, 10459, 10779, 11339,

11559, 11619, 11839, 12139, 12279, 12539, 12979, 13159, 13239, 13379, 13679, 14419, 15219, 15399, 16099, 16179, 16239, 16619, 17599, 17859, 17999, 18439, 18699, 19039, 19139, 19399 $\pmod{20020}$.

Proof. (1) By Lemma 1.1, 2 is a primitive root modulo p if and only if 2 is a quadratic non-residue modulo p. By the quadratic reciprocity law, p must be congruent $\pm 3 \pmod 8$. Thus $q \equiv 1 \pmod 4$. (2) By the quadratic reciprocity law, $(\frac{3}{p}) = -1$ if and only if $p \equiv \pm 5 \pmod{12}$.

Case. $p \equiv 5 \pmod{12}$. Then $q = 6k + 2$ for some $k \in \mathbb{Z}$. It is impossible.

Case. $p \equiv -5 \pmod{12}$. Then $q = 6k + 3$. Thus $q = 3$.

(3) Note that $(\frac{5}{p}) = -1$ if and only if $p \equiv \pm 2 \pmod 5$.

Case. $q = 5$. Then $p = 11$ and $(\frac{5}{11}) = 1$. This case must be omitted.

Case. $q = 5k + 1$. Then $p = 2q + 1 = 10k + 3 \equiv -2 \pmod 5$. In this case, we have $(\frac{5}{p}) = -1$.

Case. $q = 5k + 2$. Then $p = 2q + 1 = 10k + 5$. It is impossible.

Case. $q = 5k + 3$. Then $p = 2q + 1 = 10k + 7 \equiv 2 \pmod 5$. In this case, we have $(\frac{5}{p}) = -1$.

Case. $q = 5k + 4$. Then $p = 2q + 1 = 10k + 9 \equiv 5$. Then $(\frac{5}{p}) = 1$. This case must be omitted.

In particular, 5 is the least primitive root modulo p if and only if $q \equiv 3 \pmod 4, q \neq 3$, and $q \equiv 1, 3 \pmod 5$. By the chinese remainder theorem, $q \equiv 3, 11 \pmod{20}$.

(4) If $q \equiv 5 \pmod{12}$, then by (1), 2 is a primitive root modulo p. By Lemma 1.1, $(\frac{2}{p}) = -1$. Also, by (2), $(\frac{3}{p}) = 1$. Thus $(\frac{6}{p}) = -1$. That is 6 is a primitive root modulo p.

Conversely, if 6 is a primitive root modulo p. Then $(\frac{6}{p}) = -1$ and $p \neq 7$. We have two cases.

Case I. $(\frac{2}{p}) = 1$ and $(\frac{3}{p}) = -1$. Then by (1) and (2), $q \equiv 3 \pmod 4$ and $q = 3$. This case contradicts to $p \neq 7$.

Case II. $(\frac{2}{p}) = -1$ and $(\frac{3}{p}) = 1$. Then by (1) and the quadratic reciprocity law, we get $q \equiv 1 \pmod 4$ and $p \equiv \pm 1 \pmod{12}$. If $p \equiv 1 \pmod{12}$, then we get a contradiction. Thus we have $p \equiv -1 \pmod{12}$ and then $q \equiv 5 \pmod 6$. Thus we have $q \equiv 5 \pmod{12}$.

(5) By the quadratic reciprocity law, $(\frac{7}{p}) = -1$ if and only if $p \equiv \pm 5, \pm 11, \pm 13 \pmod{28}$.

Case. $p = 28k + 5$. Then $q = 14k + 2$.

Case. $p = 28k + 23$. Then $q = 14k + 11$.

Case. $p = 28k + 11$. Then $q = 14k + 5$.

Case. $p = 28k + 17$. Then $q = 14k + 8$.

Case. $p = 28k + 13$. Then $q = 14k + 6$.

Case. $p = 28k + 15$. Then $q = 14k + 7$.

Since q is odd prime, we have $q \equiv 5, 11 \pmod{14}$.

In particular, 7 is the least primitive root modulo p if and only if

$$\begin{cases} q \equiv 3 \pmod 4, \quad q \neq 3, \\ q \equiv 4 \pmod 5, \\ q \equiv 5, 11 \pmod{14}. \end{cases}$$

By the chinese remainder theorem, $q \equiv 19, 39 \pmod{140}$.

(6) Similar with (4).

(7) By (1), (3) and the Chinese remainder theorem, we can show (7).

(8) By the quadratic reciprocity law, 11 is a quadratic non-residue modulo p if and only if $p \equiv \pm 3, \pm 13, \pm 15, \pm 17, \pm 21 \pmod{44}$. Case. $p = 44k+3$. Then $q = 22k+1$.
Case. $p = 44k + 41$. Then $q = 22k + 20$.
Case. $p = 44k + 13$. Then $q = 22k + 6$.
Case. $p = 44k + 31$. Then $q = 22k + 15$.
Case. $p = 44k + 15$. Then $q = 22k + 7$.
Case. $p = 44k + 29$. Then $q = 22k + 14$.
Case. $p = 44k + 17$. Then $q = 22k + 8$.
Case. $p = 44k + 27$. Then $q = 22k + 13$.
Case. $p = 44k + 21$. Then $q = 22k + 10$.
Case. $p = 44k + 23$. Then $q = 22k + 11$.
Since q is odd prime, we have $q \equiv 1, 7, 11, 13, 15 \pmod{22}$.

In particular, 11 is the least primitive root modulo p if and only if

$$\begin{cases} q \not\equiv 1 \pmod 4, \quad q \neq 3, \\ q \not\equiv 1, 3 \pmod 5, \\ q \not\equiv 5, 11 \pmod{14}, \\ q \equiv 3, 9, 11, 17 \pmod{20}, \\ q \equiv 1, 7, 13, 15 \pmod{22}. \end{cases}$$

That is,

$$\begin{cases} q \equiv 3 \pmod 4, \quad q \neq 3, & \text{(i)} \\ q \equiv 4 \pmod 5, & \text{(ii)} \\ q \equiv 1, 9, 13 \pmod{14}, \quad \text{or} \quad q = 7, & \text{(iii)} \\ q \equiv 1, 7, 13, 19 \pmod{20}, & \text{(iv)} \\ q \equiv 1, 7, 13, 15 \pmod{22}. & \text{(v)} \end{cases}$$

We do not need $q \equiv 19 \pmod{20}$ in (iv) because of (i) and (ii). We also do not need (iv) because (i), (ii), (iii), (v) and (iv) has no simultaneous solution by the Chinese remainder theorem. Thus 11 is the least primitive root modulo p if and only if

$$\begin{cases} q \equiv 3 \pmod 4, \quad q \neq 3, \\ q \equiv 4 \pmod 5, \\ q \equiv 1, 9, 13 \pmod{14}, \quad \text{or} \quad q = 7, \\ q \equiv 1, 7, 13, 15 \pmod{22}. \end{cases}$$

By the chinese remainder theorem, we have $q \equiv 79$, 139, 279, 359, 419, 499, 519, 639, 799, 939, 1079, 1399 (mod 1540).

(9) By Lemma 1.1, 12 is a primitive root modulo p if and only if $(\frac{12}{p}) = -1$. That is, $(\frac{3}{p}) = -1$. Then by (2), p must be 7. But 12 is not a primitive root modulo 7.

(10) 13 is a quadratic non-residue modulo p if and only if $p \equiv \pm 2, \pm 5, \pm 6 \pmod{13}$.
Case. $q = 13$. Then $p = 27$.
Case. $q = 13k+1$. Then $p = 26k+3 \equiv 3 \pmod{13}$.
Case. $q = 13k+2$. Then $p = 26k+5 \equiv 5 \pmod{13}$.
Case. $q = 13k+3$. Then $p = 26k+7 \equiv 7 \pmod{13}$.
Case. $q = 13k+4$. Then $p = 26k+9 \equiv 9 \pmod{13}$.
Case. $q = 13k+5$. Then $p = 26k+11 \equiv 11 \pmod{13}$.
Case. $q = 13k+6$. Then $p = 26k+13$.
Case. $q = 13k+7$. Then $p = 26k+15 \equiv 2 \pmod{13}$.
Case. $q = 13k+8$. Then $p = 26k+17 \equiv 4 \pmod{13}$.
Case. $q = 13k+9$. Then $p = 26k+19 \equiv 6 \pmod{13}$.
Case. $q = 13k+10$. Then $p = 26k+21 \equiv 8 \pmod{13}$.
Case. $q = 13k+11$. Then $p = 26k+23 \equiv 10 \pmod{13}$.
Case. $q = 13k+12$. Then $p = 26k+25 \equiv 12 \pmod{13}$.
Since p is the prime of the form $p \equiv \pm 2, \pm 5, \pm 6 \pmod{13}$, $q \equiv 2, 3, 5, 7, 9, 10 \pmod{13}$.

In particular, 13 is the least primitive root modulo p if and only if

$$\begin{cases} q \equiv 3 \pmod 4, \quad q \neq 3, \\ q \equiv 4 \pmod 5, \\ q \equiv 1, 9, 13 \pmod{14}, \quad \text{or} \quad q = 7, \\ q \equiv 3, 9, 17, 21 \pmod{22}, \\ q \equiv 2, 3, 5, 7, 9, 10 \pmod{13}. \end{cases}$$

By the chinese remainder theorem, we have $q \equiv 659$, 699, 839, 919, 1219, 1359, 1539, 2239, 2319, 2459, 2759, 3039, 3299, 3779, 4139, 4299, 4579, 4839, 5179, 5319, 6119, 6159, 6379, 6819, 6939, 6999, 7079, 7519, 7699, 7919, 8479, 8759, 9239, 9799, 9939, 10019, 10299, 10459, 10779, 11339, 11559, 11619, 11839, 12139, 12279, 12539, 12979, 13159, 13239, 13379, 13679, 14419, 15219, 15399, 16099, 16179, 16239, 16619, 17599, 17859, 17999, 18439, 18699, 19039, 19139, 19399 (mod 20020).

Corollary 1.3. *([3, 4, 5]) Let $p = 2q+1$. 6 and 8 are primitive roots modulo p if and only if so is 2. In particular, 2, 6, and 8 are not primitive roots modulo p if and only if $q \equiv 3 \pmod 4$.*

Proof. By Theorem 1.2 (1), 2 is a primitive root modulo p if and only if $q \equiv 1 \pmod 4$. Then $q \equiv 5 \pmod{12}$. For $q \equiv 1 \pmod{12}$ or $q \equiv 9 \pmod{12}$ contradict to p and q are primes. By Theorem 1.2 (4), 6 must be a primitive root modulo p. By Theorem 1.2 (1) and (6), 2 and 8 occur simultaneously as a primitive root modulo p.

Remark 1.4. (1) We use Mathematica 3.0 to solve the Chinese remainder theorem and to get the following (2).

(2) Let $p = 2q + 1$. The least primitive root modulo p are relatively small. If $\chi(p)$ denotes the least primitive root modulo p. Then for $p \leq 551208899$, $\chi(p) = 2$ takes place approximately 50%, and $\chi(p) = 5$ happens approximately 33%. If we denote that $h(0)$ is the total number of primes p, $p \leq 551208899$, and $h(a)$ is the number of primes p which has a as the least primitive root modulo p. Then we have the following table:

a	$h(a)$	a	$h(a)$	a	$h(a)$	a	$h(a)$
0	1042225	19	5870	53	25	89	0
2	520747	23	3112	59	7	97	0
3	1	29	1858	61	4	101	0
5	347767	31	823	67	1	103	0
7	69369	37	456	71	2	107	0
11	46115	41	217	73	1	109	0
13	31684	43	104	79	0	$a \geq 113$	0
17	14014	47	48	83	0		

Theorem 1.5. *Let $p = 4q + 1$. Then 2 is the least primitive root modulo p for all p.*

Proof. Since q is odd, $p = 4(2k + 1) + 1 = 8k + 5$. By the quadratic reciprocity law, 2 is a quadratic non-residue modulo p for all p. The smallest p is 13, so $2^2 \equiv 4 \not\equiv -1 \pmod{p}$ for all p. By Lemma 1.1, 2 is a primitive root modulo p for all p. In particular, 2 is the least primitive root modulo p for all p.

Theorem 1.6. *Let $p = 8q + 1$.*

(1) *2 is not a primitive root modulo p for all p.*
(2) *3 is the least primitive root modulo p for all p except for $p = 41$.*

Proof. (1) 2 is not a primitive root modulo p, since $(\frac{2}{p}) = 1$.

(2) Case. $q = 3$. Then $p = 25$. It is impossible.
Case. $q = 3k + 1$. Then $p = 3(8k + 3)$. It is impossible.
Case. $q = 3k + 2$. Then $p = 24k + 17$. Then $p \equiv 5 \pmod{12}$. By the quadratic reciprocity law, $(\frac{3}{p}) = -1$ for all p. Thus by Lemma 1.1, 3 is a primitive root modulo p for all p except for $p = 41$, since $3^4 \equiv -1 \pmod{p}$ has only one p, $p = 41$. Actually, 7 is the least primitive root modulo 41.

Remark 1.7. (1) Similarly, we get the following: If $p = 2^n q + 1, n \geq 4, q \neq 3, p > 3^{2^{n-1}}$, then 3 is the least primitive root modulo p for all p. In particular, 3 is the least primitive root modulo p for all $p = 16q + 1$, $32q + 1$, $64q + 1$, $\cdots$.

(2) We get a result that is similar to Theorem 1.2 for $p = 4q + 1$, $8q + 1$.

§2. Some other cases

Lemma 2.1. *Let $p = 2^n + 1$ be a prime with $n \geq 1$. Then the set S of primitive root modulo p is the set T of quadratic non-residues modulo p.*

Proof. In the proof of Lemma 1.1, we have $S \subseteq T$. Also, $\mid S \mid = \phi(\phi(p)) = 2^{n-1}$ and $\mid T \mid = \frac{p-1}{2} = 2^{n-1}$. Thus we have $S = T$.

Proposition 2.2. *Let $p = 2^n + 1$ be a prime with $n \geq 1$.*

(1) 2 *is the least primitive root modulo p when $n = 1, 2$.*
(2) *For $n \geq 3$,* 3 *is the least primitive root modulo p for all p.*

Proof. (1) By computation, it is clear.

(2) Since $p = 2^n + 1$ and $n \geq 3$, $p \equiv 1 \pmod 4$. Also, $p \equiv 2 \pmod 3$. For if $p \equiv 1 \pmod 3$, then $2^n + 1 \equiv 1 \pmod 3$, get a contradiction. ¿From $p \equiv 1 \pmod 4$ and $p \equiv 2 \pmod 3$, we have $p \equiv 5 \pmod{12}$. By the quadratic reciprocity law, $(\frac{3}{p}) = -1$. By Lemma 2.1, 3 is a primitive root modulo p for all p. Note that $p \equiv 1 \pmod 8$, since $n \geq 3$. By the quadratic reciprocity law, $(\frac{2}{p}) = 1$. Thus 2 is not a primitive root modulo p for all p.

Corollary 2.3. *Let p be a Fermat's prime. Then* 3 *is the least primitive root modulo p.*

Remark 2.4. Erdos ([1]) asks if p is large enough, is there always a prime r so that r is a primitive root modulo p ?

If $p = 2^n + 1$ is a prime with $n \geq 1$. Then this is true. For if b is a quadratic non-residue modulo p and $b = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$, then $(\frac{p_1}{p})^{e_1} \cdots (\frac{p_t}{p})^{e_t} = -1$. Then $(\frac{p_i}{p}) = -1$ for some i. Then by Lemma 2.1, p_i is a primitive root modulo p for large enough p.

§3 Application to elliptic curves over finite field $\mathbb{F}_p$

Let p and q be odd primes and let K be a field with $\mathrm{char}(K) > 3$.

Proposition 3.1. *([6], [7]) Two elliptic curves $E_a^b : y^2 = x^3 + ax + b$ and $E_{a'}^{b'} : y^2 = x^3 + a'x + b'$ defined over K are isomorphic over K if and only if there exists $u \in K^*$ such that $u^4 a' = a$ and $u^6 b' = b$. If $E_a^b \cong E_{a'}^{b'}$ over K, then the isomorphism is given by*

$$\phi : E_a^b \to E_{a'}^{b'}, \quad \phi : (x, y) \mapsto (u^{-2}x, u^{-3}y),$$

or equivalently

$$\psi : E_{a'}^{b'} \to E_a^b, \quad \psi : (x, y) \mapsto (u^2 x, u^3 y).$$

Theorem 3.2. *Let $E_a^0 : y^2 = x^3 + ax$, $E_{ag^{2i}}^0 : y^2 = x^3 + ag^{2i}x$ and $E_{ag^{4i}}^0 : y^2 = x^3 + ag^{4i}x$ be elliptic curves defined over $\mathbb{F}_p$ and let g be a primitive root modulo p.*

(1) *If $p \equiv 1 \pmod 4$, then E_a^0 is isomorphic to $E_{ag^{4i}}^0$ where $1 \leq i \leq \frac{p-1}{4}$.*
(2) *If $p \equiv 3 \pmod 4$, then E_a^0 is isomorphic to $E_{ag^{2i}}^0$ where $1 \leq i \leq \frac{p-1}{2}$.*

Proof. (1) For each $i = 1, 2, \cdots, \frac{p-1}{4}$, take $u^4 = g^{p-1-4i}$. Then $u^4 a g^{4i} = g^{(p-1)-4i} a g^{4i}$ $= a g^{p-1} = a$. Also, $u = g^{\frac{p-1-4i}{4}} = g^{\frac{p-1}{4}} g^{-i} \in \mathbb{F}_p^*$, since $p \equiv 1 \pmod 4$. This u satisfies the conditon of Proposition 3.1. Thus $E_a^0 \cong E_{ag^{4i}}^0$ for $i = 1, 2, \cdots, \frac{p-1}{4}$. That is, $E_a^0 \cong E_{ag^4}^0 \cong E_{ag^8}^0 \cong \cdots \cong E_{ag^{p-1}}^0$.

(2) By the same way with (1), $E_a^0 \cong E_{ag^{2i}}^0$ for $i = 1, 2, \cdots, \frac{p-1}{2}$. That is, $E_a^0 \cong E_{ag^2}^0$ $\cong E_{ag^4}^0 \cong \cdots \cong E_{ag^{p-1}}^0$.

Corollary 3.3. *Let T be the set of ellitic curves of the form $y^2 = x^3 + ax$ defined over $\mathbb{F}_p$. We denote $[E_a^0]$ be the isomorphism class containing E_a^0.*

(1) *If $p \equiv 1 \pmod 4$, then the number of isomorphism classes of elliptic curves in T is 4:*

$$[E_1^0] \ni y^2 = x^3 + x,\ [E_g^0] \ni y^2 = x^3 + gx,\ [E_{g^2}^0] \ni y^2 = x^3 + g^2 x,\ [E_{g^3}^0] \ni y^2 = x^3 + g^3 x,$$

where g is a primitive root modulo p.

(2) *If $p \equiv 3 \pmod 4$, then the number of isomorphism classes of elliptic curves in T is 2:*

$$[E_1^0] \ni y^2 = x^3 + x,\ [E_g^0] \ni y^2 = x^3 + gx,$$

where g is a primitive root modulo p.

Proof. (1) We have four isomorphism classes:

$$E_1^0 \cong E_{g^4}^0 \cong E_{g^8}^0 \cong \cdots,$$

$$E_g^0 \cong E_{g^5}^0 \cong E_{g^9}^0 \cong \cdots,$$

$$E_{g^2}^0 \cong E_{g^6}^0 \cong E_{g^{10}}^0 \cong \cdots,$$

$$E_{g^3}^0 \cong E_{g^7}^0 \cong E_{g^{11}}^0 \cong \cdots.$$

(2) We have two isomorphism classes:

$$E_1^0 \cong E_{g^2}^0 \cong E_{g^4}^0 \cong \cdots,$$

$$E_g^0 \cong E_{g^3}^0 \cong E_{g^5}^0 \cong \cdots.$$

Corollary 3.4. *Let $p = 2q + 1$.*

(1) *If $q \equiv 1 \pmod 4$, then there are two isomorphism classes of elliptic curves over $\mathbb{F}_p$:*

$$[E_1^0], [E_2^0].$$

(2) *If $q = 3$, then there are two isomorphism classes of elliptic curves over $\mathbb{F}_p$:*

$$[E_1^0], [E_3^0].$$

(3) *If* $q \equiv 3, 9, 11 \pmod{20}$, *then there are two isomorphism classes of elliptic curves over* $\mathbb{F}_p$*:*

$$[E_1^0], [E_{10}^0].$$

(4) *If* $q \equiv 79, 139, 279, 359, 419, 499, 519, 639, 799, 939, 1079, 1399 \pmod{1540}$, *then there are two isomorphism classes of elliptic curves over* $\mathbb{F}_p$*:*

$$[E_1^0], [E_{11}^0].$$

Proof. (1) By Theorem 1.2, if $q \equiv 1 \pmod 4$, then 2 is the primitive root modulo p . Since q is odd, $p \equiv 3 \pmod 4$ for all p. By Corollary 3.3, we have two isomorphism classes.

(2), (3), (4) follow by Theorem 1.2 and Corollary 3.3.

Corollary 3.5. *Let* $p = 4q + 1$. *There are four isomorphism classes of elliptic curves over* $\mathbb{F}_p$*:*

$$[E_1^0], [E_2^0], [E_4^0], [E_8^0].$$

Corollary 3.6. *Let* $p = 8q + 1$ *with* $p > 41$. *There are four isomorphism classes of elliptic curves over* $\mathbb{F}_p$*:*

$$[E_1^0], [E_3^0], [E_9^0], [E_{27}^0].$$

Example 3.7. Let $E_2^0 : y^2 = x^3 + 2x$ over $\mathbb{F}_{13}$. Then E_2^0 is isomorphic to $E_6^0 : y^2 = x^3 + 6x$ and $E_5^0 : y^2 = x^3 + 5x$. In fact,

$$E_2^0(\mathbb{F}_{13}) = \{O, (0,0), (1,4), (1,9), (2,5), (2,8), (11,1), (11,12), (12,6), (12,7)\}.$$

Using by Proposition 3.1,

$$E_6^0(\mathbb{F}_{13}) = \{O, (0,0), (10,7), (10,6), (7,12), (7,1), (6,5), (6,8), (3,4), (3,9)\},$$

and

$$E_5^0(\mathbb{F}_{13}) = \{O, (0,0), (9,9), (9,4), (5,8), (5,5), (8,12), (8,1), (4,7), (4,6)\}.$$

References

[1] R. K. Guy, *Unsolved problems in number theory*, Springer-Verlag, 1994.

[2] D. R. Heath-Brown, *Artin's conjecture for primitive roots*, Quart. J. Math., Oxford Ser. (2) **37** (1986), 27-38.

[3] D. H. Lehmer and Emma Lehmer, *On runs of residues*, Proc. Amer. Math. Soc. **13** (1962), 102-106.

[4] D. H. Lehmer, Emma Lehmer and W. H. Mills, *Pairs of consecutive powerresidues*, Canad. J. Math. **15** (1963), 172-177.

[5] D. H. Lehmer, Emma Lehmer, W. H. Mills and J. L. Selfridge, *Machine proof of a theorem on cubic residues*, Math. Comput. **16** (1962), 407-415.

[6] A. Menezes, *Elliptic curve public key cryptosystems*, Kluwer Academic Publ., 1993.
[7] J. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, New York, 1986.
[8] E. Waterhouse, *Abelian varieties over finite fields*, Ann. Sci. Ecole Norm. Sup. 2 (1969), 521–560.

Department of Mathematics,
Chonbuk National University,
Chonju, Chonbuk, 561-756, Korea

Department of Mathematics,
Woosuk University,
Samlae, Wanju, Chonbuk, 565-701, Korea
jspark@core.woosuk.ac.kr

Department of Mathematics,
Chonbuk National University,
Chonju, Chonbuk, 561-756, Korea
dykim@math.chonbuk.ac.kr